



# Regulating Electronic Means to Fight the Spread of COVID-19

Argentina • Australia • Brazil • China • England  
European Union • France • Iceland • India • Iran  
Israel • Italy • Japan • Mexico • Norway • Portugal  
Russian Federation • South Africa • South Korea  
Spain • Taiwan • Turkey • United Arab Emirates

June 2020

LL File No. 2020-019000

This report is provided for reference purposes only.  
It does not constitute legal advice and does not represent the official  
opinion of the United States Government. The information provided  
reflects research undertaken as of the date of writing.  
It has not been updated.

# Contents

- Comparative Summary ..... 1
- Map: COVID-19 Contact Tracing Apps in Selected Jurisdictions ..... 4
- The Americas**
- Argentina..... 5
- Brazil ..... 11
- Mexico..... 17
- East Asia, South Asia and Pacific**
- Australia ..... 22
- China..... 41
- India ..... 49
- Japan ..... 63
- South Korea..... 70
- Taiwan ..... 75
- Europe and Central Asia**
- European Union ..... 80
- England..... 95
- France..... 107
- Iceland..... 115
- Italy ..... 124
- Norway ..... 130
- Portugal ..... 139
- Russian Federation..... 143
- Spain ..... 151

Turkey..... 158

**Middle East and Africa**

Iran ..... 167

Israel..... 177

South Africa ..... 186

United Arab Emirates ..... 201

# Comparative Summary

Jenny Gesley  
*Foreign Law Specialist*

This report surveys the regulation of electronic means to fight the spread of COVID-19 in 23 selected jurisdictions around the globe, namely Argentina, Australia, Brazil, China, England, France, Iceland, India, Iran, Israel, Italy, Japan, Mexico, Norway, Portugal, the Russian Federation, South Africa, South Korea, Spain, Taiwan, Turkey, the United Arab Emirates, and the European Union (EU).

As of June 4, 2020, a total of 6.4 million confirmed cases of COVID-19 had been reported worldwide, with the most cases being reported in the United States (1.8 million), Brazil (555,383), and the Russian Federation (432,277).<sup>1</sup> Of those cases, 383,872 people have died.<sup>2</sup> COVID-19 is caused by the SARS-CoV-2 virus and spreads from person to person through droplet and contact transmission. Currently, there is no known cure or vaccine. Countries therefore have to find other ways to control and mitigate the spread of this infectious disease in order to break the chain of human-to-human transmission, such as case identification, isolation, testing, contact tracing, quarantine, and location tracking.

Many governments have turned to electronic measures to provide information to individuals about the COVID-19 pandemic, check symptoms, trace contacts and alert persons who have been in proximity to an infected person, identify “hot spots,” and track compliance with confinement measures and stay-at-home orders. Dedicated coronavirus apps that are downloaded to an individual’s mobile phone, the use of anonymized mobility data, and creating electronic databases are the most common measures. However, it is unclear whether such digital solutions by themselves are sufficient to contain the spread of the virus. The World Health Organization (WHO) recommends using digital proximity tracking only as a supplement to other measures such as increased testing and manual contact tracing.<sup>3</sup>

Most of the surveyed jurisdictions have developed one or several dedicated coronavirus apps with different functionalities, such as general information and advice about COVID-19, symptom checkers, and contact tracing and warning. In order to be effective and provide accurate information, the applications need enough data, meaning enough people need to download the app. Some countries had low download rates, or, as in the case of Norway, only initial high enthusiasm. Other problems observed were technical glitches in computer systems that led to false information being reported, which happened in Russia, where people were erroneously fined or fined several times. In the UK, there were reports that the app was unable to work properly if another app was being actively used.

---

<sup>1</sup> WHO *Coronavirus Disease (COVID-19) Dashboard*, World Health Organization [WHO], <https://perma.cc/567D-J854>.

<sup>2</sup> *Id.*

<sup>3</sup> WHO, *Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing 1* (May 28, 2020), <https://perma.cc/5NRA-XUFA>.

In the majority of the surveyed jurisdictions, the download of a COVID-19 app is voluntary. The EU in non-binding guidance to Member States recommended the use of voluntary apps because of the “high degree of intrusiveness” of mandatory apps. However, some exceptions were observed. In the UK, a body established to consider the ethics of the app noted that it would be possible to require the app for individuals returning to work or using public transportation. In Argentina, installing the contact tracing app is generally voluntary; however, people who enter the country from abroad and people who return to work are obligated to install it. India’s contact tracing app’s use was considered voluntary when launched in early April but became mandatory for public- and private-sector employees in early May. This requirement was eased in late May after criticism from privacy and digital rights organizations. In China, even though the health code apps that assign different color codes to people depending on their infection status appear not to have been made compulsory, they are de facto compulsory in many cities as citizens without the code are not able to enter most public places. In Turkey, travelers whose HES codes on their app indicate that they were diagnosed as positive or have been in contact with a person diagnosed as such are not allowed to use public transportation or airplanes. In Russia, all people identified as having been in contact with an infected individual must install the “Social Monitoring app” or face a fine. Individuals with no cell phone receive special devices with a preinstalled Social Monitoring app. And, as noted below, in some countries persons required to quarantine must install an app to allow the authorities to monitor their movement.

Some of the surveyed jurisdictions have also established databases in which the health information of infected persons is logged. South Africa established an interim database in which health care professionals who test a person for COVID-19 must enter the person’s identification and contact information, including cellphone number, for inclusion in the database. The French government has developed two electronic databases, one where all COVID-19 test results are recorded and one to facilitate contact tracing. The data in both systems may only be accessed by medical professionals who are subject to medical confidentiality. In China, the health code apps reportedly rely on a combination of self-reporting by the user, COVID-19 databases set up by government authorities, and data held by other sources, including the public transportation, telecommunications, and banking sectors.

Technology is also used to measure compliance with quarantine measures or stay-at-home orders. South Korea has developed an electronic wristband that monitors people’s compliance with self-quarantine; however, it is not mandatory and violators must consent to wearing it. Spain used mobile phone location data to track people’s movements and verify how closely the nationwide lockdown was being observed. Norway used telecommunication data to determine whether people complied with travel restrictions during the month of March 2020; however, no individuals were targeted by that approach. In Russia, QR codes that serve as digital passes were required to use public transportation for the self-isolated population. Taiwan’s “digital fence” monitors the location of those required to undergo home quarantine via their own cellphones or government-issued cellphones, with the goal of preventing their movement. In the United Arab Emirates, people who are ordered to quarantine must install an app, which sends alerts to them to stay within the range of movement allowed during the quarantine and provides health authorities with the precise location of these individuals.

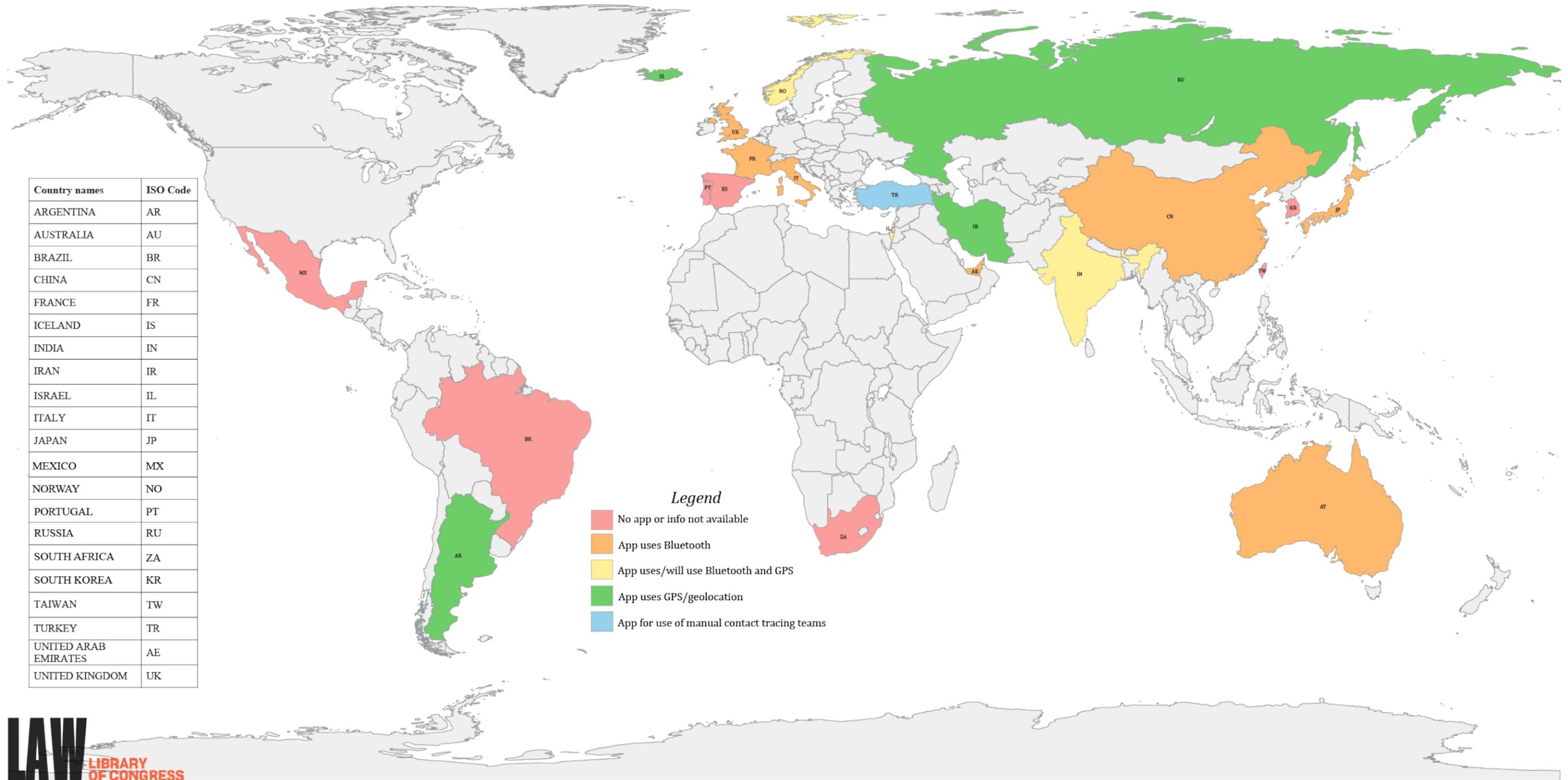
Furthermore, a few selected surveyed countries have used other electronic means to fight the spread of COVID-19. The Italian Civil Aviation Authority has approved the use of drones by local police to monitor social distancing. Israel has utilized the surveillance technologies of the Israel Security Agency (ISA) to trace patients and those with whom they came into contact during the period from mid-March 2020 to early June 2020. In response to a ruling by the Israeli Supreme Court requiring the ISA activities to be defined in legislation and public criticism over privacy concerns, the government announced on June 8, 2020, that it would no longer utilize ISA surveillance for tracing COVID-19 patients or promote relevant legislation in this regard unless a new outbreak takes place.

However, these electronic measures also raise privacy and data protection concerns, in particular as they relate to sensitive health data. Appropriate safeguards have to be put in place to ensure that the electronic measures are necessary and proportionate, such as consent, data minimization, privacy by design, transparency, nondiscrimination, security of data, deletion or anonymization of data once it is no longer necessary, and oversight mechanisms, among others. South Korea, for example, has been criticized for releasing a detailed log of movements of COVID-19 patients, including the time and names of places they visited, through the media and related websites. The European Data Protection Board has voiced concerns with regard to apps that use location tracking as they violate the principle of data minimization. In Australia, critics voiced concerns that United States law enforcement entities could gain access to the app data, because the data is being hosted in Australia by Amazon Web Services, a US company subject to the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Iceland's app, on the other hand, has received international recognition as one of the least invasive apps from a privacy perspective.

Some countries conducted rights impact assessments before the measures were deployed to ensure that individual rights would not be violated and to promote public acceptance, or had data protection agencies conduct an assessment after deployment. The French government sought advice from the independent National Commission on Information Technology and Freedoms (CNIL) twice before the introduction of the app. The Turkish Data Protection Authority released two guidance documents discussing privacy and data protection concerns with regard to electronic measures to fight the COVID-19 outbreak. In Australia, the Department of Health engaged a law firm to prepare a Privacy Impact Assessment (PIA) to advise the Department on how it needed to address and mitigate any identified privacy risks with regard to the COVIDSafe app. The PIA was published online. The Norwegian supervisory authority for the collection and use of personal data started an investigation after the introduction of the app to ensure that it complies with the Norwegian regulation on tracing and epidemic contagion related to COVID-19.

The map below shows which jurisdictions have adopted COVID-19 contact tracing apps and the technologies they use.

# COVID-19 Contact Tracing Apps in Selected Jurisdictions



**Note:** This map does not cover other COVID-19 apps that use GPS/geolocation. The European Union recommends contact tracing apps that use Bluetooth, however not all member countries utilize these.

**Source:** Prepared by Susan Taylor, Law Library of Congress. Map reflects results of jurisdictional surveys in this report.

## *The Americas*

# Argentina

Graciela Rodriguez-Ferrand  
Senior Foreign Law Specialist

**SUMMARY** Argentina declared a state of health emergency due to COVID-19 on March 12, 2020, and adopted a mandatory lockdown. The law on data privacy governs the management of health information under the health emergency. The Ministry of Health has launched the CuidAR COVID-19 free application for mobile phones, for self-diagnosis and health care guidance. It is also used to process the Unique Circulation Enabling Certificate, which allows certain people to circulate amid the lockdown. It is also used to track the spread of the virus through geo-localization. Its use is not mandatory, except for travelers entering the country and those exempted from the lockdown and returning to work.

## I. Introduction

Argentina declared a state of health emergency due to the COVID-19 epidemic for one year through the Decree of Necessity and Urgency [DECNU] 260/2020 starting on March 12, 2020.<sup>1</sup> It further mandated a lockdown through DECNU 297/2020, until March 31, 2020, which was extended until May 24, 2020.<sup>2</sup> The lockdown was to remain in place in Buenos Aires through at least June 7.<sup>3</sup>

There were 9,931 Covid-19 cases in Argentina as of May 22, 2020, and 419 deaths, according to the report from the government, which is updated daily.<sup>4</sup> This information is available in a New COVID-19 dedicated section in the Ministry of Health website, where all information, recommendations, FAQs, etc., are available.<sup>5</sup>

Of a population of almost 45 million,<sup>6</sup> there are approximately 40 million mobile phone users in Argentina, and 1.3 million users have already downloaded and used the government app CuidAR COVID-19, which is managed by the Ministry of Health and aimed at the protection and

---

<sup>1</sup> Decreto de Necesidad y Urgencia (DECNU) 260/2020, art. 1, Mar. 12, 2020, Boletín Oficial [B.O.] 34327, <https://perma.cc/2VEH-G6SF>.

<sup>2</sup> DECNU 297/2020 Aislamiento Social Preventivo y Obligatorio, Mar. 19, 2020, B.O. 34334, <https://perma.cc/9QFN-CJ68>, and DECNU 459/2020 Extensión, May 11, 2020, B.O. 34377, <https://perma.cc/8KB6-GNLA>.

<sup>3</sup> DECNU 493/2020 Aislamiento Social Preventivo y Obligatorio Extensión, B.O. May 25, 2020, <https://perma.cc/Q3AX-6TVC>.

<sup>4</sup> Ministerio de Salud, *Informe Diario Coronavirus* (May 22, 2020), <https://perma.cc/68DY-5GQQ>.

<sup>5</sup> *Covid-19 Information*, Ministerio de Salud, <https://perma.cc/BU7D-6SGQ>.

<sup>6</sup> Population, Argentina, World Bank, 2019, <https://perma.cc/2ZFT-ATYD>.

care of citizens against the COVID-19 pandemic.<sup>7</sup> No survey results on Argentinians' willingness to share personal data were located.

## II. Legal Framework

### A. Privacy and Data Protection

The Agency for Access to Public Information (AAIP) has issued an statement on the treatment of health-related private information under the current health emergency, which must be carried out in compliance with data privacy rules under Ley 25326 de Protección de Datos Personales (LPDP).<sup>8</sup>

The fundamental principles of the LPDP applicable to personal health data are as follows:

- Health data are considered sensitive and therefore warrant more rigorous protection.<sup>9</sup>
- The disclosure of the identity of a Covid-19 patient requires his or her consent.<sup>10</sup>
- Health care facilities and professionals can process and transfer patient data to each other only under professional confidentiality standards.<sup>11</sup>
- Professional confidentiality will remain effective even after the relationship with the patient has ended.<sup>12</sup>
- To use patient information for purposes other than his or her medical treatment, the patient must give a full, free and informed consent.<sup>13</sup>
- The National and Provincial Ministries of Health have the authority to request, collect, and transfer to each other or, in any other way, process health information without the patient's consent, in accordance with their explicit and implicit competences assigned by law.<sup>14</sup>

---

<sup>7</sup> *Cómo Funciona CuidAR, la Nueva App de Coronavirus Argentina*, Ambito (May 11, 2020), <https://perma.cc/H3UJ-4VNP>.

<sup>8</sup> Ley 25326 de Protección de Datos Personales, Nov. 2, 2000, B.O. 29517, <https://perma.cc/NE2W-72LH>, and *Tratamiento de Datos Personales ante el Coronavirus*, AAIP (Mar. 11, 2020), <https://perma.cc/SB6R-DQZ5>.

<sup>9</sup> Ley 25326 arts. 2 & 7.

<sup>10</sup> Id. art. 5.

<sup>11</sup> Id. art. 8.

<sup>12</sup> Id. art. 10.

<sup>13</sup> Id. arts. 4.3 and 5.

<sup>14</sup> Id. arts. 5.2 and 11.3.b.

- Any person who considers that his or her privacy or personal data is being affected has the right to file a complaint with the AAIP.<sup>15</sup>

## **B. Location Tracking**

Under DECNU 260/2020, the Ministry of Health is empowered to adopt all recommendations and measures necessary to mitigate the health impact of the COVID-19 epidemic.<sup>16</sup> It further provides that the Ministry of Health is required to provide information to the public about the epidemic, regarding the spread, containment, and mitigation of the virus, while always keeping affected people's identity confidential and complying with professional secrecy standards.<sup>17</sup>

The public health measures taken within the authority granted under DECNU 260/2020 have to be the least restrictive of rights as possible and should be based on acceptable scientific criteria.<sup>18</sup> People affected by these measures will be guaranteed their rights, especially the right to be informed about their health status, the right to nondiscrimination in access to health care, and the right to dignified treatment.<sup>19</sup>

Violations of measures adopted under the health emergency are subject to applicable administrative sanctions or to criminal penalties provided under the Penal Code, such as imprisonment for six months to two years.<sup>20</sup>

## **III. Electronic Measures to Fight COVID-19 Spread**

The Ministry of Health has launched the CuidAR COVID-19 free app, available on iOS and Android systems.<sup>21</sup> On its first day of operation, it had more than 100,000 users, and 500,000 auto tests were carried out.<sup>22</sup>

This app allows people to diagnose themselves through a platform and then receive recommendations on the steps to follow if they have symptoms that coincide with the coronavirus and information on care and prevention.<sup>23</sup> The new app enables a user to check

---

<sup>15</sup> Id.

<sup>16</sup> DNU 260/2020 art. 2, paras 1 & 16; art. 20.

<sup>17</sup> Id. art. 3.

<sup>18</sup> Id. art. 21.

<sup>19</sup> Id.

<sup>20</sup> Id. art. 22 and Código Penal art. 205, Nov. 3, 1921, B.O. 8300, <https://perma.cc/J3BJ-PPAJ>.

<sup>21</sup> COVID-19, Ministerio de Salud, <https://perma.cc/34XX-C5FS>.

<sup>22</sup> Martín Torino, *Coronavirus: La App para Detectar Síntomas Sumó 500,000 Autotests en su Primer Día*, Cronista (Mar. 24, 2020), <https://perma.cc/EJV5-P4SE>.

<sup>23</sup> *Cómo Funciona CuidAr la Nueva App de Coronavirus Argentina*, Ambito (May 11, 2020), <https://perma.cc/FM2A-CNYL>.

symptoms related to the disease without the need to leave home, avoiding the need to go to a medical center and potentially spread the virus, thus easing the strain on the health care system.<sup>24</sup>

The CuidAr-COVID-19 app requires the user to enter his or her personal data and mobile number and share their geo-location. In addition, the address, locality and province where the person is undergoing quarantine must be declared, to enable the health emergency protocol to be activated if necessary.<sup>25</sup>

To perform the self-diagnosis, the user must answer questions about his or her body temperature, other symptoms, and preexisting diseases.<sup>26</sup>

The app also provides access to the Unique Circulation Enabling Certificate, which allows its holder to circulate when meeting the requirements for the exceptions to the circulation restrictions issued by the government during the health emergency.<sup>27</sup>

The app includes a special section on the use of personal data in its terms and conditions, where the user has the option to give consent to the release of personal health data. The information provided is protected by law and is for the exclusive use of the health authorities.<sup>28</sup>

For people who enter the country from abroad, the use of the app is mandatory for a period of 14 days, according to Disposición 1771/2020 of the Dirección Nacional de Migraciones [DNM].<sup>29</sup> In the case of minors or people with disabilities, the father, mother or legal representative will have to complete the required data on their behalf.<sup>30</sup>

The DNM has the authority to require travelers prior to entering the country and travelers who return from abroad to comply by downloading the app or entering the information requested on the app website, which informs its users about the terms and conditions for its use.<sup>31</sup>

Once downloaded, Decisión Administrativa 432/2020 requires the traveler to keep it installed and active for a minimum period of 14 calendar days from its activation.<sup>32</sup> This allows the DNM

---

<sup>24</sup> Id.

<sup>25</sup> Id.

<sup>26</sup> Id.

<sup>27</sup> Id.

<sup>28</sup> Id.

<sup>29</sup> Disposición 1771/2020, Aplicación COVID-19 – Ministerio de Salud. Obligatoriedad de Uso para Toda Persona que Ingrese al País, Dirección Nacional de Migraciones, Mar. 26, 2020, B.O. 34339, <https://perma.cc/P6YT-UMTW>.

<sup>30</sup> Decisión Administrativa 432/2020, Aplicación Covid-19 – Ministerio de Salud, art. 2, Mar. 24, 2020, B.O. 34337, <https://perma.cc/XKK4-YUKW>.

<sup>31</sup> Id. art. 3.

<sup>32</sup> Id. art. 6.

to collect the data related to COVID-19 through the app, taking into consideration data privacy protections under Ley 25326.<sup>33</sup>

The measure provides the technological tools required by the Ministry of Health in the identification, monitoring, and control of potential COVID-19 infection cases.<sup>34</sup>

The use of the app will also be mandatory for those who return to work.<sup>35</sup> Using the app for the Unique Circulation Enabling Certificate will automatically grant its holder permission to circulate during the quarantine.<sup>36</sup> This will be valid exclusively for those whose work falls within the exceptions of quarantine according to the latest official announcements.<sup>37</sup>

The app drew some criticism because of concerns that the government may be able to geo-locate people all the time through the GPS of cell phones with the app, with the potential of turning it into a tool of social control.<sup>38</sup>

In response to these concerns, the government indicated it would change the app to remove the possibility of tracking the user at all times, but rather only sending the location data when using the app. Government officials stated that this change would become effective mid-May.<sup>39</sup>

The Ministry of Health also created the Database COVID-19 in order to centralize the information collected on the national epidemiological situation, optimize health policies, and enhance the operational quality of the CuidAR COVID-19 app.<sup>40</sup>

The database will allow the information collected from the app to be stored and centralized both in its versions for Android or iOS mobile devices and in its web version.<sup>41</sup> In compliance with the requirements of the LPDP, the creation of the database must state the specific purpose of the collected data, the persons whose data will be collected, whether the information released is optional or compulsory, the means for obtaining and updating the data, the structure of the file, a description of the nature of the personal data included, the data-sharing entities, the authorities responsible for the archive, and a statement as to the authority in charge of claims pertaining to

---

<sup>33</sup> Id. art. 7.

<sup>34</sup> *Coronavirus: App para Autodetectar Síntomas Será Obligatoria para los que Lleguen del Exterior*, Cronista (Mar. 24, 2020), <https://perma.cc/5NMW-L4YF>.

<sup>35</sup> *Cómo Funciona la App CuidAR, de Uso Obligatorio para Quienes Vuelven al Trabajo Durante la Cuarentena*, Nación (May 11, 2020), <https://perma.cc/L8LB-9TMQ>.

<sup>36</sup> Id.

<sup>37</sup> Id.

<sup>38</sup> *Control Social Coronavirus en Argentina: El Gobierno Analiza Cambios en la App CuidAR, para Limitar el Monitoreo de la Gente*, Clarín (May 11, 2020), <https://perma.cc/ZK4V-8NU3>.

<sup>39</sup> Id.

<sup>40</sup> *Disposición 3/2020, Jefatura de Gabinete de Ministros, art. 1, May 5, 2020, B.O. 34374*, <https://perma.cc/8JEY-NFZX>.

<sup>41</sup> Id.

the individual rights of access, correction or deletion.<sup>42</sup> Authorities will also have to specify how they plan to delete the automated registries and the measures that will be adopted for their destruction.<sup>43</sup>

---

<sup>42</sup> Id. and LPDP art. 22.

<sup>43</sup> Id.

# Brazil

*Eduardo Soares*  
*Senior Foreign Law Specialist*

**SUMMARY** As of February 2020, Brazil had over 227 million active cell phones and a population of 210 million people. A new law, which will enter into force in August 2020, has been enacted for the purpose of protecting personal data.

In an effort to help track the spread of COVID-19, the government enacted a Provisional Measure for data sharing by telecommunications companies to support the generation of official statistics. However, the Brazilian Federal Supreme Court later issued an injunction suspending the Provisional Measure as a preliminary response to several Direct Unconstitutionality Actions that were filed by different entities.

The federal government has also issued a law specifying measures that may be adopted by the authorities within the scope of their competences to address the public health emergency resulting from the COVID-19 outbreak.

## I. Introduction

On May 22, 2020, Brazil's Ministry of Health registered 310,987 confirmed cases of COVID-19 and 20,047 deaths in the country.<sup>1</sup> According to the National Agency of Telecommunications (Agência Nacional de Telecomunicações, ANATEL), in February 2020 Brazilians had 227.1 million active cell phones.<sup>2</sup>

## II. Legal Framework

### A. Privacy and Data Protection

On August 14, 2018, Brazil enacted Law No. 13,709, the General Data Protection Law (Lei Geral de Proteção de Dados), which provides for the processing of personal data, including digital media, by either a natural person or a public or private legal entity in a manner that protects a person's fundamental rights of freedom, privacy, and free development of personality.<sup>3</sup> The new law will enter into force in August 2020.<sup>4</sup>

---

<sup>1</sup> *Coronavírus Brasil*, Ministério da Saúde, <https://covid.saude.gov.br/>.

<sup>2</sup> Agência Nacional de Telecomunicações, <https://www.anatel.gov.br/paineis/ acessos/ telefonia-movel>. For comparison purposes, on July 1, 2019, the Brazilian population was estimated to be approximately 210.15 million persons. *Estimativa da população do Brasil Passa de 210 Milhões*, Agência Brasil (Aug. 28, 2019), <https://perma.cc/QJ4G-7TWD>.

<sup>3</sup> Lei No. 13,709, de 14 de Agosto de 2018, art. 1, <https://perma.cc/JY54-JZQL>.

<sup>4</sup> Id. art. 65(II).

The law regulates the protection of personal data<sup>5</sup> and applies to any processing operation carried out by a natural person or a legal entity under public or private law, regardless of the medium, the country of the entity's headquarters, or the country where the data is located.<sup>6</sup> The law also sets forth exceptions to its application<sup>7</sup> and the principles that need to be observed when processing personal data.<sup>8</sup>

The law defines how the processing of personal data is to be carried out, including, but not limited to, with the consent of the person; in compliance with the controller's legal and regulatory obligations; and for the protection of health in a procedure exclusively performed by health professionals, health services, or the health authority.<sup>9</sup> It also establishes how the processing of sensitive personal data is to occur.<sup>10</sup>

## **B. Data Retention and Location Tracking**

### *1. Provisional Measure No. 954 of April 20, 2020*

On April 17, 2020, Brazilian President Jair Bolsonaro enacted Provisional Measure<sup>11</sup> No. 954, which provides for data sharing between telecommunications companies that offer Fixed Switched Telephone Services (Serviço Telefônico Fixo Comutado, STFC) and Personal Mobile Services (Serviço Móvel Pessoal, SMP) and the Brazilian Institute of Geography and Statistics Foundation (Fundação Instituto Brasileiro de Geografia e Estatística, IBGE), for the purpose of supporting the generation of official statistics during the COVID-19 public health emergency,<sup>12</sup> which Law No. 13,979, of February 6, 2020, deals with.<sup>13</sup>

Telecommunication companies providing STFC and SMP must make available to the IBGE, in electronic form, a list of names, telephone numbers, and addresses of their consumers, whether individual persons or companies.<sup>14</sup> The data will be used directly and exclusively by the IBGE for

---

<sup>5</sup> Id. art. 2.

<sup>6</sup> Id. art. 3.

<sup>7</sup> Id. art. 4.

<sup>8</sup> Id. art. 6.

<sup>9</sup> Id. art. 7(I), (II), (VIII).

<sup>10</sup> Id. art. 11.

<sup>11</sup> Article 62 of the Brazilian Constitution determines that in relevant and urgent cases, the President of the Republic may adopt provisional measures that have the force of law. Such measures must be submitted immediately to the National Congress. Constituição Federal, art. 62, <https://perma.cc/B596-Q5UP>.

<sup>12</sup> Medida Provisória [MP] No. 954, de 17 de Abril de 2020, art. 1, <https://perma.cc/HTG3-JTSQ>.

<sup>13</sup> Lei No. 13.979, de 6 de Fevereiro de 2020, <https://perma.cc/PW22-WBL9>. Law No. 13,979 provides for the measures that may be adopted to face the public health emergency of international importance resulting from the COVID-19 outbreak.

<sup>14</sup> MP No. 954, art. 2.

generating official statistics, with the objective of conducting household surveys in a non-face-to-face manner.<sup>15</sup>

The shared data will be confidential; will be used exclusively for generating official statistics; will not be used as a certificate or evidence in administrative, fiscal, or judicial proceedings, under the terms of Law No. 5,534, which establishes the obligation to provide statistical information.<sup>16</sup>

The IBGE is prohibited from making the data available to any public or private companies or bodies, or to entities of the public administration of any of the federative entities.<sup>17</sup> The IBGE will provide information on its website concerning the situations in which the data have been used and will release an impact report on the protection of personal data, under the terms of Law No. 13,709.<sup>18</sup> Once the public health emergency resulting from COVID-19 has been overcome, pursuant to the provisions of Law No. 13,979 of 2020, the information shared must be deleted from the databases of the IBGE.<sup>19</sup>

## 2. Database and Tracking Systems

On April 12, 2020, a Brazilian newspaper reported that a group of telephone companies were planning to make a large database available to the Ministry of Science, Technology, Innovations and Communications based on information from their transmission towers, which could identify the movement of people.<sup>20</sup> A similar project has also been implemented in the State of São Paulo.<sup>21</sup> In addition to large corporations like Google and Facebook who are also developing similar tracking projects, the Brazilian startup InLoco has created a map of social isolation in the country<sup>22</sup> divided by states, the newspaper reported.<sup>23</sup>

According to the website of the startup, the social isolation index was developed to combat the COVID-19 pandemic. The map shows the percentage of the population that is respecting the isolation recommendation. The purpose of the map is to assist authorities in directing the application of public security, communication, and health resources to the appropriate areas.<sup>24</sup>

---

<sup>15</sup> Id. art. 2(§ 1).

<sup>16</sup> Id. art. 3.

<sup>17</sup> Id. art. 3(§ 1).

<sup>18</sup> Id. art. 3(§ 2).

<sup>19</sup> Id. art. 4.

<sup>20</sup> *Uso de Dados de Localização no Combate à COVID-19 Pode Ameaçar Privacidade*, Estadão, Link (Apr. 12, 2020), <https://perma.cc/87Y2-TNKQ>.

<sup>21</sup> Id.

<sup>22</sup> Id.

<sup>23</sup> *Mapa Brasileiro da COVID-19*, InLoco, <https://perma.cc/J6RZ-6M9P> (click “See the Screenshot View”).

<sup>24</sup> Id.

Furthermore, the newspaper stated that the telephone companies will use the data in an aggregate manner, which means that governments would not have access to individualized information, but only compiled data to indicate major trends.<sup>25</sup> At the end of the pandemic emergency the database will cease to be used, but during the emergency the information will be stored on a publicly owned server. The government will decide what will be done with the data and with what institutions to share it with.

### III. Electronic Measures to Fight COVID-19 Spread

#### A. Dedicated Coronavirus App to Stop Spread of the Virus

On March 2, 2020, the Ministry of Health launched the Coronavirus-SUS app for the purpose of making the population aware of COVID-19. The app provides information on various topics such as symptoms, how to prevent infection, what to do in the case of suspected or actual infection, and other relevant information. It also provides a map indicating the location of nearby health units.<sup>26</sup>

#### B. Compatibility of Measures with Privacy Rights/Data Protection Principles

##### 1. Federal Supreme Court Injunction

On April 24, 2020, Justice Rosa Weber of the Federal Supreme Court (Supremo Tribunal Federal, STF) granted an injunction (*medida cautelar*) suspending Provisional Measure No. 954, as requested in five Direct Unconstitutionality Actions (Ação Direta de Inconstitucionalidade, ADI) proposed by the Federal Council of the Brazilian Bar Association (ADI 6387) and four different political parties (ADIs 6388, 6389, 6390, and 6393).<sup>27</sup> In the preliminary analysis of the actions, Justice Weber pointed out that

the information under [Provisional Measure No.] 954 is within the scope of constitutional protection (article 5 of the Constitution), which supports the right to personal intimacy, private life, honor and reputation of people. . . . [T]he MP does not foresee any requirement of mechanisms and procedures to ensure the confidentiality and anonymity of the shared data, which does not meet the requirements established in the Constitution for the effective protection of fundamental rights of Brazilians.<sup>28</sup>

Justice Weber also highlighted that there is no legitimate public interest in sharing the personal data of users of telephone services and that the standard does not provide conditions for assessing their suitability and need, as it does not define the form or purpose of the use of the data collected, in apparent violation of the law. She further added that the seriousness and urgency resulting from the current health crisis cannot be underestimated, nor the need to formulate public policies that demand

---

<sup>25</sup> Id.

<sup>26</sup> *Coronavirus – SUS*, Governo do Brasil, <https://perma.cc/A9SM-JDFS>.

<sup>27</sup> *Ministra suspende MP que prevê compartilhamento de dados com o IBGE por empresas de telecomunicações durante pandemia*, Notícias STF (Apr. 24, 2020), <https://perma.cc/R5LU-KQU3>.

<sup>28</sup> Id. (translation by author).

specific data to face the COVID-19 outbreak. However, she stated that the fight against the pandemic cannot legitimize “the trampling of fundamental guarantees enshrined in the Constitution.”<sup>29</sup>

Under these arguments, Justice Weber granted the injunction “in order to prevent irreparable damage to the intimacy and confidentiality of the privacy of more than one hundred million users of fixed and mobile telephone services,” and determined that the IBGE must refrain from requesting the data provided for in Provisional Measure No. 954. If the information has already been requested, the request must be suspended, with immediate communication to the telephone companies, she said.

Justice Weber’s decision will be submitted to the plenary of the STF for analysis and confirmation.<sup>30</sup>

## 2. *Use of Geolocation Halted*

Under the justification that privacy risks need to be better evaluated, President Jair Bolsonaro determined that the Ministry of Science, Technology, Innovations and Communications should halt negotiations with telephone companies concerning the use by the federal government of aggregated and anonymous geolocation information from several citizens. The information had been sought as a means to monitor what percentage of people in a given region are following the government’s guidance to stay at home as much as possible.<sup>31</sup>

## C. Consequences for People Who Have Been in Close Contact with Infected Persons

Law No. 13,979 provides that the authorities may adopt, within the scope of their competences, the following measures to address the COVID-19 outbreak:

- I - isolation;
- II - quarantine;
- III - determination of compulsory:
  - a) medical examinations;
  - b) laboratory tests;
  - c) collection of clinical samples;
  - d) vaccination and other prophylactic measures; or
  - e) specific medical treatments.<sup>32</sup>

For the purposes of Law No. 13, 979, “isolation” is defined as the separation from others of sick or contaminated persons, or of luggage, means of transportation, goods, or affected postal parcels, in order to avoid contamination or the spread of the coronavirus. “Quarantine” is defined

---

<sup>29</sup> Id.

<sup>30</sup> Id.

<sup>31</sup> Mariana Schreiber, *Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?*, BBC News Brasil (Apr. 21, 2020), <https://perma.cc/KAB9-7QNU>.

<sup>32</sup> Lei No. 13.979 of February 6, 2020, art. 3, <https://perma.cc/HT6U-7RSA> (translation by author).

as the restriction of activities or separation of persons suspected of contamination from persons who are not sick, or the separation of luggage, containers, animals, means of transportation, or goods suspected of being contaminated, in order to avoid possible contamination or the spread of the coronavirus.<sup>33</sup>

People must comply with these measures and a failure to comply will result in liability, as provided by law.<sup>34</sup>

---

<sup>33</sup> Id. art. 2.

<sup>34</sup> Id. art. 3(§ 4).

# Mexico

*Gustavo Guerra*  
*Senior Foreign Law Specialist*

**SUMMARY** As of May 22, 2020, mandatory electronic measures to combat COVID-19, such as location tracking of, and contact tracing through, mobile devices, had not been ordered by Mexico's federal government. The government has released a voluntary mobile coronavirus application, "Covid-19MX," aimed at assisting users to locate pertinent information on a number of matters related to the virus, including access to epidemiological health care telephone numbers and a self-diagnosis tool. Certain issues have been reported concerning the privacy policy of this app.

## I. Introduction

According to data provided by the Mexican government, there were 62,527 confirmed cases of individuals who contracted COVID-19 and 6,989 deaths from the virus as of May 22, 2020.<sup>1</sup> However, Mexican officials have reportedly acknowledged that the number of cases is perhaps several times higher due to Mexico's low rate of testing.<sup>2</sup> Mexico, which has a population of over 125 million, has conducted approximately 230,000 tests to date, one of the lowest rates in the Western Hemisphere.<sup>3</sup>

In 2019 there were approximately 86.5 millions of users of cellphones in the country, 90% of whom had a smartphone, according to a government survey.<sup>4</sup> The survey indicates that 48.3 million cell phone users installed apps on their devices in 2019.<sup>5</sup> Most of these apps were for social media, instant messaging, and traffic information.<sup>6</sup> The surveyed individuals did not report having downloaded applications for health purposes.<sup>7</sup>

---

<sup>1</sup> *Comunicado Técnico Diario COVID-19*, Gobierno de México, Secretaría de Salud (May 22, 2020), <https://perma.cc/PWQ2-WQNR>.

<sup>2</sup> *Mexico Hit New Virus Record of over 500 Deaths Per Day*, Associated Press (May 26, 2020), <https://perma.cc/64NB-B9WP?type=image>.

<sup>3</sup> *Id.*

<sup>4</sup> Press Release, Instituto Nacional de Estadística y Geografía et al., En México hay 80.6 millones de usuarios de internet y 86.5 millones de usuarios de teléfonos celulares: ENDUTIH 2019 (Feb. 17, 2020), <https://perma.cc/NNY9-35YH>.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

## II. Legal Framework

### A. Privacy and Data Protection

“Personal data” are defined as any information pertaining to an identified or identifiable individual.<sup>8</sup> An individual is deemed to be identifiable when his or her identity may be directly or indirectly determined from any information.<sup>9</sup>

“Sensitive personal data” are those that refer to the individual’s most private information and those whose misuse may lead to discrimination against, or involve a serious risk to, the data’s owner, including his or her health status.<sup>10</sup> The processing of personal data must adhere to the principles of consent, lawfulness, purpose, proportionality, and responsibility.<sup>11</sup>

As a general rule, sensitive data may be processed provided that express consent is granted for such purpose.<sup>12</sup> There are a number of exceptions to this rule, however, including cases where personal data are needed to provide preventive treatment or diagnosis when providing health care, and when the data have been subject to a prior disaggregation procedure.<sup>13</sup> Through such procedure, personal data cannot be associated with the owner.<sup>14</sup>

In the absence of these exceptions, consent must be specifically granted and based on the privacy policy provided by the recipient of the data.<sup>15</sup> The privacy policy must inform individuals, in clear terms, of the existence and main characteristics of the processing to which their personal data will be subjected so that they can make informed decisions.<sup>16</sup>

### B. Data Retention and Location Tracking

#### 1. Health Law

Mexico’s health authorities have broad powers to prevent and control communicable diseases, including observation of human and animal contacts, to the extent required.<sup>17</sup> In places where a communicable disease acquires serious epidemic characteristics as determined by the

---

<sup>8</sup> Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados art. 3-IX, Diario Oficial de la Federación [DOF], Jan. 26, 2017, as originally enacted, <https://perma.cc/R9EX-757C>.

<sup>9</sup> Id.

<sup>10</sup> Id. art. 3-X.

<sup>11</sup> Id. art. 16.

<sup>12</sup> Id. art. 7.

<sup>13</sup> Id. art. 22(VII), (IX).

<sup>14</sup> Id. art. 3(XIII), (XXXI).

<sup>15</sup> Id. art. 20.

<sup>16</sup> Id. art. 26.

<sup>17</sup> Ley General de Salud arts. 134-XIV, 139-III, DOF, Feb. 7, 1984, as amended, <https://perma.cc/A744-J9NZ>.

Department of Health, as well as in adjoining places, private citizens and civil and military authorities must cooperate with health authorities in combatting such disease.<sup>18</sup>

## 2. *Telecommunications Law*

In addition, telecommunications companies must cooperate with law enforcement authorities in locating, in real time, mobile communications devices.<sup>19</sup> Furthermore, these companies must keep records of communications that are made from any type of line that allows for the accurate identification of pertinent data, including the following:

- Subscriber's name or corporate name and address
- Type of communication (voice, voicemail, conferencing, data)
- Multimedia or messaging services employed (including short message services, multimedia, and advanced services)
- Information needed to trace and identify the source and destination of the mobile telephone, including the destination number
- Date, time, and duration of communications, as well as the messaging or multimedia services involved
- Digital location of the geographic positioning of telephone lines<sup>20</sup>

The data retention obligation begins on the date on which the communication took place.<sup>21</sup> For the first 12 months telecommunications companies must store these data on systems that allow their delivery in real time to law enforcement authorities through electronic means.<sup>22</sup> Once this period is over, data must be retained in electronic storage systems for an additional 12 months, during which information must be delivered to the competent authorities within 48 hours from the time a pertinent request for such data is made.<sup>23</sup>

Telecommunications companies must take the necessary technical measures concerning the data being kept to guarantee their conservation, care, protection, and nonmanipulation, and must prevent unlawful access, destruction, alteration, or cancellation.<sup>24</sup>

---

<sup>18</sup> Id. arts. 140, 141, 147.

<sup>19</sup> Ley Federal de Telecomunicaciones y Radiodifusión art. 190-I, DOF, July 14, 2014, as amended, <https://perma.cc/SAY4-JHC8>.

<sup>20</sup> Id. art. 190-II.

<sup>21</sup> Id.

<sup>22</sup> Id.

<sup>23</sup> Id.

<sup>24</sup> Id.

### III. Electronic Measures to Fight COVID-19 Spread

As of May 22, 2020, mandatory electronic measures to combat COVID-19, such as location tracking of, and contact tracing through, mobile devices, had not been ordered by Mexico's federal government.<sup>25</sup> A high-ranking official with the National Institute for Access to Information (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI), Mexico's main authority on privacy matters, recently indicated that if the government decides to conduct geolocation tracking measures through electronic means, it should do so in consultation with INAI to ensure that private data are treated in accordance with applicable privacy requirements.<sup>26</sup>

The Mexican government has released a voluntary mobile coronavirus app, called "Covid-19MX," aimed at assisting users in locating the following information related to the virus:

- Direct access to epidemiological health care telephone numbers.
- Self-diagnosis: In case of suspicion that the user or a family member have contracted the virus, the app offers a questionnaire to obtain pertinent recommendations, depending on the data provided.
- Locations of healthcare providers close to the user's location, provided that geolocation permission is activated.
- Relevant information to understand how COVID-19 is transmitted, the most vulnerable groups and prevention measures.
- News: Access to official information, including press conferences and statements from Mexico's Ministry of Health.<sup>27</sup>

Socialtic, a nonprofit organization specialized in technology matters, reviewed this app in April 2020 and criticized its privacy policy, as it contains the following information:

- It indicates that personal data may be provided to third parties, but does not specify with whom and for what purposes.
- It omits the data that the app collects from the phone and other programs to which permissions are granted.

---

<sup>25</sup> *Se Declara como Emergencia Sanitaria la Epidemia Generada por Covid-19*, Gobierno de México, <https://perma.cc/7VPP-B748>.

<sup>26</sup> Press Release, INAI, Ante pandemia, la salud pública es bien prioritario, pero no se puede descuidar la privacidad de las personas: Acuña Llamas (Apr. 30, 2020), <https://perma.cc/CXE2-JNX5>.

<sup>27</sup> *Descarga la app Covid-19*, Gobierno de México, <https://perma.cc/NRJ7-RMYM>; see also *Covid-19*, Google Play, <https://perma.cc/BVJ7-C9YD>.

- It reserves the right to make any update to the privacy notice without prior notice.
- It indicates that the Ministry of Health is not responsible for the use or misuse of the content of the application.<sup>28</sup>

---

<sup>28</sup> *Análisis de la App COVID-19MX – Resumen*, Socialtic (Apr. 6, 2020), <https://perma.cc/XGC9-JNVV>.

*East Asia, South Asia and Pacific*

# Australia

*Kelly Buchanan*  
*Foreign Law Specialist*

**SUMMARY** The Australian government launched the COVIDSafe mobile phone application on April 26, 2020. The app uses Bluetooth signals to record a user's contacts with other users and saves the encrypted information on their phone; it does not record location information. The contact data of a user who tests positive for COVID-19 can be uploaded to a central storage system and accessed by state and territory authorities as part of their contact tracing processes. The app is voluntary to download and users must grant permission for their data to be uploaded. The most recent figures available show that around 23% of Australians have downloaded the app.

The collection, use, and disclosure of personal information by various entities in Australia is primarily governed by the Privacy Act 1988 (Cth). This Act applies to federal government agencies and to entities with annual revenues over a certain threshold. In addition, most states and territories have privacy and health information laws that apply to state and territory government agencies and public-sector health service providers. The use and disclosure of telecommunications and related data by mobile phone carriers, including for purposes of law enforcement and national security, is governed by specific legislation. The laws include requirements to retain certain data about telecommunications and to provide assistance to relevant government entities, including in relation to encrypted information.

At the time of its launch, use of the COVIDSafe app and the data collected were subject to a privacy policy and a determination that set out various privacy protections and prohibited people or organizations from coercing others to download or use the app. On May 15, 2020, a bill that replicated and extended those rules and protections was enacted. The bill inserted a new part into the Privacy Act 1988 (Cth) that, for example, defines the data that is collected by the app; contains rules and offenses regarding access to and use of that data; provides for oversight, complaint processes, and reporting requirements related to the app; and sets out a process for determining the end of the data period, at which point data stored in the central system will be deleted.

The COVIDSafe legislation excludes the application of other Australian laws that might allow data to be accessed, including the telecommunications laws referred to above, meaning that the data collected by the app cannot be accessed by law enforcement or national security agencies. However, some commentators remain concerned that agencies in the United States may be able to gain access to the data pursuant to the CLOUD Act because the central storage system is hosted in Australia by Amazon Web Services, a US company. They argue that the reciprocal agreement currently being negotiated between Australia and the US should specifically exclude COVIDSafe app data.

## I. Introduction

The Commonwealth of Australia is a federation of six states. In addition, two mainland territories have been granted a limited right of self-government and are often treated in a similar way to states: the Australian Capital Territory and Northern Territory.<sup>1</sup> Under the country's constitutional structure and relevant laws, plans, and arrangements,<sup>2</sup> the states and territories have primary responsibility for a range of public health measures related to responding to the COVID-19 pandemic, including testing and contact tracing, physical distancing requirements, and travel restrictions between jurisdictions.<sup>3</sup> National coordination mechanisms involve the federal Department of Health and the Australian Health Protection Principal Committee (AHPPC), while federal government responsibilities include national border measures, acquisition and distribution of certain supplies, and the country's economic response to the pandemic.<sup>4</sup>

As of May 22, 2020, a total of 7,095 confirmed cases of COVID-19 had been reported in Australia, including 101 deaths.<sup>5</sup> The country's response to the pandemic has been recognized internationally for its ability to restrict the outbreak and resulting deaths,<sup>6</sup> with an infection rate of around 280 per million people and a fatality rate of four per million people.<sup>7</sup>

On April 26, 2020, the federal government launched a mobile phone application, COVIDSafe, that records contacts between individual users through the use of Bluetooth wireless signals.<sup>8</sup> The app is available nationwide for voluntary download on both iOS and Android operating systems and the data can be accessed by state and territory authorities to supplement existing contact tracing

---

<sup>1</sup> *State and Territory Government*, Australia.gov.au, <https://perma.cc/W6ZX-KPJJ>.

<sup>2</sup> See, e.g., Department of Health, *Australian Health Sector Emergency Response Plan for Novel Coronavirus (COVID-19)* (last updated Feb. 7, 2020), <https://perma.cc/PNA9-UAWW>; Australian Health Protection Principal Committee, *CDPLAN: Emergency Response Plan for Communicable Disease Incidents of National Significance* (Sept. 2016), <https://perma.cc/286R-VBG2>.

<sup>3</sup> See Australian Government Solicitor, *Australian Jurisdictions Responses to COVID-19* (May 11, 2020), <https://perma.cc/HK4C-732Y>.

<sup>4</sup> Id.; *Government Response to the COVID-19 Outbreak*, Department of Health, <https://perma.cc/H4YZ-ADR2>; Karen Elphick, *Australian COVID-19 Response Management Arrangements: A Quick Guide* (Parliamentary Library, Apr. 28, 2020), <https://perma.cc/LXV8-8XS7>; Karen Elphick, *Australian Pandemic Response Planning: A Quick Guide* (Parliamentary Library, Apr. 28, 2020), <https://perma.cc/3FWW-WULH>; Karen Elphick, *National Emergency and Disaster Response Arrangements in Australia: A Quick Guide* (Parliamentary Library, Apr. 28, 2020), <https://perma.cc/KB2X-9E94>.

<sup>5</sup> *Coronavirus (COVID-19) at a Glance*, Department of Health, <https://perma.cc/F6QN-PKZG>.

<sup>6</sup> See, e.g., Nectar Gan, *How Did Australia Flatten Its Coronavirus Curve? Restrictions Easing as Infection Rate Continues to Fall*, CNN (May 1, 2020), <https://perma.cc/7467-5L4V>.

<sup>7</sup> *COVID-19 Coronavirus Pandemic*, Worldometer, <https://perma.cc/HYH6-TU58>.

<sup>8</sup> Press Release, Prime Minister et al., *COVIDSafe: New App to Slow the Spread of Coronavirus* (Apr. 26, 2020), <https://perma.cc/H9QP-Q9L6>; *COVIDSafe App*, Department of Health, <https://perma.cc/ZMZ5-WVQJ>. See also Ariel Bogle, *Will the Government's Coronavirus App COVIDSafe Keep Your Data Secure? Here's What the Experts Say*, ABC News (Apr. 27, 2020), <https://perma.cc/SK46-RZ6J>.

processes.<sup>9</sup> The app was developed by the Digital Transformation Agency, which had made two updates to the app as of May 18, 2020.<sup>10</sup> On launching the app, the Prime Minister stated that “[t]he Chief Medical Officer’s advice is we need the COVIDSafe app as part of the plan to save lives and save livelihoods. The more people who download this important public health app, the safer they and their family will be, the safer their community will be and the sooner we can safely lift restrictions and get back to business and do the things we love.”<sup>11</sup>

Within just over 24 hours after the app was launched, two million Australians, or around 8% of the population, had downloaded the app.<sup>12</sup> On May 20, 2020, the Minister for Health stated that there had been 5.9 million downloads of the app,<sup>13</sup> which equates to around 23% of the total population. According to a national survey conducted by consulting company Deloitte in 2019, 91% of Australians have a smartphone device.<sup>14</sup>

At the time the app was first launched, the Minister for Health issued a determination containing certain rules and restrictions regarding the use of the collected data and prohibiting anyone from coercing others to download or use the app. Subsequently, on May 4, 2020, the government published draft legislation to replace and extend the rules in the determination.<sup>15</sup> The final bill was introduced in the federal Parliament on May 12, 2020. It was passed on May 14, 2020, and received assent on May 15, 2020.<sup>16</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The federal Privacy Act 1988 (Cth) applies to most federal government agencies and to private-sector organizations with an annual revenue of more than AU\$3 million.<sup>17</sup> The Act includes 13

---

<sup>9</sup> *COVIDSafe App*, Australian Government, <https://perma.cc/3VVM-DJPK>. See Josh Taylor, *Covidsafe App: How Australia’s Coronavirus Contact Tracing App Works, What It Does, Downloads and Problems*, *Guardian* (May 14, 2020), <https://perma.cc/24L6-ZKHX>; Gavin Smith et al., *COVIDSafe – What We Now Know*, Allens, Insight (Apr. 27, 2020), <https://perma.cc/Q8Y4-WA2P>.

<sup>10</sup> *The Next Release of COVIDSafe Is Live*, Digital Transformation Agency (May 14, 2020), <https://perma.cc/9MPR-G9YX>.

<sup>11</sup> Press Release, *supra* note 8.

<sup>12</sup> Justin Hendry, *COVIDSafe App Hits 2 Million Downloads in 24 Hours*, *iTNews* (Apr. 27, 2020), <https://perma.cc/8L35-4UW7>.

<sup>13</sup> Transcript, Minister for Health, Press Conference in Melbourne about COVID-19 (May 20, 2020), <https://perma.cc/DH3J-S384>.

<sup>14</sup> *Mobile Consumer Survey 2019*, Deloitte, <https://perma.cc/2FCM-5F6C>.

<sup>15</sup> See Paul Karp, *Government Releases Draft Legislation for Covidsafe Tracing App to Allay Privacy Concerns*, *Guardian* (May 4, 2020), <https://perma.cc/QV8Z-NWJ6>.

<sup>16</sup> See Justin Hendry, *COVIDSafe Privacy Protections Now Locked in Law*, *iTNews* (May 14, 2020), <https://perma.cc/5MLH-UNMT>.

<sup>17</sup> Privacy Act 1988 (Cth) s 6 (definitions of “agency” and “APP entity”), 6C & 6D, <https://perma.cc/B9X5-DT9F>; *The Privacy Act*, Office of the Australian Information Commissioner (OAIC), <https://perma.cc/3MKU-UYHF>.

Australian Privacy Principles (APPs), which govern standards, rights, and obligations related to the collection, use, and disclosure of personal information, among other matters.<sup>18</sup> For example, APP 6 requires that APP entities only use or disclose personal information for a purpose for which it was collected (“primary purpose”) and not for another purpose (“secondary purpose”), unless the individual has either consented to the secondary use or disclosure of the information or an exception applies.

Exceptions include, for example, where the secondary use or disclosure is authorized by or under an Australian law or court order,<sup>19</sup> where a “permitted general situation” exists (including where the use or disclosure is necessary to lessen or prevent a serious threat to life, health, or safety of any individual, or to public health and safety),<sup>20</sup> and where a “permitted health situation” exists (including where the use or disclosure is necessary for research relevant to public health or public safety, or for the compilation or analysis of statistics relevant to public health or safety).<sup>21</sup> The Act also contains additional specific provisions related to health information that apply to all private-sector health service providers in Australia.<sup>22</sup>

The government may declare a national emergency or disaster under the Privacy Act.<sup>23</sup> When such a declaration is in effect, an entity may collect, use, or disclose personal information relating to an individual involved in the emergency or disaster, where such dealing with the information is for a permitted purpose in relation to the emergency or disaster.<sup>24</sup> These provisions were most recently applied in early 2020 in the context of the Australian bushfires; no declaration has been made with respect to the COVID-19 pandemic.<sup>25</sup>

The Office of the Australian Information Commissioner (OAIC) is responsible for various privacy functions, including receiving complaints and investigating possible breaches of the Privacy Act.<sup>26</sup> Several other federal laws also relate to privacy, including the telecommunications laws discussed below.<sup>27</sup> In addition, most states and territories have privacy and health information laws that apply to state and territory government agencies and public-sector health service

---

<sup>18</sup> Privacy Act 1988 (Cth) sch 1; *Australian Privacy Principles*, OAIC, <https://perma.cc/38SF-FNGM>.

<sup>19</sup> Privacy Act 1988 (Cth) sch 1 APP 6.2(b).

<sup>20</sup> APP 6.2(c) & s 16A(1) item 1.

<sup>21</sup> APP 6.2(d) & s 16B(3). See Andrew McDonald & Tessie Tan, *Coronavirus Surveillance Tactics Raise Questions about Civil Liberties*, Thomson Reuters, Legal Insight (Apr. 7, 2020), <https://perma.cc/G6HH-C456>.

<sup>22</sup> Privacy Act 1988 (Cth) ss 6FA, 16FB, & 95A. See *What Is Health Information?*, OAIC, <https://perma.cc/88PP-RJ72>; *What Is a Health Service Provider*, OAIC, <https://perma.cc/9R44-J5AW>; *Privacy for Health Service Providers*, OAIC, <https://perma.cc/9UZN-SA58>.

<sup>23</sup> Privacy Act 1988 (Cth) s 80J.

<sup>24</sup> *Id.* s 80P.

<sup>25</sup> See *Emergency Declaration – Privacy Act 1988*, Attorney-General’s Department, <https://perma.cc/CW4U-LS3R>.

<sup>26</sup> *What We Do*, OAIC, <https://perma.cc/NL8C-RGQ9>.

<sup>27</sup> See *Other Legislation*, OAIC, <https://perma.cc/9EP6-FYGC>.

providers, and every jurisdiction has a dedicated commissioner or committee to handle complaints about privacy breaches.<sup>28</sup>

The OAIC has issued privacy guidance for public- and private-sector entities in relation to responding to the COVID-19 pandemic.<sup>29</sup> It has also convened a “National COVID-19 Privacy Team,” consisting of the Australian Privacy Commissioner and state and territory privacy regulators, “to respond to personal information handling proposals with national implications.”<sup>30</sup>

## **B. Data Retention and Location Tracking**

### *1. Use and Disclosure of Information under the Telecommunications Act 1997*

The Telecommunications Act 1997 (Cth) contains provisions related to the use and disclosure of personal information by “carriers” (entities holding a carrier license for the provision of the infrastructure on which carriage and content services are provided to the public) and “carriage service providers” (providers of phone and/or internet services to the public).<sup>31</sup> This specifically includes “location information” with respect to mobile phones and other mobile communications devices.<sup>32</sup>

Under the Act, the disclosure or use of protected information is allowed in limited circumstances, including where it is required or authorized under a warrant or by or under law,<sup>33</sup> where there are reasonable grounds for believing that disclosure or use of the information “is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person,”<sup>34</sup> and disclosure to an emergency management person “for a purpose connected with persons being alerted to an emergency or likely emergency.”<sup>35</sup> Disclosures in these circumstances are deemed to be authorized by the Privacy Act.<sup>36</sup>

The Act also requires that carriers and carriage service providers give authorities “such help as is reasonably necessary” for the purposes of enforcing the criminal law and laws imposing pecuniary penalties, protecting the public revenue, and safeguarding national security.<sup>37</sup>

---

<sup>28</sup> See *Privacy in Your State*, OAIC, <https://perma.cc/QGW7-AN69>.

<sup>29</sup> *Coronavirus (COVID-19): Understanding Your Privacy Obligations to Your Staff*, OAIC (Mar. 18, 2020), <https://perma.cc/C8DB-R4S4>.

<sup>30</sup> *COVID-19*, OAIC (May 5, 2020), <https://perma.cc/FBC5-E4GP>; *COVID-19 Response from Australian Privacy Regulators*, OAIC (Mar. 27, 2020), <https://perma.cc/QZX7-6D9G>.

<sup>31</sup> Telecommunications Act 1997 (Cth) ss 5, 7 (definition of “carrier” and “carriage service”) 56, 87 & pt 13, <https://perma.cc/8FTF-N723>.

<sup>32</sup> *Id.* s 275A.

<sup>33</sup> *Id.* s 280.

<sup>34</sup> *Id.* ss 287 & 300.

<sup>35</sup> *Id.* s 285A & pt 13 div 3B.

<sup>36</sup> *Id.* s 303B.

<sup>37</sup> *Id.* ss 311 & 313(3) & (4).

## 2. Access to Telecommunications for National Security or Law Enforcement Purposes

The Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act) sets out the rules and procedures that enable government agencies to lawfully intercept or access telecommunications and related data for national security or law enforcement purposes.<sup>38</sup> It includes provisions on, for example, warrants authorizing the Australian Security Intelligence Organisation (ASIO) to intercept communications;<sup>39</sup> emergency requests authorizing officers of a carrier to intercept communications where a person is dying or seriously injured;<sup>40</sup> warrants authorizing law enforcement agencies (including at the state level) to intercept communications;<sup>41</sup> dealing with intercepted information;<sup>42</sup> the preservation of stored communications held by a carrier; access to stored communications pursuant to warrants issued to ASIO and criminal law enforcement agencies; and permitted dealings with accessed information.<sup>43</sup>

## 3. Data Retention Requirements

The TIA Act includes data retention provisions under which telecommunications companies are required to “retain a particular set of telecommunications data for at least 2 years.”<sup>44</sup> The required data involves information about communications, such as when an email was sent and the relevant email addresses, rather than the content or substance of communications.<sup>45</sup> The Act specifically requires the retention of information regarding “[t]he location of equipment, or a line, used in connection with a communication.”<sup>46</sup> Service providers are required to protect the confidentiality of such information by encrypting it and protecting it from unauthorized interference or access.<sup>47</sup>

Enforcement agencies, including state and territory police, may access telecommunications data for criminal law enforcement purposes and for the enforcement of laws imposing a pecuniary

---

<sup>38</sup> Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act), <https://perma.cc/A6DP-PLQM>; *Lawful Access to Telecommunications: Telecommunications Interception and Surveillance*, Department of Home Affairs, <https://perma.cc/AT3F-SQJ8>.

<sup>39</sup> TIA Act pt 2-2.

<sup>40</sup> *Id.* pt 2-3.

<sup>41</sup> *Id.* pt 2-5.

<sup>42</sup> *Id.* pt 2-6.

<sup>43</sup> *Id.* ch 3.

<sup>44</sup> *Lawful Access to Telecommunications: Data Retention Obligations*, Department of Home Affairs, <https://perma.cc/J29H-27BD>; TIA Act pt 5-1A.

<sup>45</sup> TIA Act s 187AA; *Lawful Access to Telecommunications: Data Retention*, Department of Home Affairs, <https://perma.cc/TT7X-FZM9>.

<sup>46</sup> TIA Act s 187AA(1) item 6.

<sup>47</sup> *Id.* s 187BA.

penalty.<sup>48</sup> Service providers may also voluntarily disclose such data when reasonably necessary for the enforcement of criminal law.<sup>49</sup>

The OAIC “has a range of powers and obligations in regards to the administration” of both the Telecommunications Act and the TIA Act, including monitoring compliance with the record-keeping requirements related to disclosures of personal information and oversight of the handling of data collected under the data retention provisions.<sup>50</sup>

#### 4. Access to Encrypted Information

Following amendments passed in 2018,<sup>51</sup> the Telecommunications Act 1997 (Cth) and the TIA Act contain provisions that seek to address “law enforcement and intelligence agencies’ challenges with the evolution of the communications environment, including the growth of encrypted communication.”<sup>52</sup> These include provisions aimed at enhancing industry cooperation with the relevant agencies and enhancing agency computer access powers to “improve the ability of agencies to operate around encryption without undermining it.”<sup>53</sup> This includes provisions related to “technical assistance requests,” “technical assistance notices,” and “technical capability notices.”<sup>54</sup>

#### 5. Other Federal and State/Territory Surveillance Laws

Other federal laws relevant to the ability of government agencies to access information held by mobile carriers include the Surveillance Devices Act 2004 (Cth),<sup>55</sup> Australian Security Intelligence Organisation Act 1979 (Cth),<sup>56</sup> and Crimes Act 1914 (Cth).<sup>57</sup> There are also laws at the state and territory level related to the use of surveillance and listening devices, including “tracking” devices. According to one law firm, writing about the possible use of location data or apps in the context of the context of the COVID-19 pandemic,

---

<sup>48</sup> Id. pt 4-1 div 4 & s 110A.

<sup>49</sup> Id. s 177.

<sup>50</sup> *Telecommunications*, OAIC, <https://perma.cc/9M4W-ADNS>.

<sup>51</sup> *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), <https://perma.cc/5QES-5F98>.

<sup>52</sup> *Lawful Access to Telecommunications: Assistance and Access: Overview*, Department of Home Affairs, <https://perma.cc/G49R-UCX4>.

<sup>53</sup> *Lawful Access to Telecommunications: The Assistance and Access Act 2018*, Department of Home Affairs, <https://perma.cc/SBN5-HJWR>; *Telecommunications Act 1997* (Cth) pt 15.

<sup>54</sup> See *Telecommunications Act 1997* (Cth) s 317A.

<sup>55</sup> *Surveillance Devices Act 2004* (Cth), <https://perma.cc/6KPX-C3XD>.

<sup>56</sup> *Australian Security Intelligence Organisation Act 1979* (Cth) pt III div 2, <https://perma.cc/5YUL-UEBX>.

<sup>57</sup> *Crimes Act 1914* (Cth) pt IAA div 2,

[i]n general terms, surveillance legislation in NSW, NT, SA and WA prohibits the installation, use or maintenance of a tracking device to determine the geographical location of a person or thing without the express or implied consent of the person. The prohibitions are targeted at individuals and corporations and carry criminal penalties.

Mobile location data, which is collected by mobile carriers, operating systems and apps, would likely not fall within the scope of these prohibitions given the prohibitions are targeted at the installation, use or maintenance of a tracking device without a person's consent. Mobile phone users would likely have either expressly consented or be considered to have impliedly consented to the use of mobile location services, through use of specific location-based services (in apps or IoT devices) or through use of a mobile network.

Further still, the prohibitions in the relevant instruments are subject to a number of exceptions which vary from state to state and include the installation, use or maintenance in accordance with a law of the Commonwealth. There is scope in a number of Commonwealth Acts for the exercise of various powers to permit the disclosure of mobile location data, including under the Telecommunications Act 1997 (Cth) and the Biosecurity Act 2015 (Cth). . . .<sup>58</sup>

## 6. *Public Health and Disaster Legislation*

Legislation related to public health responses to epidemics or pandemics, including the Biosecurity Act 2015 (Cth),<sup>59</sup> the National Health Security Act 2007 (Cth),<sup>60</sup> and state and territory public health laws<sup>61</sup> and disaster or emergency laws,<sup>62</sup> do not appear to contain specific provisions on the use of mobile phone traffic and location data for the purposes of contact tracing or otherwise responding to a pandemic. However, the Biosecurity Act allows the federal health minister to make a determination requiring that various measures be taken by specified classes of persons in order to prevent a listed human disease from entering, emerging, establishing itself, or spreading within Australia.<sup>63</sup> Such measures include “requiring a behaviour or practice” and “requiring a specified person to provide a specified report or keep specified records.”<sup>64</sup> In addition, the Act provides that “an individual may be required by a human biosecurity control order to wear either or both specified clothing and equipment that is designed to prevent a

---

<sup>58</sup> Michael Caplan et al., *Location, Location, Location! – Data, Privacy and Coronavirus*, Gilbert + Tobin (Apr. 19, 2020), <https://perma.cc/H6EL-C86J>.

<sup>59</sup> Biosecurity Act 2015 (Cth), <https://perma.cc/VGT3-NXFW>.

<sup>60</sup> National Health Security Act 2007 (Cth), <https://perma.cc/VB2U-K639>.

<sup>61</sup> See *Links to State and Territory Public Health Legislation, the Biosecurity Act, and the National Health Security Act 2007*, Department of Health, <https://perma.cc/J2FJ-GHV2>.

<sup>62</sup> See Helen Portillo-Castro, *Emergency Management and Disaster Resilience: A Quick Guide*, Australian Parliamentary Library (July 16, 2019), <https://perma.cc/G28V-ATTE>; *Emergency Management*, Department of Home Affairs, <https://perma.cc/586E-R4YG>.

<sup>63</sup> Biosecurity Act 2015 (Cth) s 51(1).

<sup>64</sup> *Id.* s 51(2).

disease from emerging, establishing itself or spreading.”<sup>65</sup> It does not appear that these provisions have been utilized in implementing electronic measures in response to the COVID-19 pandemic.

A “human biosecurity emergency” declaration regarding “human coronavirus with pandemic potential” was made by the government on March 18, 2020.<sup>66</sup> The declaration “gives the Minister for Health expansive powers to issue directions and set requirements in order to combat the outbreak” and “is the first time these powers under the *Biosecurity Act* have been used.”<sup>67</sup>

Under the National Health Security Act, “the Australian government is authorised to exchange public health surveillance information (including personal information) between the states and territories and the World Health Organisation (WHO). State and territory governments are also responsible for collecting surveillance data to contribute to the national picture and to inform the jurisdictional public health response.”<sup>68</sup>

### III. Electronic Measures to Fight COVID-19 Spread

#### A. Use of Anonymized Location Data

According to news reports from early April 2020, Vodafone Australia had provided, on request, “the mobile phone location data of several million Australians in an anonymised and aggregated form to the federal and NSW [New South Wales] governments to monitor whether people are following social distancing restrictions amid the coronavirus pandemic.”<sup>69</sup> In addition, “governments, medical experts and the media have used location data from transport apps such as CityMapper, which shows how people move throughout cities like Sydney and Melbourne using public transport, in an attempt to determine whether people’s movement has reduced.”<sup>70</sup>

One law firm notes that, if sufficiently anonymized, “data about people movements may not qualify as personal information within the meaning of the Privacy Act.”<sup>71</sup> However, it further states that “overseas experience shows how readily geo-location data can be reverse processed to re-identify individuals.”<sup>72</sup>

---

<sup>65</sup> Id. s 88. See Letter, “I See You’re at Bondi Beach Not Self Isolating”: Using Mobile Phone Data to Manage Covid-19, Gilbert + Tobin, <https://perma.cc/QY3E-WHH3>.

<sup>66</sup> Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) Declaration 2020 (Cth), <https://perma.cc/7EXN-E4EP>.

<sup>67</sup> Howard Maclean & Karen Elphik, *COVID-19 Legislative Response – Human Biosecurity Emergency Declaration Explainer*, FlagPost, Parliamentary Library (Mar. 19, 2020), <https://perma.cc/Y473-TWXT>.

<sup>68</sup> McDonald & Tan, *supra* note 21.

<sup>69</sup> Ben Grubb, *Mobile Phone Location Data Used to Track Australians’ Movements During Coronavirus Crisis*, Sydney Morning Herald (Apr. 5, 2020), <https://perma.cc/KTL7-U449>; Isabelle Lane, *Privacy Fears as Governments Use Phone Data to Track Coronavirus Rule Breakers*, New Daily (Apr. 6, 2020), <https://perma.cc/8AD3-L5T4>.

<sup>70</sup> Grubb, *supra* note 69.

<sup>71</sup> Letter, *supra* note 65.

<sup>72</sup> Id.

An NSW government minister stated that NSW would “absolutely not” use telecommunications data to enforce isolation by checking on whether people were leaving their premises.<sup>73</sup>

## B. Use of Mobile Data in Contact Tracing

According to the news reports, South Australia’s health department had “used an Apple iPhone’s inbuilt location services in a bid to trace the historical movements of a couple diagnosed with coronavirus” in February.<sup>74</sup> A spokesperson for the department said that this involved unique circumstances, and that the couple had volunteered their phones to police who worked with the chief public health officer to analyze the data.<sup>75</sup>

Apart from this instance, it has been reported that no jurisdictions are using an individual’s mobile phone data for contact tracing purposes, with health departments relying mainly on questionnaires in their efforts to locate individuals with whom a person who tested positive for COVID-19 had interacted in the previous 14 days.<sup>76</sup>

In late March, it was reported that Victoria’s health department was to start using a cloud-based messaging platform, Whispir, to “regularly interact with those who have come into close contact with someone who has contracted COVID-19” and that the platform would “also be used to enforce self-isolation for Victorians who have confirmed cases of the virus.”<sup>77</sup> According to Whispir, “[r]ecipients will be required to respond to the communications issued by the DHHS ‘contact tracing’ team by answering a series of questions, including recent activities, health and quarantine status.”<sup>78</sup>

## C. Australian Government’s Coronavirus Information App

At the end of March 2020, the Australian government released the “Coronavirus Australia” app to provide users with “official information and advice” about the COVID-19 pandemic in Australia.<sup>79</sup> It includes a “symptom checker” feature that asks for a person’s gender, age, and confirmation of symptoms. There is also an “isolation registration” option through which a person provides their location, name, phone number, age, gender, number of people in their household, and date their isolation commenced.<sup>80</sup> The app reportedly includes a privacy policy

---

<sup>73</sup> Grubb, *supra* note 69.

<sup>74</sup> *Id.*

<sup>75</sup> *Id.*; Emily Olle, *Coronavirus Couple’s Movements to be Tracked by Phone: SA Health*, 7News (Feb. 4, 2020), <https://perma.cc/UVG3-PNCF>.

<sup>76</sup> Jessie Davies, *Why Australia Isn’t Using Mobile Data to Track People Potentially Infected with Coronavirus*, ABC News (Apr. 7, 2020), <https://perma.cc/8QVD-9FFU>.

<sup>77</sup> Justin Hendry, *Victoria Ramps Up COVID-19 Contact Tracing Using Whispir*, ITNews (Mar. 26, 2020), <https://perma.cc/EL83-NMZF>.

<sup>78</sup> *Id.*

<sup>79</sup> *Coronavirus Australia App*, Department of Health, <https://perma.cc/42GE-SSFD>.

<sup>80</sup> Katharine Kemp, *Opinion: Privacy and Health: COVID-19 Tracking Apps*, UNSW Newsroom (Apr. 15, 2020), <https://perma.cc/SU7F-AFH2>.

related to the isolation registration option, which states that “[t]he Commonwealth Department of Health will share the information with other Commonwealth agencies and the state and territory government agencies as appropriate.”<sup>81</sup> Other general Department of Health privacy policies also potentially apply to the app.<sup>82</sup>

## D. COVIDSafe App

### 1. *How It Works*

#### a. Overview

The Department of Health explains that, upon downloading the COVIDSafe app, users provide their name, mobile number, and postcode, and select their age range. The user is sent a confirmation SMS text message to complete the installation of the app. The system “then creates a unique encrypted identifier” for the user.<sup>83</sup> The app uses Bluetooth to record a user’s contacts with others who have also installed the app:

COVIDSafe recognises other devices with the COVIDSafe app installed and Bluetooth enabled. When the app recognises another user, it notes the date, time, distance and duration of the contact and the other user’s reference code. The COVIDSafe app does not collect [the user’s] location.<sup>84</sup>

The information collected by the app is encrypted and “that encrypted identifier is stored securely” on the user’s phone—even the user cannot access it.<sup>85</sup> The information stored on the phone “is deleted on a 21-day rolling cycle.”<sup>86</sup>

A “frequently asked questions” document further explains that “[w]hen two (or more) app users come into close proximity their phones exchange Bluetooth signals and make a series of ‘digital handshakes,’” and that “[t]he proximity for a close contact is approximately 1.5 metres, for a period of 15 minutes or more.”<sup>87</sup> It appears that health officials are able to discern close contacts through technical processes that apply in the storage system: “A filtering process on the highly secure information storage system separates information that meets the close contact requirements and makes it available to the relevant state and territory health officials.”<sup>88</sup>

When an app user tests positive for COVID-19, state and territory health officials ask them about who they have been in contact with. If the user provides permission, “the encrypted contact

---

<sup>81</sup> Id.

<sup>82</sup> Id.

<sup>83</sup> *COVIDSafe App*, Department of Health, <https://perma.cc/ZMZ5-WVQJ>.

<sup>84</sup> Id.

<sup>85</sup> Id.

<sup>86</sup> Id.

<sup>87</sup> Department of Health, *Coronavirus Contact App FAQs 3* (Apr. 2020), <https://perma.cc/M99X-PRUJ>.

<sup>88</sup> Id. at 6.

information from the app will be uploaded to a highly secure information storage system.”<sup>89</sup> The officials will then

- use the contacts captured by the app to support their usual contact tracing
- call people to let them or their parent/guardian know they may have been exposed
- offer advice on next steps, including:
  - what to look out for
  - when, how and where to get tested
  - what to do to protect friends and family from exposure

Health officials will not name the person who was infected.<sup>90</sup>

Users will be prompted to delete the app at the end of the pandemic in Australia, thereby deleting all app information from their phones. In addition, “information contained in the information storage system will also be destroyed at the end of the pandemic.”<sup>91</sup>

The FAQs document states that “[t]he app cannot be used to enforce quarantine or isolation restrictions or any other laws” and “Commonwealth and state/territory law enforcement agencies will not be allowed to access any information from the app, unless investigating misuse of that information itself.”<sup>92</sup>

#### b. Privacy Policy

The privacy policy for the app, which has been published online, explains what personal information is collected, why it is being collected, how it is collected, how it will be stored, and how it will be used and disclosed, as well as the process for deleting personal information and for a person to access or correct their information; the contact data that the app will record (being “(1) the encrypted user ID, (2) date and time of contact and (3) Bluetooth signal strength of other COVIDSafe users with which you come into contact”); the generation of encrypted user IDs every two hours and the logging of these IDs in the National COVIDSafe data store; the fact that no location data will be collected at any time; access to and automatic deletion of contact data from a user’s phone; and the process if the user tests positive for COVID-19.<sup>93</sup>

The policy states that, when a user tests positive for COVID-19,

[a] health official will contact you and ask for consent to enter your mobile number into the data store to generate a PIN to be sent to you by SMS.

If you enter the PIN, you will give your consent to upload contact data on your device into the data store to share with health officials to enable contact tracing.

---

<sup>89</sup> *COVIDSafe App*, supra note 83.

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> Coronavirus Contact App FAQs, supra note 87, at 4.

<sup>93</sup> *Privacy Policy for COVIDSafe App*, Department of Health, <https://perma.cc/S836-HYVF>.

If another user tests positive to COVID-19, they may upload their contact data, which may include details of their contact with you.<sup>94</sup>

The policy also states that “[n]o user should feel pressured to install or continue to use COVIDSafe, or to agree to upload contact data to the data store,” and explains that complaints can be made to the Department of Health, OAIC, or the Australian Human Right Commission if a person feels pressured to do these things.<sup>95</sup>

Registration information, encrypted user IDs, and contact data is stored in a cloud-based facility, “using infrastructure located in Australia.”<sup>96</sup> A user can submit a request form for the deletion of personal information held in the data store.

The privacy policy for the app indicates that the Department of Health’s general privacy policy also applies, and that this policy contains information about how a person may complain about a breach of the APPs or an applicable APP code.<sup>97</sup> The FAQs document also states that, “[i]n accessing and using the uploaded data, health officials will be required to comply with the Australian Privacy Principles and all applicable data protection and information security obligations. It will only be able to be used for alerting individuals if they have come into contact with a person who has contracted coronavirus.”<sup>98</sup>

The OAIC “will have independent oversight of personal information handling by the app and the National COVIDSafe Data Store,” and can audit the system and investigate complaints.<sup>99</sup>

## 2. *Privacy Impact Assessment*

During the development of the app, the Department of Health engaged a law firm to prepare a Privacy Impact Assessment (PIA) to advise the Department on how it needed to address and mitigate any identified privacy risks.<sup>100</sup> Such PIA are required under the Australian Government Agencies Privacy Code for projects “involving new ways of handling personal information.”<sup>101</sup> The PIA identifies the potential impacts of the app on individuals’ privacy and sets out 19 recommendations for how these can be managed, minimized, or eliminated. The PIA, along with the Department’s response to the recommendations, were published online at the time the app was released.<sup>102</sup>

---

<sup>94</sup> Id.

<sup>95</sup> Id.

<sup>96</sup> Id.

<sup>97</sup> Id. See also *Privacy Policy*, Department of Health, <https://perma.cc/DK3F-654N>.

<sup>98</sup> *Coronavirus Contact App FAQs*, supra note 87, at 4.

<sup>99</sup> *Privacy Protections in COVIDSafe Contact Tracing App*, OAIC (Apr. 26, 2020), <https://perma.cc/BML2-AT5Q>.

<sup>100</sup> *COVIDSafe Application Privacy Impact Assessment*, Department of Health, <https://perma.cc/8CK2-CCGP>.

<sup>101</sup> See *Privacy Protections in COVIDSafe Contact Tracing App*, supra note 99.

<sup>102</sup> *COVIDSafe Application Privacy Impact Assessment – Agency Response*, Department of Health, <https://perma.cc/B6VA-PAVX>.

The PIA states that the law firm was “satisfied that Australian Government has considered the range of privacy risks associated with the App and has already taken steps to mitigate some of these risks. The PIA makes a range of recommendations to ensure privacy issues continue to be addressed as the App is rolled out and App information is collected and used.”<sup>103</sup> The PIA recommended, for example, that the Department of Health

- “consider making the source code for the App publicly available”;
- “continue to consider and investigate the legislative options in relation to the collection, use, disclosure, and deletion, of personal information in connection with the App”;
- “ensure that the App seeks consent from Users at two different points—an initial notice which is provided to individuals before they agree to their Registration Information being uploaded to the National COVIDSafe Data Store, and a further notice which is provided before they agree to upload the Digital Handshake information on their device to the National COVIDSafe Data Store”;
- “consider developing training and/or scripts for Public Health Officials and Contact Tracers in connection with the App”;
- “has contractual or other administrative arrangements in place with the State and Territory public health authorities responsible for contact tracing”;
- “seek independent assurance from security experts (including as appropriate, the Australian Signals Directorate and the Australian Cybersecurity Centre), to provide additional testing and assurance that the security arrangements for the App and the National COVIDSafe Data Store, and the use of information in it, are appropriate”; and
- “further consider the processes in the App if a User is a Child User.”<sup>104</sup>

The Department’s response to the PIA agreed with all of the recommendations and set out the actions being taken to address them.<sup>105</sup> The OAIC stated that it would monitor the implementation of the recommendations and closely review the relevant legislation.<sup>106</sup> The Australian Human Rights Commission also stated it would assess whether additional human rights safeguards should be included in the legislation.<sup>107</sup>

---

<sup>103</sup> Maddocks, *Department of Health: The COVIDSafe Application – Privacy Impact Assessment* ¶ 1.5 (Apr. 24, 2020), <https://perma.cc/YXP9-Q8JG>.

<sup>104</sup> *Id.* at 5-13.

<sup>105</sup> Department of Health, *The COVIDSafe Application: Privacy Impact Assessment – Agency Response* (2020), <https://perma.cc/8H5N-UAZH>.

<sup>106</sup> Privacy Protections in COVIDSafe Contact Tracing App, *supra* note 99.

<sup>107</sup> *Commission Welcomes COVIDSafe App*, Australian Human Rights Commission (Apr. 27, 2020), <https://perma.cc/6ADV-QGGK>.

### 3. *Interim Determination*

Upon launching the COVIDSafe app in late April, the federal Minister for Health made a determination under the Biosecurity Act 2015 (Cth)<sup>108</sup> that set out rules about the collection and disclosure of data collected via the app and prohibited the coercion of individuals to download or use the app.<sup>109</sup> The government explained that this was an interim measure and that legislation was being developed that would govern the app and resulting data. The Attorney-General's Department explained that the provisions in the determination

- ensure that data from COVIDSafe is only used to support state and territory health authorities' contact tracing efforts, and only to the extent required to do so
- outline limited additional circumstances when data from COVIDSafe can be used, including to investigate a breach of the determination and allow the administrator of the National COVIDSafe Data Store to produce de-identified statistics about COVIDSafe registrations
- require that users must consent before data from their device can be uploaded to the National COVIDSafe Data Store
- prevent data from COVIDSafe being retained outside of Australia, and protect against unauthorised disclosure outside of Australia
- require all COVIDSafe data held in the National COVIDSafe Data Store to be deleted at the end of the COVID-19 pandemic
- protect against decryption of COVIDSafe data stored on users' devices
- provide that no one can be forced to download or use COVIDSafe or upload their data to the National COVIDSafe Data Store.<sup>110</sup>

### 4. *Legislation*

On May 4, 2020, the Australian government released a draft bill related to the COVIDSafe app:<sup>111</sup> the Privacy Amendment (Public Health Contact Information) Bill 2020.<sup>112</sup> The final version of the legislation was introduced in the Parliament on May 12, 2020, and passed on May 14, 2020.<sup>113</sup> The Bill "substantially reproduces the obligations and prohibitions contained in the COVIDSafe Determination, with some amendments to strengthen potential gaps in protection."<sup>114</sup> The Bill

---

<sup>108</sup> Biosecurity Act 2015 (Cth) s 477(1).

<sup>109</sup> Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements – Public Health Contact Information) Determination 2020, <https://perma.cc/H2TM-MHEF>.

<sup>110</sup> *COVIDSafe Draft Legislation*, Attorney-General's Department, <https://perma.cc/YMM6-GDG7>.

<sup>111</sup> Press Release, Attorney-General, Legislation for COVIDSafe App Privacy Protections (May 4, 2020), <https://perma.cc/66AQ-TBTR>. See also Justin Hendry, *Govt Unveils COVIDSafe Contact Tracing App Bill*, ITNews (May 5, 2020), <https://perma.cc/Y58J-PLUU>.

<sup>112</sup> *COVIDSafe Draft Legislation*, supra note 110; Exposure Draft: Privacy Amendment (Public Health Contact Information) Bill 2020, <https://perma.cc/S6XB-VSGN>.

<sup>113</sup> *Privacy Amendment (Public Health Contact Information) Bill 2020*, Parliament of Australia, <https://perma.cc/UK7M-DY6Y>.

<sup>114</sup> Claire Petrie, *Privacy Amendment (Public Health Contact Information) Bill 2020*, at 4 (Parliamentary Library, Bills Digest No. 98, 2019-20, May 12, 2020), <https://perma.cc/7533-U5EZ>.

repealed the determination when it came into force. The Attorney-General's Department summarized the key additional protections in the Bill as follows:

- The national privacy regulator, the Office of the Australian Information Commissioner (OAIC), will have oversight of COVIDSafe. They can manage complaints about mishandling of COVIDSafe data and conduct assessments relating to maintenance and handling of that data.
- The Privacy Act's Notifiable Data Breaches scheme will be extended to apply to COVIDSafe data.
- The interaction between the powers and obligations of the OAIC in relation to COVIDSafe data with the powers of state and territory privacy regulators and the Australian Federal Police will be clarified.
- The administrator of the National COVIDSafe Data Store will delete users' registration data upon request.
- An individual will be required to delete COVIDSafe data if they receive it in error.
- No data can be collected from users who have chosen to delete COVIDSafe.
- A process will be put in place for COVIDSafe data to be deleted at the end of the COVID-19 pandemic and users to be notified accordingly.<sup>115</sup>

The Bill added a new part to the Privacy Act, part VIIIA.<sup>116</sup> A provision in the Bill "expressly cancels the effect of any Australian law which would otherwise permit or require conduct, or an omission to act, that is prohibited under" the new part.<sup>117</sup> According to information provided by the government to the Senate committee tasked with overseeing the response to COVID-19, the legislation "overrides all other Commonwealth and state and territory laws that would provide for any form of law enforcement access."<sup>118</sup>

The Bill contains various offenses, including collecting, using, or disclosing app data outside of the circumstances permitted by the Bill; "retaining uploaded COVID app data which has been uploaded to the COVIDSafe Data Store on a database outside Australia, or disclosing such data to another person outside Australia (other than for contact tracing purposes)"; "uploading, or causing to be uploaded, COVID app data from a communication device to the COVIDSafe Data Store without the consent of the COVIDSafe user . . ."; decrypting app data that is stored on a communication device; and coercive actions in respect of the app, including, for example, requiring a person to download or use the app or upload data from the app.<sup>119</sup> Each offense "carries a maximum penalty of five years imprisonment and/or 300 penalty units (\$63,000 [about US\$40,780]). This is the same as the maximum penalty applicable under the Biosecurity Act for breaches of the COVIDSafe Determination."<sup>120</sup>

---

<sup>115</sup> COVIDSafe Draft Legislation, *supra* note 110.

<sup>116</sup> Privacy Amendment (Public Health Contact Information) Act 2020 (Cth), <https://perma.cc/UN3V-B5M5>.

<sup>117</sup> Petrie, *supra* note 114, at 4.

<sup>118</sup> Quoted in *id.* at 5.

<sup>119</sup> *Id.* at 7.

<sup>120</sup> *Id.* at 8.

Under the Notifiable Data Breaches scheme,

the data store administrator or relevant health authority is required to notify the [OAIC] where they have reasonable grounds to believe they have breached a requirement in relation to COVID app data. The [OAIC] will determine whether the administrator/health authority is required to comply with the data breach notification requirements by preparing a statement about the data breach and notifying affected individuals of (or otherwise publicising) the contents of this statement.<sup>121</sup>

The OAIC also has the power to conduct assessments of whether state and territory authorities are complying with the part, and to conduct investigations (either in response to a complaint or on its own initiative) into interferences with individuals' privacy.<sup>122</sup>

The Bill introduced in the Parliament included reporting requirements that had not been contained in the original draft. These include a requirement that the Minister for Health "cause a report to be prepared on the operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store" every six months, and to present the report to the Parliament.<sup>123</sup> The OAIC must also prepare reports on the performance of its functions, and exercise of its powers, under the new part.<sup>124</sup> The explanatory memorandum for the Bill states that the reporting obligations are "designed to ensure an appropriate degree of transparency and to build public confidence in the strong privacy protections that will apply under the Bill."<sup>125</sup>

The Minister for Health must determine a particular day to be the end of the COVIDSafe data period. The Minister must first consult the Chief Medical Officer or AHPPC and must be satisfied that by that day "the use of the app is no longer required to prevent or control, or no longer likely to be effective in preventing or controlling, COVID-19 in Australia."<sup>126</sup> At the end of the period, no further app data may be collected and the app must not be available for download. The data store administrator must also delete all app data from the data store, inform the Minister for Health and OAIC that it has been deleted, and take all reasonable steps to inform current users of this fact. The Bill provides for the repeal of all provisions inserted into the Act at the end of 90 days after the date specified as being the end of the data period.<sup>127</sup>

##### *5. Concerns Raised*

Privacy advocates and legal experts have raised various concerns about the privacy protections provided by the app itself, by the interim determination, and by the draft and final bill. These include, for example, potential conflicts with other apps, the possibility of Bluetooth tracking

---

<sup>121</sup> Id.

<sup>122</sup> Id. at 9.

<sup>123</sup> Id.

<sup>124</sup> Id.

<sup>125</sup> Attorney-General, Explanatory Memorandum: Privacy Amendment (Public Health Contact Information) Bill 2020, at 7, <https://perma.cc/DMJ6-E2C5>.

<sup>126</sup> Petrie, *supra* note 114, at 10.

<sup>127</sup> Id.

location on other apps, vulnerabilities to data interception, failure to clearly limit data collection and decryption to information about “close contacts,” failure to include decrypted records in the definition of COVID app data in the legislation, and loopholes in the rules against coercing individuals to download and use the app.<sup>128</sup>

However, many appear to believe that the COVIDSafe Bill passed in May “does go a long way to protecting the use and disclosure of information collected by the app.”<sup>129</sup> The opposition party in Parliament agreed, stating that “[i]n many ways the privacy protections included in this bill are—to use the word of our times—unprecedented in Australian law.”<sup>130</sup> According to the deputy chief medical officer, “all states and territories have now signed up to allow their health officials to use the data.”<sup>131</sup> He stated that “[w]e are now absolutely certain privacy and data security issues are all taken care of in terms of states and territories agreeing to our proposals.”<sup>132</sup>

One of the remaining major concerns raised by critics is whether United States law enforcement entities could gain access to the app data.<sup>133</sup> This is because the data is being hosted in Australia by Amazon Web Services, a US company subject to the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)—“a law which can force US companies to hand over data to US law enforcement regardless of where that data is held.”<sup>134</sup> The government has argued that the Bill makes it an offense to transfer any of the data to any country outside Australia. However, critics have noted that the Telecommunications Legislation Amendment (International Production Orders) Bill 2020,<sup>135</sup> currently before Parliament, which was developed with the CLOUD Act in mind, “make[s] it possible for Australia to facilitate agreements with other nations so that Australian law enforcement agencies could access data held in those countries and vice versa.”<sup>136</sup> For example, the Law Council raised concerns about the adequacy of safeguards in the

---

<sup>128</sup> See James Jin Kang & Paul Haskell-Dowland, *How Safe is COVIDSafe? What You Should Know About the App’s Issues, and Bluetooth-related Risks*, The Conversation (May 7, 2020), <https://perma.cc/7KX4-QSZV>; Stilgherrian, *Australia’s Wobbly Start to the COVIDSafe App Transparency*, ZDNet (May 11, 2020), <https://perma.cc/GG3A-R5BF>; Graham Greenleaf & Katharine Kemp, *The COVIDSafe Bill: Privacy Protections Improved, But More Needed*, UNSW, Newsroom (May 5, 2020), <https://perma.cc/329M-PVZK>; Gavin Smith et al., *The COVIDSafe Bill – Good Progress, But There’s More to Do*, Allens, Insight (May 6, 2020), <https://perma.cc/NV3T-RQSJ>; Sheila McGregor et al., *Does the 80:20 Rule Apply? – Federal Government Releases Draft COVIDSafe App Privacy Legislation*, Gilbert + Tobin, COVID-19 Hub (May 7, 2020), <https://perma.cc/B6D6-DA84>.

<sup>129</sup> Paul Farrell, *Experts Raise Concerns about Security of Coronavirus Tracing App COVIDSafe*, ABC News (May 14, 2020), <https://perma.cc/8T5J-FFZQ>.

<sup>130</sup> *Id.*

<sup>131</sup> *Deputy Medical Officer Says All Coronavirus Tracing App Privacy Concerns ‘Are Taken Care Of’*, SBS News (May 14, 2020), <https://perma.cc/5F5Y-BNUJ>.

<sup>132</sup> *Id.*

<sup>133</sup> See Dylan Welch & Linton Besser, *Experts Warn There Are Still Legal Ways the US Could Obtain COVIDSafe Data*, ABC News (Apr. 27, 2020), <https://perma.cc/88XD-UGY6>.

<sup>134</sup> Josh Taylor, *Questions Remain over Whether Data Collected by Covidsafe App Could be Accessed by US Law Enforcement*, Guardian (May 14, 2020), <https://perma.cc/935X-3DXC>.

<sup>135</sup> *Telecommunications Legislation Amendment (International Production Orders) Bill 2020*, Parliament of Australia, <https://perma.cc/HGX7-NM6H>.

<sup>136</sup> Taylor, *supra* note 134.

COVIDSafe Bill to “quash” US requests for data under the CLOUD Act and argued that the relevant reciprocal executive agreement with the US government, currently being negotiated, would need to ensure the app data is excluded.<sup>137</sup>

On May 19, 2020, several news articles reported that the NSW government was still “formally evaluating the use of the COVIDSafe app,” and other states also confirmed that their health officials had not yet accessed any of the app data.<sup>138</sup> *The Guardian* reported that NSW Health had contacted the Digital Transformation Agency regarding a technical problem.<sup>139</sup> In response to the reports, the federal Department of Health issued a statement saying that “[a]ny claims that technical issues are restricting access are not correct,” and that each state and territory has “undertaken training and adopted clear protocols on access of information when a person tests positive.”<sup>140</sup> The statement further said that,

[a]s is expected, each state will refine how they operate, noting that currently there are only a small number of cases nationally. We hope this continues. The app will be an essential tool for containing any further outbreaks.

The key is to have as many people registered with the app so in the event of an outbreak, public health officials can find cases faster and rapidly contain it. This will be increasingly important as restrictions are eased around the country and people are more mobile.<sup>141</sup>

---

<sup>137</sup> Id.

<sup>138</sup> Kelly Burke, *Coronavirus Testing: Australia’s COVIDSafe App Still an Untried Tool*, 7News (May 19, 2020), <https://perma.cc/YE6X-ANBQ>.

<sup>139</sup> Josh Taylor, *NSW is Unable to Use Covidsafe App’s Data for Contact Tracing*, Guardian (May 19, 2020), <https://perma.cc/6BC9-QQGK>.

<sup>140</sup> Press Release, Department of Health, *Operation of the COVIDSafe App* (May 19, 2020), <https://perma.cc/8FBY-TL78>.

<sup>141</sup> Id.

# China

Laney Zhang  
Foreign Law Specialist

**SUMMARY** In China, the national legislature is considering a comprehensive personal information protection law. Currently, the Cybersecurity Law, which went into effect in 2017, sets out general data protection requirements for network operators. The nonbinding national guidelines for personal data protection provide detailed data protection rules. China's civil and criminal laws, as well as laws and regulations relating to specific sectors, also contain provisions on privacy and data protection.

The data protection law generally requires consent from the data subjects to collect, store, process, disclose, and use their personal data. The personal data protection guidelines provide additional protection for sensitive personal data, which is defined to include location records and health records. For the purposes of prevention and control of the pandemic, however, authorized parties may collect personal data without the consent of data subjects.

The health code apps reportedly rely on a combination of self-reporting by the user, COVID-19 databases set up by government authorities, and data held by other sources, including the public transportation, telecommunication, and banking sectors. In response to data privacy concerns, the national health code guidelines, issued in April 2020, specify the requirements for the collection, processing, and use of personal health information.

The itinerary card app tracks places users have visited over the past 14 days and has the function of contact tracing using Bluetooth. This app asks for consent from the user to access travel history, but claims not to collect the national ID number, home address, or any other personal data of the user.

## I. Introduction

As of May 22, 2020, the National Health Commission of the People's Republic of China (PRC or China) had reported 82,971 COVID-19 cases, with 82 active cases.<sup>1</sup> China has been gradually easing COVID-19 restrictions as the cases decline, although there is still fear about the resurgence of the epidemic.<sup>2</sup>

---

<sup>1</sup> National Health Commission of the People's Republic of China, *Updated COVID-19 Pandemic Information as of 24:00, May 21*, <https://perma.cc/N6FD-MJJ6> (in Chinese).

<sup>2</sup> *Coronavirus: Wuhan in First Virus Cluster since End of Lockdown*, BBC (May 11, 2020), <https://perma.cc/A8TC-S3FM>.

According to the market and consumer data provider Statista, China is the world's largest smartphone market, with the number of smartphone users projected to reach about 780 million by 2020. As of September 2019, mobile phone subscriptions had reached about 1.6 billion.<sup>3</sup>

Leakage of personal data has become a widespread problem in the country. In a survey done by a Chinese newspaper in 2019, 95% of respondents said their personal data had been stolen and almost 80% were concerned that their facial recognition data could be leaked from apps.<sup>4</sup> A legal framework to strength the protection of personal data is being built, although there is still no significant protection of individual's data privacy against government intrusion, a study comparing China's approach on data privacy law with that of the US and EU finds.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

China has not adopted comprehensive legislation focusing on the regulation of privacy and data protection. The National People's Congress Standing Committee (NPCSC) has announced that a Personal Information Protection Law is on the national legislature's 2020 legislative agenda.<sup>6</sup> Currently, data protection requirements are found in a series of laws and regulations, outlined below.

#### 1. Legislative Decision, Cybersecurity Law, and National Guidelines

The 2012 NPCSC Decision on Strengthening Network Information Protection provides high-level national rules relating to the protection of personal data in electronic form. The decision requires internet service providers and other enterprises and public institutions to (1) clearly indicate the purposes, methods, and scope of collection and use of citizens' personal electronic data, abiding by the principles of "legality, legitimacy, and necessity"; (2) obtain consent from the persons whose personal electronic data is collected; and (3) make public their rules for collection and use of personal electronic data.<sup>7</sup>

The PRC Cybersecurity Law, which was promulgated in 2016 and went into effect in 2017, sets out general rules of data protection requirements for network operators. Network operators

---

<sup>3</sup> Samantha Wong, *Smartphone Market in China - Statistics & Facts*, Statista (Apr. 27, 2020), <https://perma.cc/VC54-77UF>.

<sup>4</sup> Laurie Chen, *China Wakes Up to Wide Web of Online Data Leaks and Privacy Concerns*, South China Morning Post (Jan. 27, 2020), <https://perma.cc/S2N7-PCPS>.

<sup>5</sup> Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU?*, 8(1) Penn State J.L. & Int'l Aff. 51 (2020), <https://perma.cc/TDB9-WXM2>.

<sup>6</sup> *China's Top Legislature to Formulate Law on Personal Information Protection*, Xinhuanet (May 25, 2020), <https://perma.cc/34YV-VPSE>.

<sup>7</sup> Decision on Strengthening Network Information Protection (adopted by the NPCSC on Dec. 28, 2012, effective the same day) art. 2, <https://perma.cc/L9KD-D9VE> (in Chinese); Laney Zhang, *China: NPC Decision on Network Information Protection*, Global Legal Monitor (Law Library of Congress, Jan. 4, 2013), <https://perma.cc/2B8Z-86J8>.

under the Law include not only owners and administrators of a network, but also network service providers.<sup>8</sup> The Law specifically requires network operators to provide technical support and assistance to the public security organs (the police) and the national security organs in the authorities' activities of protecting national security and investigating crimes.<sup>9</sup> It also contains an article prohibiting government authorities and their staff from leaking, selling, or otherwise illegally providing personal data they are aware of in performing cybersecurity supervision duties.<sup>10</sup>

Detailed data protection rules are found in national and local guidelines, in particular the personal data protection guidelines that were first issued in 2017 and recently revised in March 2020 (Personal Data Protection Guidelines). The Personal Data Protection Guidelines, however, are recommended guidelines that lack the force of law.<sup>11</sup>

## 2. *Civil Law, Criminal Law, and Sector-Specific Laws*

The PRC General Rules of Civil Law prescribe the rights that natural persons are entitled to, including the right to privacy and the right to have their personal data legally protected.<sup>12</sup> Any organization or individual that needs to obtain the personal data of others must obtain such information pursuant to the law and ensure information security, and may neither illegally collect, use, process, or transmit the personal data of others, nor illegally trade, provide, or disclose the personal data of others.<sup>13</sup> The new PRC Civil Code, which is expected to be passed in this year's NPC annual session which opened on May 22, 2020, contains a chapter on privacy and personal data protection.<sup>14</sup>

Under the PRC Criminal Law, an individual may be sentenced to imprisonment for up to seven years, if the circumstances are especially serious, for: (1) illegally selling or providing to others personal data; or (2) stealing or otherwise illegally obtaining personal data.<sup>15</sup>

Requirements to collect, analyze, store, and share personal data can also be found in various laws and regulations relating to specific sectors such as the banking, insurance, medical, credit

---

<sup>8</sup> PRC Cybersecurity Law (adopted by the NPCSC on Nov. 7, 2016, effective June 1, 2017) art. 76, <https://perma.cc/3HAP-D6MZ> (in Chinese).

<sup>9</sup> Id. art. 28.

<sup>10</sup> Id. art. 45.

<sup>11</sup> State Administration for Market Regulation & Standardization Administration of China, PRC National Guidelines, Information Security Technology – Personal Information Security Specification, GB/T 35273 – 2020 (Mar. 6, effective Oct. 1, 2020) (Personal Data Protection Guidelines), <https://perma.cc/9XQ4-72GA> (in Chinese).

<sup>12</sup> PRC General Rules on the Civil Law (adopted by the National People's Congress on Mar. 15, 2017, effective Oct. 1, 2017) art. 110, <https://perma.cc/AY65-LA2N>.

<sup>13</sup> Id. art. 111.

<sup>14</sup> *China Focus: China Moves Closer to Civil Code*, Xinhuanet (May 20, 2020), <https://perma.cc/4TSX-XCHQ>.

<sup>15</sup> Ninth Amendments to the PRC Criminal Law (adopted by the NPCSC on Aug. 29, 2015, effective Nov. 1, 2019) art. 253a, <https://perma.cc/U4QB-YKN4> (in Chinese).

information, and telecommunications sectors. The new E-commerce Law passed in 2018 contains strong data protection requirements applicable to e-commerce operators.<sup>16</sup>

## **B. Data Retention and Location Tracking**

### *1. Requirements under Cybersecurity Law and National Guidelines*

The data protection laws generally require consent from data subjects to collect, store, process, disclose, and use their personal data. The Cybersecurity Law provides that network operators may only collect, store, process, disclose, and use personal data if individuals are notified of the purpose, manner, and scope of such activities, and have consented to it. According to the Law, network operators must not collect personal data that are irrelevant to the services they provide and must dispose of the personal data they have stored in accordance with applicable laws, administrative regulations, and agreements with the user.<sup>17</sup>

The Cybersecurity Law does not distinguish between personal data and sensitive personal data. The definition of “sensitive personal data” and its additional protection are found in the Personal Data Protection Guidelines. The Guidelines define sensitive personal data as personal data the leakage, illegal provision, or abuse of which may endanger the safety of life and property; easily damage the personal reputation or physical and mental health of a person; or easily cause discriminatory treatment.<sup>18</sup> Identity card numbers, personal biometric information, bank account numbers, communication records and content, property information, credit information, location records (行踪轨迹), accommodation information, health and physiological information, transaction information, and the personal data of children at or under the age of 14 are sensitive personal data under the Guidelines.<sup>19</sup>

The Guidelines provide additional protection for processing sensitive personal data. The explicit consent of the data subject must be obtained when collecting sensitive personal data.<sup>20</sup> Security measures such as encryption must be implemented in transmitting and storing sensitive personal data.<sup>21</sup>

### *2. Criminal Punishments*

Illegally selling or providing to others location tracking data is criminally punishable under the PRC Criminal Law. The Law itself does not specify the scope of the personal data to be protected. In 2017, the Supreme People’s Court (the highest court) and the Supreme People’s Procuratorate (the prosecutor) jointly released a judicial interpretation on the infringement of personal data in

---

<sup>16</sup> Laney Zhang, *China: E-Commerce Law Passed*, Global Legal Monitor (Law Library of Congress, Nov. 21, 2018), <https://perma.cc/BJ9F-UQMN>.

<sup>17</sup> PRC Cybersecurity Law art. 41.

<sup>18</sup> Personal Data Protection Guidelines § 3.2.

<sup>19</sup> *Id.*

<sup>20</sup> *Id.* § 5.4.

<sup>21</sup> *Id.* § 6.3.

criminal cases. The interpretation defines the scope of personal data: name, ID number, correspondence and telecommunications contact information, resident address, account name and password, property ownership, and whereabouts and tracking data (行踪信息).<sup>22</sup>

### 3. *Data Collection under Health Laws*

The PRC Law of Prevention and Treatment of Infectious Diseases (Infectious Diseases Law) obliges all entities and individuals in China to “provide truthful information about diseases” to disease control agencies and medical institutions.<sup>23</sup> The Law further requires disease control agencies to collect, analyze, investigate, and verify information of the epidemic, and report to relevant governments.<sup>24</sup>

## III. Electronic Measures to Fight COVID-19 Spread

### A. Circular on Personal Data Protection and Big Data

China has deployed digital technologies, including artificial intelligence, big data, cloud computing, blockchain, and 5G, in fighting the COVID-19 spread, and these technologies “have effectively improved the efficiency of the country’s efforts in epidemic monitoring, virus tracking, prevention, control and treatment, and resource allocation,” according to an article authored by an official of the Cyberspace Administration of China.<sup>25</sup>

In response to public concerns about numerous data leakage incidents that happened around the country during the outbreak of COVID-19, on February 4, 2020, the Cyberspace Administration of China released a circular on protecting personal data in fighting the pandemic.<sup>26</sup>

#### 1. *Exception to the Requirement of Consent*

The Circular states that those parties authorized by the health department of the State Council pursuant to the Cybersecurity Law, Law of Prevention and Treatment of Infectious Diseases, and Regulation on Responses to Public Health Emergencies may collect personal data for the purposes of prevention and control of the epidemic. Unless otherwise provided by relevant laws

---

<sup>22</sup> Supreme People’s Court & Supreme People’s Procuratorate, Judicial Interpretation on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens’ Personal Information (May 8, 2017, effective June 1, 2017), <https://perma.cc/S9SF-44J7> (in Chinese); Laney Zhang, *China: Judicial Interpretation on Infringement of Personal Information Released*, Global Legal Monitor (Law Library of Congress, Sept. 1, 2017), <https://perma.cc/V3Q7-TH92>.

<sup>23</sup> PRC Law of Prevention and Treatment of Infectious Diseases (adopted by the NPCSC on Feb. 21, 1989, amended June 29, 2013) art. 12, <https://perma.cc/287T-JNGP> (in Chinese).

<sup>24</sup> *Id.* art. 33.

<sup>25</sup> Qi Xiaoxia, *How Next-Generation Information Technologies Tackled COVID-19 in China*, World Economic Forum (Apr. 8, 2020), <https://perma.cc/TU48-DG2K>.

<sup>26</sup> Cyberspace Administration of China, Circular on Ensuring Effective Personal Information Protection and Utilization of Big Data to Support Joint Efforts for Epidemic Prevention and Control (Feb. 4, 2020), <https://perma.cc/6WUS-ZLQV> (in Chinese).

and administrative regulations, unauthorized parties may not collect data for pandemic prevention and control purposes without the consent of the data subjects.<sup>27</sup>

## 2. Requirements for Data Collection

The Circular provides that the collection of personal data must refer to the Personal Data Protection Guidelines. Subjects whose personal data may be collected are limited to a key group comprised of confirmed carriers, suspected carriers, and close contacts.<sup>28</sup> Personal data collected for preventing or treating epidemic diseases cannot be used for any other purpose and cannot be made public without the consent of the data subjects unless public disclosure is necessary for the prevention of the epidemic and the information is first redacted or anonymized.<sup>29</sup> The Circular also requires entities that collect and possess personal data to have strict data security measures in place to prevent data breaches.<sup>30</sup>

The Circular encourages capable enterprises to utilize big data to support the control and prevention of the pandemic and monitor the movement of confirmed carriers, suspected carriers, and close contacts.<sup>31</sup>

## B. Health Code Apps

Since February 2020, Chinese provinces and municipalities have started to introduce their own color-based health code systems to control people's movements and curb the spread of the coronavirus. There is also a national health code system. The health code systems are largely operated as mini apps embedded in the popular social media app WeChat and the payment app Alipay. The mini apps automatically generate and assign quick response codes (QR codes) to citizens as an indicator of their health status. Most systems use three colors: users with a green code can move freely, users with a yellow code have to go into government quarantine or self-quarantine for up to seven days, and users with a red code will be quarantined for 14 days.<sup>32</sup>

The health code apps reportedly rely on a combination of self-reporting by the user, COVID-19 databases set up by government authorities, and data held by other sources including the public transportation, telecommunication, and banking sectors. Typically, the user is required to report his or her name, gender, cellphone number, national ID number, home address, and travel history; indicate whether he or she has been in contact with someone diagnosed with COVID-19; and complete a health survey. The apps also have access to data held by the public transportation systems, including the civil aviation, railroad, highway, electronic toll collection, and city bus

---

<sup>27</sup> Id. art. 1.

<sup>28</sup> Id. art. 2.

<sup>29</sup> Id. art. 3.

<sup>30</sup> Id. art. 4.

<sup>31</sup> Id. art. 5.

<sup>32</sup> *Where Are Health Codes Going in the Future?*, The Paper (Apr. 24, 2020), <https://perma.cc/68C3-XXTW> (in Chinese); Nectar Gan & David Culver, *China Is Fighting the Coronavirus with a Digital QR Code. Here's How It Works*, CNN Business (Apr. 16, 2020), <https://perma.cc/9WBF-8NBF>.

systems; data from telecommunication operators; and payment data held by banks and other financial institutions.<sup>33</sup>

Although the health code apps do not appear to have been made compulsory, in many cities, citizens without the code wouldn't be able to leave their residential compounds or enter most public places. The apps may serve as a tracker for people's movements in public areas, as users have their codes scanned as they enter public places.<sup>34</sup>

Privacy experts have warned about the leakage and abuse of personal data associated with the health code apps and have urged Chinese authorities to make sure the health code apps meet data privacy principles.<sup>35</sup> On April 29, 2020, the State Administration for Market Regulation and Standardization Administration of China released a series of national guidelines for personal health information codes, which specify requirements for the collection, processing, and use of personal health information and aim to help the provinces acknowledge health codes from each other and facilitate travel.<sup>36</sup>

Under the guidelines, the collection, processing, and use of personal health information must comply with the Personal Data Protection Guidelines. Health codes must be encrypted and stored using an algorithm satisfying the requirements for national password management. Personal health information services and apps must obtain the express consent or authorized consent of users when collecting data, and must keep the private content confidential. The guidelines, however, are recommended guidelines that lack the force of law.<sup>37</sup>

### C. Itinerary Card App

Another COVID-19 app, the "communication big data-based itinerary card," was launched by China's Ministry of Industry and Information Technology with the aim of helping users "easily prove your itinerary, improve the efficiency of itinerary inspection of enterprises, communities, transportation departments and other agencies, and speed up the process of work resumption."<sup>38</sup>

The itinerary card app does not require self-reporting by users, but asks for consent from users to access their travel history. It tracks places users have visited over the past 14 days, including

---

<sup>33</sup> Id.

<sup>34</sup> Gan & Culver, *supra* note 32.

<sup>35</sup> Id.; *Expert Warns Against Health Code Data Leakage and Abuse*, Xinhuanet (Mar. 18, 2020), <https://perma.cc/WAT5-NBG7> (in Chinese).

<sup>36</sup> *National Guidelines for Personal Health Information Codes Released and Implemented*, China Electronics Standardization Institute (Apr. 30, 2020), <https://perma.cc/GZ2J-2974> (in Chinese).

<sup>37</sup> *Frequently Asked Questions on Personal National Guidelines for Personal Health Information Codes*, China Electronics Standardization Institute (May 7, 2020), <https://perma.cc/7SCE-CSB3> (in Chinese).

<sup>38</sup> *How Can I Prove that I Have Not Been to Any Epidemic-Stricken Region or Country in the Past 14 Days? Use This!*, China Academy of Information and Communications Technology, <https://perma.cc/DB8V-QGTX>.

any domestic cities they stayed in for over four hours and any other countries visited. A color card will be assigned mainly based on the places the user visited.<sup>39</sup>

Responding to data privacy concerns, the app claims that it does not collect the national ID numbers, home addresses, or any other personal data of users.<sup>40</sup> An updated version of the app has the function of contact tracing using Bluetooth. A user will receive a risk alert when any other user who has been in close contact with him or her is diagnosed positive.<sup>41</sup>

---

<sup>39</sup> Id.

<sup>40</sup> Id.

<sup>41</sup> *Communication Big Data Travel Card User Guide*, China Academy of Information and Communications Technology, <https://perma.cc/9ZYK-AWXF> (in Chinese).

# India

*Tariq Ahmad*  
*Foreign Law Specialist*

**SUMMARY** The Supreme Court of India has held that the right to privacy is a fundamental right protected under article 21 (right to life and personal liberty) of India’s Constitution. India currently does not have a comprehensive Privacy Bill, though one is being developed, but specific provisions to protect electronic data can be found in the Information Act, 2000, and its subsidiary privacy rules. No central law lays out data retention provisions for government agencies and departments but various agencies have adopted their own data retention policies.

Both the Union and state governments have launched numerous COVID-19-related apps over the last two months to curtail the spread of the disease in the country. The most prevalently used app is the Union government’s official COVID-19 tracking app, Aarogya Setu (“bridge to health”), which was launched in April for Android and iOS users. The app was developed by the National Informatics Centre of the Ministry of Electronics and Information Technology as a contact tracing app. It uses both Bluetooth and GPS location data technology and allows users to assess the risk of their catching the coronavirus infection based on their interactions with others.

## I. Introduction

According to the Ministry of Health and Family Welfare website, as of May 22, 2019, India had 66,330 active cases of COVID-19, 48,533 cured/discharged COVID-19 patients, and 3,583 deaths from the disease.<sup>1</sup>

There are an estimated 450 million smartphone users and 550 million feature phone users in India.<sup>2</sup> According to a 2019 KPMG report, the smartphone user base is forecast to be 829 million by 2022, growing at a compound annual growth rate of 15.5%.<sup>3</sup> According to Statista, “[i]t was predicted that by 2022, 36 percent of mobile phone users in the country would use a smartphone, up from 26 percent in 2018.”<sup>4</sup>

Most surveys on users’ willingness to share personal data appear to be focused on the private sector. One recent survey by Accenture found that “[n]early six in ten consumers would be willing to share significant personal information, such as location data and lifestyle information,

---

<sup>1</sup> *COVID-19 India*, Ministry of Health and Family Welfare, <https://perma.cc/QVT3-7ZBQ>.

<sup>2</sup> Himanshi Lohchab, *Overall India Handset Market Growth to Fall in 2020*, *The Economic Times* (Dec. 24, 2019), <https://perma.cc/9ERD-UJRD>.

<sup>3</sup> KPMG, *Fintech in India – Powering Mobile Payments 6-8* (Aug. 2019), <https://perma.cc/VKC2-KPG3>.

<sup>4</sup> *Share of Mobile Phone Users that Use a Smartphone in India from 2014 to 2022*, Statista (Oct. 24, 2019), <https://perma.cc/942Z-XUUS>.

with their bank and insurer in exchange for lower pricing on products and services.”<sup>5</sup> However, “consumers believe that privacy is paramount, with three quarters (75 percent) saying they are very cautious about the privacy of their personal data. In fact, data security breaches were the second-biggest concern for consumers, behind only increasing costs, when asked what would make them leave their bank or insurer.”<sup>6</sup> One 2018 survey by the Analytics India Magazine found that “50.6% of the respondents said they trust banks most with their personal data—more than the government, e-commerce companies, social media websites or online media companies,” and “[o]verall, 33% respondents said they trust government departments with their data. 27% are neutral and 40% of respondents admitted that they do not trust them with their data.”<sup>7</sup>

## II. Legal Framework

### A. Privacy and Data Protection

On August 24, 2017, the Supreme Court of India, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,<sup>8</sup> held that privacy is a fundamental right protected by article 21 (right to life and personal liberty) of India’s Constitution.<sup>9</sup>

Currently, the Information Technology Act, 2000,<sup>10</sup> “contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically).”<sup>11</sup> India’s Ministry of Electronics and Information Technology (IT) adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules),<sup>12</sup> which took effect in 2011 and “require corporate entities collecting, processing and storing personal information, including sensitive personal information, to comply with certain procedures.”<sup>13</sup> The rules contain “specific provisions regarding the collection of sensitive personal data or information. They apply to all body corporates in India other than those providing services related to the processing of sensitive personal data or information to any person under a contract.”<sup>14</sup>

---

<sup>5</sup> Six in Ten Consumers Willing to Share Significant Personal Data with Banks and Insurers in Exchange for Lower Pricing, Accenture Study Finds, Accenture (Mar. 14, 2019), <https://perma.cc/AJ6D-W9FQ>.

<sup>6</sup> Id.

<sup>7</sup> Smita Sinha, *Annual Consumer Survey on Data Privacy in India 2018*, Analytics India Magazine (May 25, 2018), <https://perma.cc/E2K5-44HD>.

<sup>8</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1, <https://perma.cc/FF7F-YD7Z>.

<sup>9</sup> *Data Protection Laws of the World: India*, DLA Piper, <https://perma.cc/2YRD-P5GB>.

<sup>10</sup> Information Technology Act, 2000, <https://perma.cc/H4DG-9FZ7>.

<sup>11</sup> DLA Piper, *supra* note 9.

<sup>12</sup> Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules), 2011, <https://perma.cc/4WVQ-QC43>.

<sup>13</sup> DLA Piper, *supra* note 9.

<sup>14</sup> Talwar Thakore & Associates, *Data Protected*, Linklaters, (Mar. 2020) <https://perma.cc/6KXV-P7TT>.

The above Supreme Court ruling has led to the drafting of the wide-ranging Personal Data Protection Bill 2019,<sup>15</sup> which was introduced by the Minister of Electronics and Information Technology and is currently being reviewed by the Joint Parliamentary Committee (JPC).<sup>16</sup> It would apply to the processing of personal data by the state and private sector,<sup>17</sup> but the processing of “anonymous data” is outside the scope of the Bill,<sup>18</sup> except that the central government could direct organizations to disclose “anonymized” personal data or “non-personal data” under section 91 “to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government.”<sup>19</sup> The proposed Bill has “a broad definition of sensitive personal data and also identifies financial data, data about caste, tribe, religious and political belief or affiliation as sensitive personal data,” and has “stringent requirements with respect to the processing of sensitive personal data and information including requiring explicit consent, imposing additional conditions for cross-border transfers and requiring a copy to be stored in India.”<sup>20</sup>

## **B. Data Retention and Location Tracking**

### *1. Data Retention*

There is no central law for government agencies and departments in India that lays out data retention provisions, but various agencies have adopted their own data retention policies.

For the private sector, Rule 5(4) of the Privacy Rules states that a “[b]ody corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.”<sup>21</sup> Record and document preservation provisions are also set out in various laws and mostly vary from 5-8 years or permanent preservation.<sup>22</sup>

### *2. Location Tracking*

The 2000 Information Technology Act allows the central government to authorize any agency of the government to monitor and collect data generated, transmitted, received, or stored in any computer source for the purpose of enhancing cyber security and for “identification, analysis and

---

<sup>15</sup> Personal Data Protection Bill, No. 373 of 2019, <https://perma.cc/S9PF-CSSN>.

<sup>16</sup> *The Personal Data Protection Bill, 2019*, PRS Legislative Research, <https://perma.cc/Y6H5-J3T7>.

<sup>17</sup> Personal Data Protection Bill, No. 373 of 2019, § 2(A).

<sup>18</sup> *Id.* § 2(B).

<sup>19</sup> *Id.* § 91(2).

<sup>20</sup> Talwar Thakore & Associates, *supra* note 14.

<sup>21</sup> Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules), 2011, Rule 5(4).

<sup>22</sup> *Period of Preservation of Accounts/Records under Different Laws*, Bombay Chartered Accountants Society, <https://perma.cc/RCV6-STMD>.

prevention of intrusion or spread of computer contaminant in the country.”<sup>23</sup> Procedures and safeguards for monitoring and collecting traffic data under this provision are regulated by the Information Technology Act and the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.<sup>24</sup> These Rules stipulate

who may issue directions for interception and monitoring; how such directions are to be executed; the duration they remain in operation; to whom data may be disclosed; the confidentiality obligations of intermediaries; periodic oversight of interception directions by a Review Committee under the Telegraph Act; the retention of records of interception by intermediaries; and the mandatory destruction of information in appropriate cases.<sup>25</sup>

### III. Electronic Measures to Fight COVID-19 Spread

Both the Union and state governments have launched “a host of coronavirus-related apps over the last few weeks to curb the spread of the pandemic in the country.”<sup>26</sup>

#### A. Aarogya Setu Contact Tracing App

##### 1. How It Works

The official COVID-19 tracking app of the Union government, Aarogya Setu (“Bridge to Health”), was launched in April for Android and iOS users. The app was developed by the National Informatics Centre, which comes under the Ministry of Electronics and IT.<sup>27</sup> The app has reportedly been installed 114 million times with 50 million installs in 13 days and 100 million in 41 days.<sup>28</sup> There does not appear to be any particular legal framework that governs the app apart from a privacy policy and terms of service<sup>29</sup> that have been updated a number of times.<sup>30</sup> Some aspects of its use—for example, mandatory use in certain circumstances—have been included in orders issued under the Disaster Management Act, 2005,<sup>31</sup> which allows the union government

---

<sup>23</sup> Information Technology Act, 2000, § 69B.

<sup>24</sup> Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009, The Gazette of India Extraordinary, pt. II, § 3(i) (Oct. 27, 2009), <https://perma.cc/373K-HESJ>.

<sup>25</sup> Privacy International, *State of Privacy India* (Jan. 29, 2019), <https://perma.cc/BFR3-3FXM>.

<sup>26</sup> Abhik Sengupta, *Government Launches Aarogya Setu COVID-19 Tracker App on Android, iOS*, Gadgets 360 (Apr. 2, 2020), <https://perma.cc/7SEZ-X9RV>.

<sup>27</sup> *Aarogya Setu App: COVID-19 Tracker Launched to Alert You and Keep You Safe*, National Informatics Centre, Ministry of Electronics & IT, <https://perma.cc/44NU-YERK>.

<sup>28</sup> Tushar Burman, *Aarogya Setu, India's Contact-tracing App, Goes Open-source*, FirstPost (May 27, 2020), <https://perma.cc/U3DP-Q7FE>.

<sup>29</sup> Amit Anand Tiwari, *Covid-19: Aarogya Setu Needs Legislative Backing*, Hindustan Times (May 21, 2020), <https://perma.cc/EM4K-NDHX>.

<sup>30</sup> Aditi Agrawal, *Aarogya Setu Updates Privacy Policy, Terms of Service: Reverse Engineering Not Banned, but Function Creep Now Legitimized*, Medianama (May 24, 2020), <https://perma.cc/89JY-6GKE>.

<sup>31</sup> Disaster Management Act, 2005, <https://perma.cc/S3B6-SWM9>.

to issue emergency measures in “unforeseen emergent situations.”<sup>32</sup> According to the Ministry of Electronics and IT, the app is a contact tracing app that uses both Bluetooth and GPS location data technology, using “algorithms and artificial intelligence.” It allows users to assess their own risk of catching the coronavirus and will “calculate this based on their interaction with others.”<sup>33</sup> According to one government FAQ,

[w]hen two registered users come within Bluetooth range of each other, their Apps will automatically exchange unique Digital IDs (DiDs) and record the time and GPS location at which the contact took place. The information that is collected from the User’s App will be securely stored on the mobile device of the other registered user and will not be accessible by such other user. In the event such other registered user tests positive for COVID-19, this information will be securely uploaded from his/her mobile device and stored on the Server. Then this information is used to further carry out the contact tracing and find out all possible persons who may have come in close contact with the person who has tested positive for COVID-19.<sup>34</sup>

The app tries to “determine if the user has been within six-feet of an infected person, by cross-referencing” the pan-India database (referred to as the “Server” in the above quote) of all COVID-19 patients.<sup>35</sup> The app also allows the Department of Health to “inform users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19.”<sup>36</sup>

## 2. Data Collected

When the Aarogya Setu app is registered by a user, the following details are collected: “(i) name; (ii) phone number; (iii) age; (iv) sex; (v) profession; and (vi) countries visited in the last 30 days.”<sup>37</sup> This information is stored on the “back-end Server and it is hashed with a unique digital id (DiD)” that is pushed to the user’s app. The DiD is used to identify the user in all subsequent app-related transactions and will be associated with any data or information uploaded from the app to the database. The user’s location details are also captured and uploaded to the database.<sup>38</sup>

The app collects location data continuously at 15-minute intervals, which is stored on the mobile device and includes a record of all the places the user has been” at those intervals. This information is uploaded to the database along with the user’s DiD,

---

<sup>32</sup> Vidisha Singh, *India’s Aarogya Setu Contact Tracing App – Compromising Privacy in a Pandemic?*, Jurist (May 18, 2020), <https://perma.cc/2A4X-VKRR>.

<sup>33</sup> Press Release, Ministry of Electronics & IT, Government of India Launches ArogyaSetu App to Track Covid 19 Infection (Apr. 2, 2020), <https://perma.cc/GW6E-56NK>.

<sup>34</sup> Government of Assam, *Frequently Asked Questions on Aarogya Setu App*, Q3, <https://perma.cc/AN8L-2HBA>.

<sup>35</sup> Shubhang Gopal, *Aarogya Setu: 9 Things You Must Know before Downloading the Contact Tracing App*, The Indian Express (May 10, 2020), <https://perma.cc/7X79-WA5T>.

<sup>36</sup> Arogya Setu – Govt. of India Initiative to Fight against Corona Virus – Bluetooth Based COVID-19 Tracker Mobile Application, District Court, <https://perma.cc/DK4J-LQRU>.

<sup>37</sup> Government of Assam, *supra* note 34, Q2.

<sup>38</sup> *Id.*

- (i) if the person tests positive for COVID-19; and/or
- (ii) if the persons self-declared symptoms indicate that they are likely to be infected with COVID-19; and/or
- (iii) if the results of a self-assessment test are either *yellow* or *orange*. This information will not be uploaded to the Server if you are not unwell or if the result of your self-assessment test is *green*.<sup>39</sup>

Yellow or orange signifies “a high level of risk for contracting COVID-19.”<sup>40</sup>

### 3. Persons Required to Download the App

When the app was launched in early April its use was considered voluntary but became mandatory for persons in certain containment zones and for public and private sector employees in May.

On May 1 the Union Home Secretary issued new guidelines<sup>41</sup> under section 10(2)(I) of the Disaster Management Act, 2005,<sup>42</sup> that designated districts into Red, Orange, and Green Zones based on risk. Green Zones are those that had no cases as of the date of the guidelines or within the previous 21 days; Red Zones were designated based on the “total number of active cases, doubling rate of confirmed cases, extent of testing and surveillance feedback.”<sup>43</sup> Orange zones are those that do not fit the criteria for the Green or Red designations.

Within the Red and Orange Zones authorities may set up Containment Zones or areas for more intense surveillance, such as contact tracing, home or institutional quarantining, and house-to-house surveillance by special teams. According to the guidelines, “[t]he local authority shall ensure 100% coverage of [the] Aarogya Setu app among the residents of Containment Zones.” The guidelines also required all employees in the public and private sector to use the Aarogya Setu app, with the head of each organizations being responsible for ensuring use by all employees. However, after criticisms from privacy advocates, it appears the government is easing its position on mandatory use of the app in offices: On May 17, the Ministry of Home Affairs issued new guidelines that stated, “[w]ith a view to ensur[ing] safety in offices and work places, employers on [a] *best effort basis* should ensure that the application is installed by all employees having compatible mobile phones.”<sup>44</sup> The new guidelines also stipulate that “[d]istrict authorities may advise individuals to install the Aarogya Setu application on compatible mobile phones and regularly update their health status on the app. This will facilitate timely provision of medical

---

<sup>39</sup> Id. Q4.

<sup>40</sup> Manavi Kapur, *The Indian Government Fixes Privacy Flaws in Its Coronavirus App*, Quartz India (Apr. 16, 2020), <https://perma.cc/6EN2-SYKB>.

<sup>41</sup> Government of India, Ministry of Home Affairs, Order No. 40-3/2020-DM-I(A) (May 1, 2020), <https://perma.cc/6SW7-779L>.

<sup>42</sup> Disaster Management Act, 2005, § 10(2)(I).

<sup>43</sup> *New Guidelines See Home Ministry Ease Up on Compulsory Use of Aarogya Setu in Offices*, The Wire (May 17, 2020), <https://perma.cc/JC3U-5JRR>.

<sup>44</sup> Press Release, Extension of Lockdown up to May 31, 2020, Ministry of Home Affairs (May 17, 2020), <https://perma.cc/CA6Y-W56S> (emphasis added).

attention to those individuals who are at risk.”<sup>45</sup> Another set of guidelines were issued on May 30, 2020, for the phased reopening of the country outside containment zones, which included the same provisions on the use of the app.<sup>46</sup> Noida, a suburb of the capital, Delhi, had made it “compulsory for all residents to have the app, saying they can be jailed for six months for not complying.”<sup>47</sup> However, the order was reversed on May 20 “after some residents submitted a representation to the Additional Deputy Commissioner (Law and Order) challenging the directive’s legal basis.”<sup>48</sup> The Ahmedabad Municipal Corporation (AMC) has “also made it mandatory for personnel engaged in delivery of grocery and food item to download the app on their mobile phones. The revised guidelines issued by the Union Health ministry for home isolation of very mild/pre-symptomatic cases also call for downloading the app on the mobile and made it clear it should remain active at all times (through Bluetooth and Wi-Fi).”<sup>49</sup> Since the new federal guidelines removing the mandatory requirement were issued some states such as Uttar Pradesh have still made the use of the app mandatory and are imposing a fine for not doing so.<sup>50</sup>

In addition, some private companies such as Zomato and Xiaomi have made it mandatory for employees to download the app.

According to guidelines for international arrivals, “[a]ll passengers shall be advised to download Arogya Setu app on their mobile devices.” Those who for “exceptional and compelling reasons such as cases of human distress, pregnancy, death in [the] family, serious illness and parent(s) accompanied by children below 10 years, as assessed by the receiving states,” cannot carry out an institutional quarantine are permitted to home quarantine for 14 days but are required to use the Aarogya Setu app.<sup>51</sup> Union guidelines for domestic travel, including air and train, also advise passengers to download the Arogya Setu app on their mobile devices.<sup>52</sup> On May 25 domestic flights had resumed operations and the use of the app was made mandatory. According to a news report “[a]ll passengers, except children below 14 years, must be registered on the Aarogya

---

<sup>45</sup> Id.

<sup>46</sup> Government of India, Ministry of Home Affairs, MHA Order No. 40-3/2020-DM-I(A), (May 30, 2020), <https://perma.cc/2TX9-W7UL>.

<sup>47</sup> Andrew Clarence, *Aarogya Setu: Why India’s Covid-19 Contact Tracing App Is Controversial*, BBC News (Delhi) (May 15, 2020), <https://perma.cc/K5TY-4TYZ>.

<sup>48</sup> Neerad Pandharipande, *‘Indian Govt Should Convince Public on Aarogya Setup’s Efficacy rather than Forcing It on Them’: Cybersecurity Expert Elliot Alderson Tells Firstpost*, Firstpost (May 23, 2020), <https://perma.cc/A6S2-MRZ9>.

<sup>49</sup> *Covid-19 Contact Tracing App Aarogya Setu Has Alerted 1.4 Lakh Users: Official*, LiveMint (May 12, 2020), <https://perma.cc/AQ2S-QT6M>.

<sup>50</sup> *Government Climbs Down on Aarogya Setu by Removing Mandatory Provision*, LiveMint (May 30, 2020), <https://perma.cc/F7UH-GVVZ>.

<sup>51</sup> Government of India Ministry of Health and Family Welfare Guidelines for International Arrivals (May 24, 2020), <https://perma.cc/HWV6-GL8L>.

<sup>52</sup> Government of India Ministry of Health and Family Welfare Guidelines for Domestic Travel (Air/Train/Inter-state Bus Travel) (May 24, 2020), <https://perma.cc/CVD9-BGNL>.

Setu app and it will be verified at the entry gate of the terminal building.”<sup>53</sup> Another news report noted that “passengers ‘not showing Green’ on Aarogya Setu app will not be allowed to enter into the airports.”<sup>54</sup> The Aarogya Setu app was also made mandatory for train passengers in the country.<sup>55</sup>

#### 4. Government Use

According to the government, the personal information collected upon registration will

only be used by the Government of India in anonymized, aggregated datasets for the purpose of generating reports, heat maps and other statistical visualisations for the purpose of the management of COVID-19 in the country or to provide you general notifications pertaining to COVID-19 as may be required. Your DiD will only be co-related with your personal information in order to communicate to you the probability that you have been infected with COVID-19 and/or to provide persons carrying out medical and administrative interventions necessary in relation to COVID-19, the information they might need about you in order to be able to do their job.<sup>56</sup>

In the event a person has tested positive for COVID-19, the information collected is used to map the places the person has visited over the past 14 days “in order to identify the locations that need to be sanitised and where people need to be more deeply tested and identify emerging areas where infection outbreaks are likely to occur.”<sup>57</sup> In late May the privacy policy and terms of service were updated so that “location data for the last 30, not 14, days will now be pinged to the server if a user comes in close proximity of an infected person.”<sup>58</sup> Other data retention requirements are as follows:

All traced personal information shared between users, risk assessment tests and location information will be retained on the mobile device for a period of 30 days from the date of collection. All personal information uploaded to the Server will, to the extent that such information relates to people who have not tested positive for COVID-19, will be purged from the Server 45 days after being uploaded.

Persons who have tested positive for COVID-19 will be purged from the Server 60 days after such persons have been declared cured of COVID-19.<sup>59</sup>

There is an exception for “anonymized/ aggregated datasets” generated by the “personal data of registered users of the App or any reports, heat maps or other visualization created using such

---

<sup>53</sup> *Text Bulletin Details: Morning News*, All India Radio (May 25, 2020), <https://perma.cc/LZ23-PFVE>.

<sup>54</sup> Prabhakar Thakur, *Aarogya Setu App Mandatory for Airline Passengers, No Entry Without ‘Green’ Status*, NDTV’s Gadgets360 (May 21, 2020), <https://perma.cc/HV5M-D84K>.

<sup>55</sup> *Id.*

<sup>56</sup> Government of Assam, *supra* note 34, Q5.

<sup>57</sup> *Id.* Q6.

<sup>58</sup> Aditi Agrawal, *supra* note 30.

<sup>59</sup> Tripti Dhar, *Aarogya Setu – Carrying Your Privacy in Your Hands?*, PrivSec Report (May 29, 2020), <https://perma.cc/T6NJ-XE7T>.

datasets, the medical reports, diagnoses or other medical information generated by medical professionals in the course of treatment will be retained.”<sup>60</sup> (For more on this topic see subsection (f), below.)

### 5. Privacy Concerns

As per the head of this project, Arnab Kumar, the app was built to the standards of the draft data privacy bill, which is currently in the country’s parliament, and “access to the data it collects is strictly controlled.”<sup>61</sup> Such data “is encrypted using state-of-the-art technology and stays secure on the phone till it is needed for facilitating medical intervention.”<sup>62</sup>

However, when the app was first introduced and even now, political leaders, experts and human rights organizations have expressed several criticisms and highlighted a number of privacy concerns. Rahul Gandhi, a prominent MP and former leader of the opposition Indian National Congress is reportedly among those who are critical of the app, arguing that it has “no institutional oversight” and raises “serious data security and privacy concerns.”<sup>63</sup>

In a blog post on *Medium* on May 6, French ethical hacker Robert Baptiste, who goes by the name Elliot Alderson, observed a number of security concerns and flaws with the app, including that it was “possible to modify the location of the app, which can enable one to identify how many people are unwell or infected even without being physically present in their vicinity.”<sup>64</sup> However, he stated that in a subsequent version of the app, “this issue was ‘fixed silently’ by the developers.”<sup>65</sup> In mid-May, a software engineer in the city of Bangalore, growing concerned that installing the app was slowly becoming mandatory in India, hacked the app so it was “collecting no data but still flashing a green badge declaring that the user was at low risk of infection.”<sup>66</sup>

Experts have noted that India is currently the only democratic nation in the world that had made the coronavirus tracking app mandatory for a significant portion of its population.<sup>67</sup> Some observers have also criticized the app on the ground that it “stores both location data and requires constant access to the phone’s Bluetooth,” which makes it “invasive from a security and privacy viewpoint.”<sup>68</sup> Until recently, Aarogya Setu was not open source, so the app was also criticized because it could not be “audited for security flaws by independent coders and researchers.”

---

<sup>60</sup> Id.

<sup>61</sup> *Aarogya Setu: Lack of Data Privacy Laws, Transparent Policies Make App Worrisome, Say MIT Researchers*, First Post (May 11, 2020), <https://perma.cc/E3S5-TUQE>.

<sup>62</sup> Id.

<sup>63</sup> Id.

<sup>64</sup> Pandharipande, *supra* note 48.

<sup>65</sup> Id.

<sup>66</sup> Pranav Dixit, *India’s Contact Tracing App Is All But Mandatory. So This Programmer Hacked It So that He Always Appears Safe*, BuzzFeed News (May 12, 2020), <https://perma.cc/9J5X-PZ4W>.

<sup>67</sup> Patrick Howell O’Neill, *India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy*, MIT Technology Review (May 7, 2020), <https://perma.cc/Q5ZS-VZSL>.

<sup>68</sup> Clarence, *supra* note 47.

Experts felt that “[m]ore transparency could lead to ‘potentially improved security as it would be open to scrutiny from third-party experts,’ ” according to news reports. Experts also noted that the app used “a static ID and is more easily amenable to de-anonymisation i.e. identifying the owner, in case someone else gets hold of the DID, because there is only a single layer of encryption.”<sup>69</sup> On May 7, the *MIT Technology Review* highlighted a number of similar concerns including the absence of a national data protection law.<sup>70</sup> This has raised the concern that the use of the app and its data collection has an “ambiguous legal basis.”<sup>71</sup>

Though MIT researchers had given the app 2 out of 5 stars in their review, they later downgraded the rating to one star, according to *The Quint*. “[T]he app lost more points on the parameters of ‘data minimisation’ which means the app is collecting more data than needed for the app to work,” the article said, citing a *Times of India* report.<sup>72</sup> One recent report highlights certain examples of this “non-adherence to the principle of data minimization”:

- The personal information collected includes detail of the individual’s profession[,] which has no direct relation with the effective use of the App
- Proximity data should be used (as opposed to location tracking)<sup>73</sup>

Concern has also been expressed over the lack of definition of collected “anonymised data” and conflicting reports over how long such data can be retained.<sup>74</sup> There is also concern that health surveillance, which is “a necessity in a pandemic,” “can soon evolve into mass surveillance.”<sup>75</sup>

On May 26 the Ministry of Electronics and IT announced that the software has been made open source. “The source code for the Android version of the application is available for review and collaboration,” the Ministry said, and an “iOS version of the application will be released as open source within the next two weeks and the server code will be released subsequently. Almost 98% of Aarogya Setu Users are on Android platform.”<sup>76</sup>

---

<sup>69</sup> Anuj Srivas, *Aarogya Setu: Six Questions for the Centre on the COVID-19 Contact Tracing App*, *The Wire* (May 4, 2020), <https://perma.cc/JDD2-QYEA>.

<sup>70</sup> O’Neill, *supra* note 67.

<sup>71</sup> Tripti Dhar, *supra* note 59.

<sup>72</sup> *MIT Researchers Downgrade Aarogya Setu App to One Star in Review*, *The Quint* (May 22, 2020), <https://perma.cc/EF6B-HFCA>.

<sup>73</sup> Tripti Dhar, *supra* note 59.

<sup>74</sup> *Id.*

<sup>75</sup> Anand Venkatanarayanan, *Op-ed, Covid-19: How the Aarogya Setu App Handles Your Data*, *BloombergQuint* (Apr. 17, 2020), <https://perma.cc/Q5DN-URWE>.

<sup>76</sup> Press Release, Ministry of Electronics & IT, *Aarogya Setu Is Now Open Source* (May 26, 2020), <https://perma.cc/CCD6-GDWZ>.

## 6. Aarogya Setu Data Access and Knowledge Sharing Protocol

On May 11, 2020, in response to the many privacy concerns, the Ministry of Electronics and IT published through a notification the Aarogya Setu Data Access and Knowledge Sharing Protocol.<sup>77</sup> The Protocol was issued by the chairperson of the “empowered group on technology and data management,” “which is one of the 11 empowered groups created by the National Executive Committee of the National Disaster Management Authority”<sup>78</sup> to “provide legal safeguards for the operation of the Aarogya Setu mobile application.”<sup>79</sup> Some of the key highlights of the protocol include the following:

**1. Data points collected from the individuals:** ‘Response data’ collected from people using the Aarogya Setu app will have the following data points-

**1.1 Demographic data**, which includes the name, mobile number, age, gender, profession and travel history of the person;

**1.2 Contact data** i.e. data about another person that a given person has come in close proximity with, including the duration of the contact, the proximate distance between the individuals and the geographical location at which the contact occurred;

**1.3 Self-assessment data** i.e. the responses provided by the person to the self-assessment test on the Aarogya Setu app, and

**1.4 Location data** i.e. data about the geographical position of an individual in latitude and longitude.

**2. Implementing agency:** MeitY will be responsible for overall implementation of the protocol. The National Informatics Centre (“NIC”) under the MeitY will collect, process and manage ‘response data’.

**3. Application of collection limitation, purpose limitation and period limitation principles:** The Protocol requires that- (a) the response data to be collected and its purpose must be specified in the privacy policy of the Aarogya Setu app; (b) the data must be used in a ‘necessary and proportionate’ manner only for the purpose of framing appropriate health responses and to improve such responses; (c) the contact data, location data and self-assessment data will not be retained beyond a period of 180 days, unless extended by the EG; (d) demographic data will be stored till the Protocol is in force i.e. 180 days, unless extended by the EG; in case a person requests her data to be deleted, then it must be deleted within 30 days of her request.

**4. Third party sharing of response data:**

**4.1 Sharing of personal response data:** It can be shared with- (a) the Ministry of Health and Family Welfare; (b) Health departments of the state/union territory/local government, NDMA and state disaster management authorities (“SDMAs”), and any other department/ministry/public health institution of the central/state/local

---

<sup>77</sup> Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020, <https://perma.cc/WPH6-S6CY>.

<sup>78</sup> Ikigai Law, *A Summary of the Aarogya Setu Data Access and Knowledge Sharing Protocol* (May 11, 2020), <https://perma.cc/MLH8-XPLD#acceptLicense>.

<sup>79</sup> Vidhi Centre for Legal Policy, *Aarogya Setu’s Data Access and Knowledge Sharing Protocol, 2020* (May 11, 2020), <https://perma.cc/V4J7-9G5X>.

government, but only if the data is necessary to frame/implement an appropriate health response.

**4.2 Sharing of de-identified response data:** It can be shared with the ministry/department/public health institution of the central/state/union territory/local government, NDMA and SDMA, where the data needs to be shared for framing/implementation of a critical health response. De-identified data means data which has been stripped of personally identifiable data.

**4.3 Maintaining records of third parties:** NIC will, to a reasonable extent, maintain a list of agencies with whom response data is shared, and record details such as the purpose of sharing, categories of data shared etc.

**4.4 Application of collection limitation, purpose limitation and period limitation principles:** These principles will also apply to third-party sharing of response data. The data must be permanently deleted in all circumstances after 180 days from the date on which it is accessed. Any ministry/department/public health institution with whom the data is shared must implement reasonable security practices and procedures under the Information Technology Act, 2000.

**4.5 Further sharing of response data:** Any ministry/department/public health institution shall further share response data only when it is strictly necessary to frame/implement appropriate health responses. It must ensure compliance of the Protocol by other such entities with whom data is further shared. Such entities can be subject to an audit and review of their usage of response data by the central government.

## **5. Sharing of response data for research purposes:**

**5.1 Availability of response data to Indian universities and research institutions:** Such universities and research institutions must be registered in India. The response data provided to them must be subject to 'hard anonymisation' (as opposed to de-identification). The anonymisation protocols for 'hard anonymisation' will be developed by an expert committee appointed by the Principal Scientific Advisor of the Indian government.

**5.2 Data access subject to approval of expert committee:** An institution will need to submit a request to the PSA-appointed expert committee to seek access to response data. The expert committee can approve such request only if it is satisfied that the access is sought for the purposes of statistical, epidemiological, scientific or any other form of academic research. It can also specify additional terms for accessing the data.

**5.3 Reverse anonymisation/re-identification banned:** If the institution, irrespective of its intention, conducts reverse anonymisation or re-identification of the response data, its access rights will be terminated. It will also be subject to penalties under the applicable laws.

**5.4 Further sharing of response data:** Institutions can share the anonymised response data with any other institution, provided that- (a) the sharing is for the purpose approved by the expert committee; (b) there is a contract between both parties, mentioning particulars such as nature of data shared, purpose of sharing data, the duration of such sharing and other details specified by the expert committee. The institution must provide a copy of the contract to the expert committee.

**6. Penalties:** Any violation of the protocol will be punishable under the Disaster Management Act, 2005 and any other applicable legal provisions.

**7. Termination of protocol:** The Protocol will be in force for 6 months i.e. till 11 November 2020. However, its enforcement period may be extended upon a review by the EG.<sup>80</sup>

The Protocol has still come under criticism by privacy groups for not being legally binding; lacking a complaint mechanism for violations of the protocol; not providing a process by which to request deletion of data; not going far enough with the privacy safeguards, particularly in regard to the anonymization of data and data sharing with third parties; and including a sunset clause for the protocol but not for the app itself.<sup>81</sup>

The privacy policy and terms of service have been updated to address some of these concerns including updates as of late May by which the government may now be held liable for “unauthorised access to your information or modification thereof” and removal of the ban on reverse engineering of the app.<sup>82</sup>

### 7. *Judicial Response*

On May 12, the Kerala High Court “refused to pass an interim order to stay the mandatory downloading of ‘Arogya Setu’ app on employees’ phones and sought a statement from the central government on data safeguards of the app being developed by the National Informatics Centre,” the *Hindustan Times* reported.<sup>83</sup>

### **B. State-Level Apps**

According to one news report several states and municipalities in India have developed their own COVID-19 contact tracing, home quarantine, and information advisory apps over the past two months, with most of these having been developed by private companies “that have unprecedented access to sensitive patient data with little liability in case of a breach.”<sup>84</sup> The *Indian Express* highlighted a number of privacy concerns for these apps:

“Most of these apps have been developed by private companies and they have access to all the data while the liability provisions in case of breach are very vaguely worded, sometimes even asking the user to completely wave the liability and accountability of the service provider in case of data breach or loss,” Salman Waris, founder & partner at TechLegis Advocates & Solicitors said.

...

---

<sup>80</sup> Ikigai Law, *supra* note 78.

<sup>81</sup> Vakasha Sachdev, *Does Govt’s New Data Protocol Address Concerns over Aarogya Setu?*, *The Quint* (May 13, 2020), <https://perma.cc/KM2E-R8BR>.

<sup>82</sup> Aditi Agrawal, *supra* note 30.

<sup>83</sup> *Kerala High Court Refuses Stay on Mandatory Use of Arogya Setu App*, *Hindustan Times* (May 12, 2020), <https://perma.cc/XBE9-2AS8>.

<sup>84</sup> Aashish Aryan, *Coronavirus Tracking Apps: States on Launching Spree; Privacy Concerns over Unfettered Access Raised*, *The Indian Express* (May 20, 2020), <https://perma.cc/6VNA-U236>.

The permissions sought by the most of these contact tracing apps and home quarantine portals is another security issue which must be paid attention to, cyber-security experts said. "Excessive permissions are required by applications that undertake tracing and surveillance through capturing information from different internal broadcasts from components of the device. In some cases, apps which are only informative and intended to issue advisories have sought permissions for location, photos, storage and camera," a SFLC spokesperson said.

For example, Telangana's app 'T-Covid-19' developed by Quantela Inc, a US-based company, aims only to "provide citizens with preventive care information and other government advisories". "However, for an information and advisory serving app, it asks for several permissions which include monitoring components including 'extra location provider commands' which pertains to state of location," legal cyber-security advisory group Software Freedom Law Centre said.

A similar COVID-19 dashboard, developed by the Madhya Pradesh Agency for Promotion of Information Technology was taken down after Robert Baptiste, a French ethical hacker who used the pseudonym Elliot Alderson on Twitter, pointed out flaws and showed that it violated the basic personal privacy laws. The quarantine and information vending apps of Punjab and Kerala, similarly seek more information than is necessary for these programs to function, experts said.

Punjab's information vending app 'Cova Punjab' seeks to have full network access and even view network connections. The app even seeks to pair with Bluetooth devices in its vicinity without express approval of the device holder, which can be extremely problematic and invasive, a cyber-law expert said. "The problem is that all the state apps are using Centre's Aarogya Setu framework and foundation as the starting point. That will not be a correct approach," Supreme Court lawyer and cyber-law expert Pavan Duggal told *The Indian Express*.<sup>85</sup>

In Uttar Pradesh, the "Chikitsa Setu" app was launched to "ensure safety of COVID-19 frontline workers," with the objective "to provide official training content, spread awareness, and ensure safety of healthcare workers, sanitation workers and police personnel who are actively involved to protect citizens, breaking the chain of COVID-19 infection."<sup>86</sup>

---

<sup>85</sup> Id.

<sup>86</sup> UP CM Yogi Adityanath Launches 'Chikitsa Setu' App to Ensure Safety of Frontline Workers, eHealth Network (May 20, 2020), <https://perma.cc/UDJ5-9QVW>.

# Japan

Sayuri Umeda  
Senior Foreign Law Specialist

**SUMMARY** Privacy and private information are protected in Japan, including a person's location information. The location of a person who communicates via a mobile device is treated as information relating to the secrecy of communication that the Constitution of Japan protects. Telecommunications carriers can collect such information only when a user has consented, when a judge has issued a warrant, or when there is a legally justifiable cause. Law enforcement cannot track a suspect by secretly attaching a GPS device to the suspect's belongings without a warrant issued by a judge. When the government conducts an epidemiological investigation, a health center official tracks the past locations of the person. If the person refuses to cooperate with the investigation, the investigation cannot be conducted.

The government, in cooperation with information technology organizations, has tried to utilize an infection route tracking application software on mobile devices. The government expects to launch the system in June 2020.

## I. Introduction

As of May 22, 2020, according to the Ministry of Health, Labour and Welfare (MHLW), the number of confirmed COVID-19 cases is 16,513 in Japan, a rate of 131 per million. The number of deaths is 796.<sup>1</sup> It is "among the lowest death rates in the world."<sup>2</sup>

Most people have smartphones in Japan. As of 2018, 95.7% of households owned mobile information and communication devices, according to a survey by the Ministry of Internal Affairs and Communications (MIC). Among them, the percentage of smartphones was 79.2%.<sup>3</sup> A more recent survey by a private institution found that the percentage of smartphones among mobile phones reached 88.9% in January 2020. Especially among people who are younger than 50 years of age, almost everyone has a smartphone.<sup>4</sup>

---

<sup>1</sup> Press Conference, Minister Kato Katsunobu, Ministry of Health, Lab. & Welfare (MHLW), About Coronavirus Disease 2019 (COVID-19) (May 22, 2020), <https://perma.cc/W2N6-DAQG>.

<sup>2</sup> William Sposato, *Japan's Halfhearted Coronavirus Measures Are Working Anyway*, Foreign Pol'y (May 14, 2020), <https://perma.cc/N9PQ-JRRE>.

<sup>3</sup> MIC, *Information and Communications in Japan: White Paper 2019 44* (2019), <https://perma.cc/UC4T-2BDE>.

<sup>4</sup> スマホ比率 88.9%に：40代以下は9割以上がスマホ所有 [*Smartphone Ratio Reached 88.9%: More than 90% of People Under 50 Years Old Own Smartphones*], Mobile Soc'y Res. Inst. (Mar. 17, 2020), <https://perma.cc/QF9L-HK3Q>.

Regarding willingness to share personal information, it appears that the Japanese are reluctant to do so. According to an international study, the Japanese were the least willing overall to share information with organizations online among people in the studied countries.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

There is a no legal provision that explicitly protects the right to privacy, however, the right to privacy has been recognized by the courts.<sup>6</sup> Courts and scholars have found the legal basis of the right to privacy in the right to the pursuit of happiness that is guaranteed under the Constitution.<sup>7</sup> Regarding personal information and privacy, in 2003, the Supreme Court decided that even basic information about a person, such as names, addresses, and telephone numbers, can be protected as private, depending on the circumstances. In that case, a university had disclosed such information about applicants for attendance at a foreign leader's lecture to the police, without their prior consent. The Court decided the disclosure constituted a tort.<sup>8</sup>

There are three laws regulating the handling of personal information. The Act on the Protection of Personal Information (APPI) applies to the private sector.<sup>9</sup> The Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO) applies to government agencies.<sup>10</sup> The Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc., (APPIHIAA) applies to independent administrative agencies.<sup>11</sup> These laws aim to protect personal information while they set rules to properly utilize personal information for the development of relevant industries.<sup>12</sup> These laws define personal information as follows:

---

<sup>5</sup> KPMG, *Crossing the Line: Staying on the Right Side of Consumer Privacy* 23 (2016), <https://perma.cc/5MHN-7GW2>.

<sup>6</sup> Hiromitsu Naito, モデル小説における表現の自由とプライバシーの権利 [Freedom of Expression and Right to Privacy on Novels Based on Real Person], 専修法学論集 [107 Specialized Law Stud. Collection 1, 6-9 (2009)], <https://perma.cc/JV6K-782W>.

<sup>7</sup> Id. and Const. of Japan (1946), art. 13, <https://perma.cc/3Y8U-CL9S>.

<sup>8</sup> 2002 (Ju) 1656, 57(8) Minshu 973 (S. Ct. Sept. 12, 2003). A summary of the case is available on the Courts in Japan website at <https://www.courts.go.jp/english/index.html>.

<sup>9</sup> 個人情報の保護に関する法律 [Act on the Protection of Personal Information] (APPI), Act No. 57 of 2003 (May 30, 2003), amended by Act No. 16 of 2019 (Reiwa), <https://perma.cc/548A-V32A> (unofficial translation as amended by Act No. 65 of 2015).

<sup>10</sup> 行政機関の保有する個人情報の保護に関する法律 [Act on the Protection of Personal Information Held by Administrative Organs] (APPIHAO), Act No. 58 of 2003 (May 30, 2003), last amended by Act No. 37 of 2019 (Reiwa), <https://perma.cc/3QTP-QHQ4> (unofficial translation as amended by Act No. 51 of 2016).

<sup>11</sup> 独立行政法人等の保有する個人情報の保護に関する法律 [Act on the Protection of Personal Information Held by Independent Administrative Agencies] (APPIHIAA), Act No. 59 of 2003 (May 30, 2003), amended by Act No. 37 of 2019 (Reiwa), <https://perma.cc/E773-EY7M> (unofficial translation as amended by Act No. 51 of 2016).

<sup>12</sup> APPI art. 1, APPIHAO art. 1, and APPIHIAA art. 1.

Information about a living person that

- contains a name, date of birth, or other descriptions (any matters stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record) whereby a specific individual can be identified, including those which can be readily collated with other information and thereby identify a specific individual; and
- contains an individual identification code that can identify a specific person, user, purchaser, or recipient.<sup>13</sup>

In general terms, anyone who handles personal information must disclose the purpose of the collection and must not disclose it to a third party without the consent of the individual unless disclosure is allowed by law.<sup>14</sup> When personal information is processed so that it cannot identify a person (anonymously processed information), a person who handles personal information can provide the anonymously processed information to a third party without the consent of the subjects of the information if the person follows the measures set forth by the APPI, APPIHAO, and APPIHIAA.<sup>15</sup>

## B. Data Retention and Location Tracking

### 1. APPI, APPIHAO, and APPIHIAA

When the location information of a person can enable a third party to identify that person, the APPI, APPIHAO, and APPIHIAA treat it as personal information. If location information is anonymized, the information can be transferred and utilized under certain conditions.<sup>16</sup>

### 2. Guidelines for Telecommunications Carriers

The Constitution states that the secrecy of any means of communication must not be violated.<sup>17</sup> The Telecommunications Business Act also states that “[t]he secrecy of communications handled by a telecommunications carrier must not be violated.”<sup>18</sup> Because the telecommunications business deals with this right to protection of the secrecy of communications, the handling of personal information by telecommunications carriers requires special consideration. The MIC has issued the Guidelines for Personal Information Protection in Telecommunications Business that

---

<sup>13</sup> APPI art. 2, para. 1 & 2; APPIHAO art. 2, para. 2 & 3; APPIHIAA art. 2, para. 2 & 3.

<sup>14</sup> Taro Komukai, ICT 技術と位置情報に関する制度の動向 [*Development of System for ICT Technology and Location Information*], 日本データ通信[Nippon Data Comm. (July 1, 2017)], <https://perma.cc/HKS5-G4VD>.

<sup>15</sup> APPI arts 36 & 37, APPIHAO art. 44-2, and APPIHIAA art. 44-2.

<sup>16</sup> Komukai, *supra* note 14.

<sup>17</sup> Const. art. 21, para. 2.

<sup>18</sup> 電気通信事業法 [Telecommunications Business Act], Act No. 86 of 1984, amended by Act No. 5 of 2019 (Reiwa), art. 4, <https://perma.cc/LL3T-AAYM> (unofficial translation, as amended by Act No. 26 of 2015).

telecommunications carriers must comply with regarding the proper handling of personal information. MIC updates the Guidelines every few years.<sup>19</sup>

The Guidelines state that telecommunications carriers may collect personal information relating to the right to secrecy of communication only when the subject person has agreed or when there is justifiable cause for noncompliance with the law.<sup>20</sup> The location information of mobile telecommunication device users is private information. Among other things, information about a device user's terminal base or wifi access point is information that relates to the secrecy of communications.<sup>21</sup> The Guidelines state that telecommunications carriers can collect the location information of mobile communication devices when it is necessary for the telecommunications carrier's business or when there is justifiable cause for noncompliance with the regulation.<sup>22</sup> A telecommunications carrier can provide a third party with the location information of a holder of a mobile communication device in the following cases: The customer has consented to it in advance, a judge issued a warrant for it, or there are other justifiable causes for noncompliance with the law.<sup>23</sup>

In addition, telecommunication carriers can provide a third party with the location information of a telecommunication device without customers' consent when the life or body of the holder of the device is likely in danger.<sup>24</sup>

### 3. Criminal Investigation

Law enforcement used Global Positioning System (GPS) devices to investigate suspects. The police believed tracking suspects with a GPS device during a criminal investigation could be allowed as a non-compulsory measure.<sup>25</sup> However, the Supreme Court decided in 2017 that the police need a warrant issued by a judge to secretly track the location of a suspect's car.<sup>26</sup> The Court said it is a method of investigation that allows the police to encroach upon an individual's private sphere against the person's reasonably inferred desire, enabling an invasion of privacy.<sup>27</sup>

---

<sup>19</sup> 電気通信事業における個人情報保護に関するガイドライン [*Guidelines for Personal Information Protection in Telecommunications Business*], MIC, <https://perma.cc/E2D4-3MFM>.

<sup>20</sup> 電気通信事業における個人情報保護に関するガイドライン [*Guidelines for Personal Information Protection in Telecommunications Business*], MIC Notification No. 152 (Apr. 18, 2017), amended by MIC Notification No. 297 (Sept. 14, 2017), art. 7, para. 3, <https://perma.cc/Q9J5-ZZ84>.

<sup>21</sup> 緊急時等における位置情報の取扱いに関する検討会, 位置情報プライバシーレポート [*Report on Privacy and Location Information 6-9*] MIC (July 2014)], <https://perma.cc/GTR4-39JT>.

<sup>22</sup> Id. art. 35, para. 1.

<sup>23</sup> Id. art. 35, para. 2.

<sup>24</sup> Id. art. 35, para. 5.

<sup>25</sup> Code of Criminal Procedure, Act No. 131 of 1948, amended by Act No. 63 of 2019 (Reiwa), art. 197, <https://perma.cc/L3S7-AM76> (unofficial translation as amended by Act No. 74 of 2011).

<sup>26</sup> 2016 (A) 442, Keishu 71-3 (S. Ct. Mar. 15, 2017). A summary of the case is available on the Courts in Japan website.

<sup>27</sup> Id. See also Const. art. 35.

#### 4. Infectious Disease Prevention Act

Under the Infectious Disease Prevention Act, when a prefectural governor deems it necessary to prevent or monitor the outbreak of an infectious disease or investigate the cause of outbreaks, the governor may direct prefecture officials to question the patients, suspected disease carriers or asymptomatic carriers of certain diseases and to carry out necessary investigations.<sup>28</sup> When the Minister of MHLW deems it urgently necessary for the purpose of preventing the outbreak or spread of an infectious disease, the Minister may direct relevant officials of the MHLW to do the same.<sup>29</sup> Under these provisions, local health centers conduct an epidemiological investigation. Health centers ask patients where they visited, among other things.<sup>30</sup> However, there is no provision in the Act to force the patients to answer the questions. In a recent news article, it was reported that those people who refused to answer questions made the investigation of transmission routes difficult.<sup>31</sup>

### III. Electronic Measures to Fight COVID-19 Spread

#### A. Infection Route Tracking Application Software

The government has formed the Anti-COVID-19 TECH Team (ACTT), which examines the utilization of information technology and various data to counter COVID-19 and adopt IT measures while receiving assistance from IT companies. ACTT had its first meeting on April 6, 2020.<sup>32</sup> The government decided on April 7, 2020, to develop an infection route tracking application software, modeled on TraceTogether in Singapore, as a measure against the spread of COVID-19 infections.<sup>33</sup> On May 8, 2020, the government decided to move jurisdiction over the

---

<sup>28</sup> 感染症の予防及び感染症の患者に対する医療に関する法律 [Act on the Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases](Infectious Disease Prevention Act), Act No. 114 of 1998, amended by Act No. 115 of 2014, art. 15, para. 1, <https://perma.cc/H2HA-BGEW> (unofficial translation).

<sup>29</sup> Id. art. 15, para. 2.

<sup>30</sup> 国立感染症研究所 感染症疫学センター [Infectious Diseases Surveillance Center, National Institute of Infectious Diseases], 新型コロナウイルス感染症患者に対する積極的疫学調査実施要領 [Guidelines for Active Epidemiological Surveys on New Coronavirus Infections 1] (Apr. 20, 2020), <https://perma.cc/MH3V-6WMS>.

<sup>31</sup> 「調査の電話に出てくれない」感染拡大の若年層、追跡拒否のケースも [*'They do not answer phone calls': Infection Expanded Among Young, Some Refuse Tracking of Transmission Routes*], Yomiuri (Apr. 5, 2020), <https://www.yomiuri.co.jp/medical/20200405-OYT1T50044/>.

<sup>32</sup> 新型コロナウイルス感染症の拡大防止対策に資するIT活用について [Regarding Utilization of IT that Contributes to Measures Against Spread of Novel Corona Virus Disease Material No. 1 for ACTT Kick-off Meeting] (Apr. 6, 2020), Gov't Chief Info. Off., <https://perma.cc/M8EW-HQH5>.

<sup>33</sup> 緊急事態宣言／日本でも感染経路追跡 [Declaration of Emergency/Japanese Infection Route Tracking], Nikkan Kogyo Shimbun (Apr. 8, 2020), <https://www.nikkan.co.jp/articles/view/00554438>.

software from ACTT to the MHLW in order to satisfy a policy of Apple and Google limiting application development to health authorities.<sup>34</sup>

The summary of the tentative tracking system as of May 8, 2020, is as follows:

- The application software utilizes the application programming interface (API) provided by Apple and Google. The application, when installed in a device, will store the identifiers of other devices that have the application installed when these devices come within a certain distance for a certain duration of time, using Bluetooth. Identifiers are not connected to the individuals who have the devices, and they change periodically. Stored identifiers are deleted after a certain period.
- When a health care provider tests one of the device holders and the person is confirmed to be infected with COVID-19, the provider will notify a local health center. The health center inputs the information in the COVID-19 management system operated by the MHLW. The health center notifies the infected person of the result of the test.
- The notified person inputs the information that he or she received the positive test result from the health center on the application on his/her device. The application sends other device holders who have come in close contact with the person a warning. Persons who received the warning input the information on the application on their devices. The application program sends the information to the health center.

To protect privacy of the users, the software will not keep track their geolocation data. The system will not notify when and where they were in close proximity or the identity of the infected person.<sup>35</sup>

The government planned to operate the system in early May, but it was delayed until June. According to a news article, the agreement with Apple and Google has not been completed yet.<sup>36</sup>

---

<sup>34</sup> 接触確認アプリ、所管を厚労省にアップル・グーグルの方針受け [Contact Tracing App, Jurisdiction to MHLW, Due to Policy by Apple and Google], Nikkei (May 8, 2020), <https://www.nikkei.com/article/DGXMZO58875030Y0A500C2EA3000/>. See also ACTT Secretariat, 接触確認アプリの導入に向けた取組について（案） [Efforts to Introduce Contact Tracking App (Draft)], Material 1-1 for ACTT Meeting 8] (May 8, 2020), <https://perma.cc/FPX6-ADBU>.

<sup>35</sup> ACTT Secretariat, supra note 34, at 3-6. See also Press Release, Code For Japan, コンタクト・トレーシング・アプリの開発に関して [Regarding Development of Contact Tracing App], PR Times (Apr. 15, 2020), <https://perma.cc/K8ZH-AV9J>.

<sup>36</sup> <新型コロナ> 接触通知アプリ 来月導入の方針 [ <Novel Corona Virus> Contact Notification App, Introduced Next Month], Tokyo Shimbun (May 18, 2020), <https://www.tokyo-np.co.jp/article/economics/list/202005/CK2020051802000104.html>.

## **B. Returnee Follow-Up**

When residents of Japan come back from a certain area where the possibility of contacts with COVID-19 is heightened, health centers will track the health conditions of the returnees for 14 days. If returnees agree, they can communicate with the health center by using a smartphone application.<sup>37</sup>

---

<sup>37</sup> Press Release, MHLW, 帰国者への健康フォローアップに LINE アプリ等を活用します [*Utilizing LINE App to Follow Up Returnees' Health Conditions*] (Apr. 13, 2020), <https://perma.cc/MMF7-4E3C>.

# South Korea

Sayuri Umeda  
Senior Foreign Law Specialist

**SUMMARY** The right to privacy is guaranteed by South Korea’s Constitution. South Korea also has data protection laws, including a law specifically to protect location data. However, after the Middle East Respiratory Syndrome outbreak in South Korea in 2015, surveillance was strengthened, and the Infectious Disease Prevention and Control Act has a provision that overrides the location information law. People must cooperate with epidemiological investigations. Persons who are required to self-quarantine are monitored, and violators can face criminal punishment. The movements of infected or quarantined people are monitored by the use of credit cards, the location information of smartphones and, in some cases, electronic wristbands.

## I. Introduction/Overview

According to the website of the Ministry of Health and Welfare (MOHW), confirmed cases of COVID-19 totaled 11,142 as of May 22, 2020. The number of deaths was 264.<sup>1</sup>

Smartphone ownership in South Korea is high. About 95% of South Koreans own a smartphone—the highest nationwide level of smartphone ownership in the world.<sup>2</sup> Older people have switched to smartphones in recent years. In 2019, about 80% of people in their 60s had smartphones.<sup>3</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The South Korean Constitution has a provision guaranteeing the right to privacy.<sup>4</sup> Korean courts recognize a tort of invasion of privacy.<sup>5</sup> The Act on the Protection, Use, etc. of Location

---

<sup>1</sup> Press Release, MOHW, *Updates on COVID-19 in Republic of Korea 22 May 2020* (May 25, 2020), <https://perma.cc/3FKW-UE2Z>.

<sup>2</sup> Laura Silver, *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*, Pew Res. Ctr. (Feb. 5, 2019), <https://perma.cc/587D-EVRW>.

<sup>3</sup> 郭道英, 「スマートフォン人類」60代の普及率も80%を超えた [“Smartphone Human Race”: Ownership over 80% Among People in Their 60s], DongA.com (Aug. 6, 2019), <https://perma.cc/L45L-74HU>.

<sup>4</sup> Constitution of the Republic of Korea, Const. No. 10, Oct. 29, 1987, art. 17, <https://perma.cc/8LJ4-26HD>.

<sup>5</sup> Stacey Steele, *Defamation Law, Privacy and the #MeToo Movement in Korea*, Asian Currents (May 6, 2020) (interview of Judge Juhui Cha), <https://perma.cc/ZE4K-572H>.

Information (Location Information Act) regulates the use of location information to protect against its misuse.<sup>6</sup>

There are several laws that protect personal data. Among them, the Personal Information Protection Act (PIPA)<sup>7</sup> is the comprehensive general data protection law. PIPA states the general principles for handling personal information. For example, a personal information controller must specify explicitly the purposes for processing personal information and collect personal information lawfully and fairly to the minimum extent necessary for such purposes. A personal information controller must not use it beyond those purposes. A personal information controller must manage personal information safely. A 2020 amendment that will become effective in August 2020 states further that, if it is still possible to fulfill the purposes of collecting personal information by processing anonymized or “pseudonymised” personal information, the personal information controller shall endeavor to do so.<sup>8</sup>

There are also sector-specific laws for protection of personal information, such as the Act on Promotion of Information and Communications Network Utilization and Information Protection,<sup>9</sup> as well as the Credit Information Use and Protection Act.<sup>10</sup>

## **B. Data Retention and Location Tracking**

The Location Information Act defines “personal location information” as information about a place where a particular person exists or has existed at a certain time, which is collected using telecommunications equipment facilities. It includes information readily combinable with other information to track the location of a particular person even though location information alone is not sufficient to identify the location of the person.<sup>11</sup>

The Location Information Act prohibits the collection, use, or provision of location information regarding an individual or mobile object without the consent of the individual or the owner of the mobile object. In a case of an emergency rescue or as otherwise provided by other laws, such consent is not required.<sup>12</sup> The Act also requires that when a person lends an object with devices

---

<sup>6</sup> Act on the Protection, Use, etc. of Location Information (Location Information Act), Act No. 7372, Jan. 27, 2005, amended by Act No. 16087, Dec. 24, 2018, art. 1, <https://perma.cc/7ZCG-VSW2> (unofficial translation as amended by Act No. 14224, May 29, 2016).

<sup>7</sup> Personal Information Protection Act (PIPA), Act No. 10465, Mar. 29, 2011, amended by Act No. 16930, Feb. 4, 2020, <https://perma.cc/M3EP-UEZ5>.

<sup>8</sup> Act No. 16930 art. 3

<sup>9</sup> Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., Act No. 6360, Jan. 16, 2001, amended by Act No. 16021, Dec. 24, 2018, <https://perma.cc/REX2-QVM3>.

<sup>10</sup> Credit Information Use and Protection Act, Act No. 9617, Apr. 1, 2009, amended by Act No. 15146, Nov. 28, 2017, <https://perma.cc/5PUN-94UM>.

<sup>11</sup> Location Information Act art. 2, subparas. 1 & 2.

<sup>12</sup> Id. art. 15, para. 1.

capable of collecting location information, the person must notify the borrower of the fact that the object has a built-in location information collection device.<sup>13</sup>

Any person who intends to engage in the business of collecting location information and providing such information to service providers must obtain permission from the Korea Communications Commission (KCC).<sup>14</sup> Only corporations can obtain permission.<sup>15</sup> In addition, any person who intends to engage in the business of providing services based on personal location information must report its trade name, the address of the main office, the type of business, and its location information systems, among other things, to the KCC.<sup>16</sup>

Before collecting location information, a corporation that has obtained permission for a location information business must specify in its terms and conditions the contact information, rights held by the subjects of personal location information, details of its services to a provider of a service that uses personal location information, and the period of data retention, among other things.<sup>17</sup> Any service provider based on location information must do the same before providing service.<sup>18</sup> A corporation that has obtained permission for a location information business and a service provider utilizing personal location information can use or provide personal location information if it is processed in such a way that any specific person cannot be identified, and it is provided for the purpose of statistics, academic research, or market research.<sup>19</sup>

A person who has obtained permission for a location information business and a service provider utilizing personal location information must take managerial and technical measures to prevent the divulging, alteration or impairment of location information in accordance with the government decree.<sup>20</sup> The KCC may examine the measures.<sup>21</sup>

### III. Electronic Measures to Fight COVID-19 Spread

Under the Infectious Diseases Control and Prevention Act, the Director of the Korea Centers for Disease Control and Prevention (KCDC), governors, and the heads of municipal governments conduct an epidemiological investigation when an infectious disease breaks out and is likely to become predominant.<sup>22</sup> Epidemiological investigation includes identification of the path of

---

<sup>13</sup> Id. art. 15, para. 3.

<sup>14</sup> Id. art. 5, para. 1.

<sup>15</sup> Id. art. 5, para. 5.

<sup>16</sup> Id. art. 9, para. 1.

<sup>17</sup> Id. art. 18, para. 1.

<sup>18</sup> Id. art. 19, para. 1.

<sup>19</sup> Id. art. 21, para. 1.

<sup>20</sup> Id. art. 16, para. 1.

<sup>21</sup> Id. art. 16, para. 3.

<sup>22</sup> Infectious Diseases Control and Prevention Act, Act No. 9847, Dec. 29, 2009, amended by Act No. 17067, Mar. 4, 2020, art. 18, para. 1, <https://perma.cc/9GY9-WNSB> (unofficial translation, as amended by Act No. 14286, Dec. 2, 2016).

infection and the source of infection by the disease.<sup>23</sup> No one is allowed to refuse, interfere with, or evade the epidemiological investigation without a justifiable reason; to make a false statement; or to intentionally omit any fact.<sup>24</sup> Violations are punishable by imprisonment for not more than two years or a fine not exceeding KRW20 million (about US\$16,150).<sup>25</sup>

In addition, in order to prevent the further spread of an infectious disease upon its outbreak, the MOHW or a local government may keep persons suspected of being infected by the pathogen of an infectious disease hospitalized or quarantined in a proper place for a certain period.<sup>26</sup> A recent amendment adds a penalty for violations. A violation is punishable by imprisonment for up to one year or a fine not exceeding KRW10 million (about US\$8,080).<sup>27</sup>

South Korea experienced the largest outbreak of the Middle East Respiratory Syndrome (MERS) virus outside of the Middle East in 2015.<sup>28</sup> Following the MERS outbreak, South Korea took measures to strengthen its ability to carry out more accurate epidemiological studies and disease surveillance. The Infectious Diseases Control and Prevention Act was amended in December 2015.<sup>29</sup> Amended article 76-2, paragraph 2, states that, if necessary to prevent infectious diseases and block the spread of infection, the Minister of HOMW and heads of local governments may request law enforcement to provide the location information of patients with an infectious disease and persons likely to be infected by an infectious disease.<sup>30</sup> It further states that, in such cases, the head of the relevant police agency may request any location information provider and any telecommunications business operator to provide location information of the person despite restrictions under the Location Information Act,<sup>31</sup> as well as restrictions under the Protection of Communications Secrets Act.<sup>32</sup> The location information provider and the telecommunications business operator cannot refuse the request except in extenuating circumstances.<sup>33</sup> This provision

---

<sup>23</sup> Enforcement Decree of Infectious Diseases Control and Prevention Act, Presidential Decree No. 22564, Dec. 29, 2010, amended by Presidential Decree No. 30596, Apr. 2, 2020, art. 14, <https://perma.cc/G3JE-DSTM> (unofficial translation as amended by Presidential Decree No. 29180, Sept. 18, 2018); and Enforcement Rule of Infectious Diseases Control and Prevention Act, art. 14 & att. 1-3, MOHW Decree No. 32, Dec. 30, 2010, amended by MOHW Decree No. 717, Apr. 3, 2020.

<sup>24</sup> Infectious Diseases Control and Prevention Act art. 18, para. 3.

<sup>25</sup> Id. art. 79.

<sup>26</sup> Id. art. 47, subpara. 3

<sup>27</sup> Id. art. 79-3.

<sup>28</sup> *2015 MERS Outbreak in Republic of Korea*, World Health Org., <https://perma.cc/BT7G-9FRD>. By the end of the outbreak, 186 laboratory-confirmed cases and 38 deaths had been recorded.

<sup>29</sup> Act to Partially Amend the Infectious Diseases Control and Prevention Act, Act No. 13639, Dec. 29, 2015.

<sup>30</sup> Infectious Diseases Control and Prevention Act art. 76-2, para. 2.

<sup>31</sup> Location Information Act art. 15.

<sup>32</sup> Protection of Communications Secrets Act, Act No. 4650, Dec. 27, 1993, amended by Act No. 14839, July 26, 2017, art. 3, <https://perma.cc/9PKZ-9N9F>.

<sup>33</sup> Infectious Diseases Control and Prevention Act art. 76-2, para. 2 and art. 79-2 (penal provision).

allows the police to access individuals' private information, ranging from credit card records to cell phone Global Positioning System data, without a warrant.<sup>34</sup>

In March 2020, the government launched a new system to track the movements of people infected with COVID-19 and their contacts more quickly. The Ministry of Land, Infrastructure and Transport, the Ministry of Science and ICT (Information and Communication Technologies), and the KCDC jointly developed the system. The Korean National Police Agency, the Credit Finance Association, South Korea's three mobile carriers, and 22 credit card issuers have joined the system.<sup>35</sup>

Additionally, because the number of cases of people breaching the self-quarantine raised concerns, the government announced the use of electronic wristbands on people who violate self-isolation rules to better contain the spread of COVID-19 on April 11, 2020.<sup>36</sup> Although some indicated concern about a breach of privacy, 80.2% of people in a government survey supported the idea of using electronic wristbands to keep track of those under self-quarantine.<sup>37</sup> However, the government cannot force people to wear the wristbands because there is no law requiring it. Since April 27, 2020, if a violator agrees, he or she wears a wristband for two weeks.<sup>38</sup> Some foreign countries have started importing the wristbands and may follow South Korea's monitoring method.<sup>39</sup>

The Infectious Diseases Control and Prevention Act states that citizens should be provided with detailed information, such as the movement paths, transportation means, and medical treatment institutions and contacts of infected persons.<sup>40</sup> The KCDC and metropolitan and provincial governments release a detailed log of the movements of COVID-19 patients, including the time and name of places they visited, through the media and related websites. Out of privacy concerns, the National Human Rights Commission of Korea called on "the authorities to publish the time and names of locations visited by infected people, rather than providing the travel history of each individual, and specify disinfection and protective measures taken by the public health authorities for these locations."<sup>41</sup>

---

<sup>34</sup> Jae-hee Choi, *South Korea's Best Method of Tracking COVID-19 Spread: Credit Card Transactions*, Korea Herald (Apr. 9, 2020), <https://perma.cc/M8P3-6VXH>.

<sup>35</sup> *S. Korea Set to Launch Quick Tracking System for Virus Cases*, Yonhap News Agency (Mar. 25, 2020), <https://perma.cc/L3HV-384A>.

<sup>36</sup> *Wristband for Self-Isolation Violators*, Yonhap News Agency (Apr. 24, 2020) (photograph of wristband), <https://perma.cc/94BB-D5PY>.

<sup>37</sup> *S. Korea to Use Electronic Wristbands on Violators of Self-Isolation Rules: PM*, Yonhap News Agency (Apr. 11, 2020), <https://perma.cc/2U4J-F259>.

<sup>38</sup> *(2nd LD) New Virus Cases Surely on Downward Trend, No Additional Death Reported*, Yonhap News Agency (Apr. 24, 2020), <https://perma.cc/AX9W-RXYV>.

<sup>39</sup> *S. Korea Exports Wristband Trackers for Quarantine Violators*, Yonhap News Agency (May 20, 2020), <https://perma.cc/TMN8-SL37>.

<sup>40</sup> Infectious Diseases Control and Prevention Act art. 34-2.

<sup>41</sup> Press Release, Nat'l Hum. Rts. Comm'n of Korea, *NHRCK Chairperson's Statement on Excessive Disclosure of Private Information of COVID-19 Patients* (Mar. 9, 2020), <https://perma.cc/WL78-36WM>.

# Taiwan

Laney Zhang  
Foreign Law Specialist

**SUMMARY** Under Taiwan’s Personal Data Protection Act 2015 (PDPA), the collection, processing, and use of personal data must be carried out in an honest and good-faith manner that respects the data subject’s rights and interests, does not exceed the necessary scope of the specific purposes, and has a legitimate and reasonable connection with the purposes of collection. Both government and nongovernment agencies are required to delete personal data when the specific purpose of data collection no longer exists or the retention period ends.

In response to COVID-19, Taiwan launched the Digital Fence Intelligent Monitoring System, known as the “digital fence,” in February 2020, to monitor the location of those required to undergo home quarantine via their own cellphones or government-issued cellphones, with the goal of preventing their movement and stopping the spread of the infection. Taiwan implemented a mandatory 14-day home quarantine for the contacts of confirmed cases and all overseas arrivals.

The government has acknowledged that cellphone location data is protected by the PDPA. It reportedly argues, however, that it is within the necessary scope of the government’s performance of its statutory duties to subject location data to regulation in the current circumstances; it notes that telecom companies are “furthering the public interest” by participating in the tracking effort and therefore are also exempt from liability. The tracking system will be discontinued after the pandemic passes and all stored personal data will be deleted at that time.

## I. Introduction

Taiwan has won global praise for its effective control of the COVID-19 pandemic. As of May 22, 2020, a total of 441 confirmed cases of COVID-19 had been reported in Taiwan, including seven deaths, out of a population of almost 24 million.<sup>1</sup>

A highly tech-savvy democracy, Taiwan is believed to have implemented the first phone-based tracking system to enforce quarantine in the current pandemic. It began working on the system, described as a “digital fence,” as early as in late January 2020, a week after Taiwan recorded its first imported case of the novel coronavirus from China.<sup>2</sup> Although there have been concerns over data privacy, the public opinion in general firmly supports the government in its handling of the pandemic. A telephone poll conducted in mid-February by the Taiwanese Public Opinion

---

<sup>1</sup> CECC Reports No New Confirmed Cases; 408 Patients Released from Isolation, Taiwan Centers for Disease Control (Taiwan CEC) (May 22, 2020), <https://perma.cc/QR83-WPH4>; Mary Hui, *How Taiwan Is Tracking 55,000 People under Home Quarantine in Real Time*, Quartz (Apr. 1, 2020), <https://perma.cc/9LAF-C8M4>.

<sup>2</sup> Yasheng Huang et al., *How Digital Contact Tracing Slowed Covid-19 in East Asia*, Harvard Bus. Rev. (Apr. 15, 2020), <https://perma.cc/HW3C-VJ73>.

Foundation found that people on average gave the government a score of 84 points out of 100 for its epidemic response.<sup>3</sup> In terms of smartphone usage, over 98% of the Taiwanese population owned smartphones as of 2019.<sup>4</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The primary Taiwanese legislation governing the collection, process, and use of personal data is the Personal Data Protection Act 2015 (PDPA).<sup>5</sup> The PDPA provides two sets of data protection rules applying to government agencies and nongovernment agencies, respectively. Government agencies include central and local government and administrative entities that are authorized to exercise public authority. Nongovernment agencies include individuals, legal persons, and other entities that are not government agencies.<sup>6</sup>

Personal data under the PDPA include names, dates of birth, ID Card numbers, passport numbers, characteristics, fingerprints, marital status, family, education, occupation, medical records, medical treatment, genetic information, sexual life, health examinations, criminal records, contact information, financial situation, social activities, and other information or data that may be used to identify a natural person, directly or indirectly.<sup>7</sup>

According to the PDPA, the collection, processing, and use of personal data must be carried out in an honest and good-faith manner that respects the data subject's rights and interests, does not exceed the necessary scope of the specific purposes, and has a legitimate and reasonable connection with the purposes of collection.<sup>8</sup>

Sensitive data under Taiwanese law may refer to medical records, medical treatment, genetic information, sexual life, health examinations, and criminal records. According to the PDPA, these data may not be collected, processed, or used unless expressly required by law or within an exception specified by the PDPA. One such exception concerns those cases where collection, processing, or use of sensitive data is within the necessary scope for a government agency to perform its statutory duties or for a nongovernment agency to fulfill its statutory obligations, provided that proper security and maintenance measures are adopted prior or subsequent to such collection, processing, or use of personal data.<sup>9</sup>

---

<sup>3</sup> Hui, *supra* note 1.

<sup>4</sup> Samantha Wong, *Smartphone Market in Taiwan – Statistics & Facts*, Statista (Apr. 20, 2020), <https://perma.cc/UC9J-XFRG>.

<sup>5</sup> Personal Data Protection Act (promulgated Aug. 11, 1995, amended Dec. 30, 2015), <https://perma.cc/WM7B-PNED> (in Chinese), <https://perma.cc/MTB4-D9LX> (English translation).

<sup>6</sup> *Id.* art. 2.

<sup>7</sup> *Id.*

<sup>8</sup> *Id.* art. 5.

<sup>9</sup> *Id.* art. 6.

## B. Data Retention and Location Tracking

Although location data is not specified by the PDPA as a form of personal data, it may be deemed “other information or data which may be used to identify a natural person,” and therefore subject to the requirements of the PDPA on the collection, processing, and use of personal data.

Under the PDPA, the collection or processing of personal data by a government agency must be for specific purposes and on one of the following bases:

1. where it is within the necessary scope to perform its statutory duties;
2. where consent has been given by the data subject; or
3. where the rights and interests of the data subject will not be infringed upon.<sup>10</sup>

The collection or processing of personal data by a nongovernment agency must be for specific purposes and expressly required by law, consented to by the data subject, necessary for furthering the public interest, or on others grounds specified by the PDPA.<sup>11</sup>

Furthermore, a government agency may only use personal data within the necessary scope of its statutory duties and for the specific purpose of collection. The use of personal data for any other purposes must be on the following grounds:

1. where it is expressly required by law;
2. where it is necessary for ensuring national security or furthering public interest;
3. where it is to prevent harm to the life, body, freedom, or property of the data subject;
4. where it is to prevent material harm to the rights and interests of others;
5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;
6. where it is for the data subject’s rights and interests; or
7. where consent has been given by the data subject.<sup>12</sup>

A nongovernment agency may only use personal data within the necessary scope of the specific purpose of collection, or if it is expressly required by law, consented to by the data subject, necessary for furthering public interests, or on other grounds specified by the PDPA.<sup>13</sup>

---

<sup>10</sup> Id. art. 15.

<sup>11</sup> Id. art. 19.

<sup>12</sup> Id. art. 16.

<sup>13</sup> Id. art. 20.

Both government and nongovernment agencies are required by the PDPA to delete personal data, voluntarily or upon the request of the data subject, when the specific purpose of data collection no longer exists or the retention period ends.<sup>14</sup>

### III. Electronic Measures to Fight COVID-19 Spread

#### A. Digital Fence and Entry Quarantine System

In response to the pandemic, Taiwan implemented a mandatory 14-day home quarantine for contacts of confirmed cases and all overseas arrivals and launched the Digital Fence Intelligent Monitoring System, known as the “digital fence,” in February 2020. The system monitors the location of those required to undergo home quarantine via their own cellphones or government-issued cellphones to prevent their movement and stop the spread of the infection.<sup>15</sup>

The telecom companies track the quarantined individuals by triangulating the location of their phones relative to nearby cell towers. Venturing too far from homes triggers the alert system, and text messages are sent to the quarantined individuals, government civil affairs and health authorities, and local police to ascertain their whereabouts. The government also contacts those in quarantine on a daily basis to ensure they do not evade tracking by leaving their phones at home. Anyone caught breaching their quarantine can be fined up to NT\$1 million (about US\$33,000).<sup>16</sup>

Taiwan has also launched an Entry Quarantine System that seeks to expedite entry of all international arrivals by requiring them to scan a QR code upon entering Taiwan and fill out a health declaration. This system has been integrated with the digital fence system, allowing hospitals, clinics, and pharmacies to gain access to patients’ travel histories.<sup>17</sup>

#### B. Government Response to Data Privacy Concerns

In response to concerns arising from the tracking system over data privacy, the government has reportedly cited the Communicable Disease Control Act and the Special Act for Prevention, Relief and Revitalization Measures for Severe Pneumonia with Novel Pathogens, which authorize the government to impose “necessary measures” in epidemic control.<sup>18</sup> The government has acknowledged that cellphone location data is protected by the PDPA. It argues, however, that it is within the necessary scope of the government’s performance of its statutory duties to subject

---

<sup>14</sup> Id. art. 11.

<sup>15</sup> *Lawfully Comply with 14-Day Home Quarantine, Protect Health of People*, Taiwan CDC (Mar. 27, 2020), <https://perma.cc/687T-9QFB> (in Chinese).

<sup>16</sup> Id.; Hui *supra* note 1; Huang et al., *supra* note 2.

<sup>17</sup> Huang et al., *supra* note 2; *To Integrate Entry Quarantine System with Digital Fence Intelligent Monitoring System, Tracking Whereabouts through Cellphone Location*, Ministry of Health and Welfare (May 14, 2020), <https://perma.cc/7TWF-92TF> (in Chinese).

<sup>18</sup> Pai-ching Hou, *Is the Digital Fence that Other Countries Are Striving to Imitate Unconstitutional? Questioned by Legal Professionals, Government Has Something to Say*, The Storm Media (Apr. 17, 2020), <https://perma.cc/XD8G-69SB> (in Chinese).

location data to regulation and asserts that telecom companies are “furthering the public interest” and therefore also exempt from liability.

The government has said the tracking system will be discontinued after the pandemic passes and all stored personal data will be deleted at that time.<sup>19</sup>

---

<sup>19</sup> Id.

*Europe and Central Asia*

# European Union

*Jenny Gesley*  
*Foreign Law Specialist*

**SUMMARY** In order to fight the spread of COVID-19 in the European Union (EU), the European Commission has suggested developing contact tracing and warning mobile apps, complemented by other measures such as increased testing capabilities. It recommends voluntary apps that comply with data protection and privacy rules and are deleted once they are no longer necessary. Its recommendation sets out detailed rules for the development of such apps and for the use of anonymized mobility data. The eHealth Network, a voluntary network that provides a platform of Member States' competent authorities dealing with digital health, has published a practical guide for Member States for developing privacy-preserving mobile apps for contact tracing. It is planning on publishing another toolbox for the use of mobility data in June 2020.

The protection of personal data and the respect for private life are fundamental rights in the EU. The data protection legal framework in the EU currently consists of two main pillars, the Directive on Privacy and Electronic Communications (ePrivacy Directive) and the General Data Protection Regulation (GDPR). The GDPR and the ePrivacy Directive set out various requirements for the processing of traffic and location data. In general, consent is required or processing must be necessary for the provision of the service; however, exceptions are possible for reasons of public interest such as public health, or for public security. Derogations must be necessary, appropriate, and proportionate measures. In addition, the EU Decision on Combating Serious Cross-Border Threats to Health, which lays down rules on epidemiological surveillance and on monitoring, early warning, and responsive measures to combat serious cross-border threats to health, allows the transmission of personal data necessary for the purpose of contact tracing.

## I. Introduction

On April 17, 2020, the European Commission (Commission) published a "Joint European Roadmap Towards Lifting COVID-19 Containment Measures" that sets out recommendations for the EU Member States to reopen their economies.<sup>1</sup> The three criteria used to assess whether measures taken can be relaxed are epidemiological criteria, sufficient health system capacity, and appropriate monitoring capacity.<sup>2</sup> With regard to monitoring, the Commission suggests, among other things, creating a "framework for contact tracing and warning with the use of mobile apps, which respects data privacy."<sup>3</sup> For that purpose, it has adopted a recommendation to develop a common European approach ("toolbox") for the use of mobile applications and has published

---

<sup>1</sup> Joint European Roadmap Towards Lifting COVID-19 Containment Measures, 2020 O.J. (C 126) 1, <https://perma.cc/M67Z-YEUL>.

<sup>2</sup> Id. at 4.

<sup>3</sup> Id. at 4 & 6.

guidance for the development of such mobile apps with regard to data protection and privacy.<sup>4</sup> The common EU toolbox was published by the eHealth Network on April 15, 2020, and provides a practical guide for Member States for developing privacy-preserving mobile apps for contact tracing.<sup>5</sup>

As of May 22, 2020, there have been a total number of 1.34 million cases of COVID-19 in the European Union (EU)/European Economic Area (EEA) and the United Kingdom (UK), with the most cases being reported in the UK (250,908), Spain (233,037), and Italy (228,006).<sup>6</sup> Of those cases, 160,002 people have died in the EU/EEA and the UK combined.<sup>7</sup> A Eurobarometer survey published in July 2018 found that a total of 89% of the respondents in each EU Member State have at least one mobile phone, ranging from 83% in Italy to 99% in Finland.<sup>8</sup> Furthermore, at least two-thirds of respondents in each Member State live in a household with mobile internet access, with the highest rate (91%) reported in the Netherlands and Denmark.<sup>9</sup> In response to another survey published in March 2020, 60% of the respondents stated that they were willing to share personal data securely to improve public services, with 43% willing to share personal data to improve medical research and care and 31% willing to do so to improve the response to a crisis situation such as an epidemic.<sup>10</sup>

---

<sup>4</sup> Commission Recommendation (EU) 2020/518 on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit From the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data, 2020 O.J. (L 114) 7, <https://perma.cc/XL2M-3UJX>; Commission Communication 2020/C 124 I/01, Guidance on Apps Supporting the Fight Against COVID 19 Pandemic in Relation to Data Protection (App Guidance), 2020 O.J. (C 124 I) 1, <https://perma.cc/S7CZ-8NMV>.

<sup>5</sup> eHealth Network, *Mobile Applications to Support Contact Tracing in the EU's Fight Against COVID-19. Common EU Toolbox for Member States. Version 1.0* (Apr. 15, 2020), <https://perma.cc/C98Y-7NNV>; eHealth Network, *Annex IV: Inventory Mobile Solutions Against COVID-19* (Apr. 16, 2020), <https://perma.cc/HW9F-AMHL>. The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent authorities dealing with digital health. See eHealth Network, *Mobile Applications*, at 2.

<sup>6</sup> *Situation Update for the EU/EEA and the UK, as of 22 May 2020*, European Centre for Disease Prevention and Control [ECDC] (last updated May 22, 2020), <https://perma.cc/A9UZ-Z9XU>.

<sup>7</sup> *Id.*

<sup>8</sup> European Commission, *Special Eurobarometer 462. Report. E-Communications and Digital Single Market 37* (July 2018), <https://perma.cc/L6BY-DRMJ>.

<sup>9</sup> *Id.* at 49.

<sup>10</sup> European Commission, *Special Eurobarometer 503. Report. Attitudes Towards the Impact of Digitalisation on Daily Lives 33* (Mar. 2020), <https://perma.cc/U29Z-UPYK>.

## II. Legal Framework

### A. Privacy and Data Protection

The protection of personal data and the respect for private life are fundamental rights in the EU.<sup>11</sup> Personal data is defined as “any information relating to an identified or identifiable natural person (data subject).”<sup>12</sup> Among other things, location data is one of the factors that can make a person identifiable.<sup>13</sup> The data protection legal framework in the EU currently consists of two main pillars, the Directive on Privacy and Electronic Communications (ePrivacy Directive)<sup>14</sup> and the General Data Protection Regulation (GDPR).<sup>15</sup> The ePrivacy Directive is slated to be replaced by an ePrivacy Regulation; however, the legislative process is still ongoing, with the last action taken in November 2019, and there appears to be no consensus among the EU countries.<sup>16</sup>

#### 1. General Data Protection Regulation

As a regulation, the GDPR is directly applicable in the EU Member States with generally no domestic implementing legislation needed.<sup>17</sup> Processing of personal data<sup>18</sup> according to the GDPR must comply with the principles of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy and keeping data up to date; storage limitation; and

---

<sup>11</sup> Charter of Fundamental Rights of the European Union (EU Charter) arts. 7, 8, 2012 O.J. (C 326) 391, <https://perma.cc/PAX8-4MYJ>; Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 16, para. 1, 2016 O.J. (C 202) 1, <https://perma.cc/GPB6-64TG>.

<sup>12</sup> General Data Protection Regulation (GDPR), art. 4, point (1), 2016 O.J. (L 119) 1, <https://perma.cc/7T85-89ZQ>.

<sup>13</sup> An “identifiable natural person” is “one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” See GDPR, art. 4, point (1).

<sup>14</sup> Consolidated Version of the Directive on Privacy and Electronic Communications (ePrivacy Directive), 2002 O.J. (L 201) 37, <https://perma.cc/YHA5-EFXV>.

<sup>15</sup> GDPR, *supra* note 12.

<sup>16</sup> ePrivacy Regulation Proposal, COM(2017) 10 final (Jan. 10, 2017), <https://perma.cc/N2WU-H2RL>; *Legislative Train Schedule. Proposal for a Regulation on Privacy and Electronic Communication*, European Parliament (last updated Dec. 15, 2019), <https://perma.cc/M49E-Q5UR>.

<sup>17</sup> TFEU, art. 288, para. 2; GDPR, art. 99. Some provisions nonetheless require for their implementation the adoption of measures of application by the Member States – for example, the appointment of a national regulator and administrative sanctions for a violation of the GDPR. The GDPR also contains “opening clauses” that permit diverging national legislation in certain areas – for example, for the processing of special categories of personal data or in the context of employment.

<sup>18</sup> “Processing” means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.” GDPR, art. 4, point (2).

integrity and confidentiality.<sup>19</sup> Article 6 of the GDPR sets out the conditions under which data processing is considered lawful, with the most common ground being consent given by the data subject.<sup>20</sup>

The processing of certain special categories of personal data (sensitive data), such as data concerning health, is generally prohibited.<sup>21</sup> However, as an exception, sensitive data may be processed if it is “necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health . . . , on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject.”<sup>22</sup> Recital 52 of the GDPR clarifies that derogations from the general prohibition are possible for reasons of “health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health.” Furthermore, processing is allowed when it is necessary to protect the vital interests of the data subject.<sup>23</sup> The GDPR explains that this exception may be used as a basis to monitor epidemics and their spread.<sup>24</sup>

Pseudonymization means the “processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.” The GDPR views pseudonymization of personal data as an appropriate technical and organizational measure to achieve “privacy by design” and to ensure the security of data processing.<sup>25</sup> It is not to be confused with anonymization of data, which allows use of the data without any restriction.<sup>26</sup>

## 2. *ePrivacy Directive*

The aim of the ePrivacy Directive is to ensure an equivalent level of protection of fundamental rights and freedoms (particularly the right to privacy) with respect to data processing in the electronic communications sector and to ensure the free movement of such data.<sup>27</sup> The ePrivacy Directive covers the processing of personal data by traditional telecom providers in public communications networks in the EU and mandates that Member States protect the confidentiality of the content of electronic communications through national legislation.<sup>28</sup> In particular, Member

---

<sup>19</sup> Id. art. 5, para. 1. For a more detailed overview, see Jenny Gesley, *Online Privacy Law: European Union* (Law Library of Congress, Dec. 2017), <https://perma.cc/D36L-7EH8>.

<sup>20</sup> GDPR, art. 6, para. 1(a), art. 7.

<sup>21</sup> Id. art. 9, para. 1.

<sup>22</sup> Id. art. 9, para. 2(g).

<sup>23</sup> Id. art. 9, para. 2(c).

<sup>24</sup> Id. recital 42.

<sup>25</sup> Id. arts. 25, 32.

<sup>26</sup> European Data Protection Board (EDPB), *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak* para. 17 (Apr. 21, 2020), <https://perma.cc/3GYK-JYD4>.

<sup>27</sup> ePrivacy Directive, art. 1, para. 1.

<sup>28</sup> Id. arts. 3, 5.

States must “prohibit listening, tapping, storage, or other kinds of interception or surveillance of communications and the related traffic data . . . without the consent of the users concerned.”<sup>29</sup> The proposed ePrivacy Regulation would extend coverage to internet-based voice and messaging services such as WhatsApp, Facebook Messenger, and Skype.<sup>30</sup>

## **B. Data Retention and Location Tracking**

### *1. ePrivacy Directive*

The ePrivacy Directive allows processing of traffic and other location data under certain circumstances. Traffic data, defined as “any data processed for the purpose of a conveyance of a communication on an electronic communications network or for the billing thereof,”<sup>31</sup> may be processed for billing purposes and must be deleted or made anonymous when no longer needed.<sup>32</sup> Traffic data may also be processed for marketing purposes if prior consent from the user was obtained.<sup>33</sup> Other location data, defined as “any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service,”<sup>34</sup> may only be processed after being made anonymous, or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision of a value-added service.<sup>35</sup> Value-added services are commonly known as location-based services. Users must be informed whether the data will be transmitted to a third party for the purpose of providing the service and must be able to withdraw consent at any time.<sup>36</sup>

Furthermore, storing or gaining access to information already stored on a device requires the consent of the user or must be necessary to provide the service.<sup>37</sup> The user must be provided with clear and comprehensive information on the purpose of the processing in line with the requirements set out in the GDPR.<sup>38</sup>

Derogations from the obligations and rights with regard to traffic and other location data, in particular the requirement to obtain consent, are allowed for national or public security reasons or for law enforcement purposes, among others, if the restriction is a necessary, appropriate, and proportionate measure.<sup>39</sup>

---

<sup>29</sup> Id. art. 5.

<sup>30</sup> ePrivacy Regulation Proposal, art. 18.

<sup>31</sup> ePrivacy Directive, art. 2(b).

<sup>32</sup> Id. art. 6.

<sup>33</sup> Id. art. 6, para. 3.

<sup>34</sup> Id. art. 2(c).

<sup>35</sup> Id. art. 9, para. 1.

<sup>36</sup> Id.

<sup>37</sup> Id. art. 5, para. 3.

<sup>38</sup> Id.

<sup>39</sup> Id. art. 6; art. 15, para. 1.

## 2. *Data Retention Directive*

The EU Data Retention Directive, which was declared invalid by the Court of Justice of the European Union (CJEU) on April 8, 2014, was another EU legislative instrument that is relevant in the context of data protection and storing traffic and location data.<sup>40</sup> The CJEU held that the Data Retention Directive violated the right to privacy (article 7), the right to protection of personal data (article 8), and the principle of proportionality (article 52) as codified in the EU Charter.<sup>41</sup> The Directive has not been replaced with new EU legislation. Instead, national data retention laws are applicable, but they are subject to review by the CJEU.<sup>42</sup> The CJEU stated that data retention obligations and access to that data are only permissible under EU law if they are strictly necessary.<sup>43</sup> In the Court's opinion, EU law precludes national legislation that prescribes general and indiscriminate retention of data.<sup>44</sup> The Commission announced in 2017 that it would develop guidance as to how national data retention laws can be constructed to comply with the CJEU ruling; however, such guidance has not yet been released.<sup>45</sup>

## 3. *Decision on Combating Serious Cross-Border Threats to Health*

Decision No. 1082/2013/EU on Combating Serious Cross-Border Threats to Health lays down rules on epidemiological surveillance and on monitoring, early warning, and responsive measures to combat serious cross-border threats to health.<sup>46</sup> Recital 25 to the Decision points out that cross-border threats to health

could require the Member States concerned to take particular control or contact-tracing measures in a coordinated manner to identify those persons already contaminated and those persons exposed to risk. Such cooperation could require the exchange of personal data through the system, including sensitive information related to health and information about confirmed or suspected human cases of disease, between those Member States directly involved in the contact-tracing measures.

Data processing for this purpose must comply with the EU data protection framework and must provide specific safeguards for the exchange of personal data.<sup>47</sup> In particular, personal data must

---

<sup>40</sup> Data Retention Directive, 2006 O.J. (L 105) 54, <https://perma.cc/7NM9-LX64>.

<sup>41</sup> Joined Cases C-293/12 and C-594/12, *Dig. Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*, ECLI:EU:C:2014:238, <https://perma.cc/DS6L-C2UK>. For background information, see Theresa Papademetriou, *European Union: ECJ Invalidates Data Retention Directive* (Law Library of Congress, June 2014), <https://perma.cc/KE7S-EB93>.

<sup>42</sup> Joined Cases C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v. Tom Watson*, paras. 75–81, ECLI:EU:C:2016:970, <https://perma.cc/KE9W-9M6M>.

<sup>43</sup> *Id.* at 96.

<sup>44</sup> *Id.* at 112.

<sup>45</sup> Commission Communication, at 8, COM (2017) 41 final (Jan. 25, 2017), <https://perma.cc/MPJ9-NVZL>.

<sup>46</sup> Consolidated Version of Decision No. 1082/2013/EU, art. 1, 2013 O.J. (L 293) 1, <https://perma.cc/UBY9-BVEH>.

<sup>47</sup> *Id.* art. 16, recital 27.

be protected against accidental or illegal destruction, accidental loss, or unauthorized access and against any form of illegal processing.<sup>48</sup>

The Decision establishes an Early Warning and Response System (EWRS) for information exchange on serious cross-border threats to health between the Commission and the competent national authorities.<sup>49</sup> Member States must notify an alert in the EWRS where a threat to health that is unusual or unexpected, causes significant mortality/morbidity in humans, grows rapidly in scale, or exceeds national response capacity affects more than one Member State and requires a coordinated response at the EU level.<sup>50</sup> Among other things, Member States must transmit personal data necessary for the purpose of contact tracing.<sup>51</sup> The national authorities are considered controllers of data for that purpose.<sup>52</sup> They must use the selective messaging functionality of the EWRS for the transfer of such contact tracing data and only communicate it to the other Member States involved in the contact tracing measures.<sup>53</sup> The personal data will be automatically deleted from the selective messaging functionality of the EWRS after 12 months.<sup>54</sup>

The Commission has issued a recommendation that provides guidance to national authorities on data protection issues within the framework of the EWRS and has published an indicative list of personal data for contact tracing.<sup>55</sup> The indicative list allows the exchange of the following personal data for coordinating contact tracing measures:

1. PERSONAL INFORMATION

- First name and surname,
- Nationality, date of birth, sex,
- Country of residence,
- ID type, number and issuing authority,
- Current home/residence address (street name and number, city, country, postal code),
- Telephone numbers (mobile, residential, business),
- Email (private, business).

2. TRAVEL SPECIFICATIONS

- Conveyance data (such as flight number, date and length of flight, ship name, plate number),
- Seat number(s),
- Cabin number(s).

---

<sup>48</sup> Id. art. 16, para. 1.

<sup>49</sup> Id. art. 8.

<sup>50</sup> Id. art. 9, para. 1.

<sup>51</sup> Id. art. 9, para. 3(i).

<sup>52</sup> Id. art. 16, para. 7.

<sup>53</sup> Id. art. 16, paras. 2, 3.

<sup>54</sup> Id. art. 16, para. 5.

<sup>55</sup> Id. art. 16, para. 9; Commission Recommendation (EU) 2017/1140, 2017 O.J. (L 164) 65, <https://perma.cc/D9NX-SVMW>. The indicative list of personal data that may be communicated by the EWRS competent authorities is included in the Annex to the Commission Recommendation.

3. CONTACT INFORMATION
  - Names of visited persons/places of stay,
  - Dates and addresses of the places of stay (street name and number, city, country, postal code),
  - Telephone numbers (mobile, residential, business),
  - Email (private, business).
4. INFORMATION ON ACCOMPANYING PERSONS
  - First name and surname,
  - Nationality,
  - Country of residence,
  - ID type, number and issuing authority,
  - Current home address (street name and number, city, country, postal code),
  - Telephone numbers (mobile, residential, business),
  - Email (private, business).
5. EMERGENCY CONTACT DETAILS
  - Name of person to be contacted,
  - Address (street name and number, city, country, postal code),
  - Telephone numbers (mobile, residential, business),
  - Email (private, business).<sup>56</sup>

### III. Electronic Measures to Fight COVID-19 Spread

#### A. COVID-19 Mobile Applications

##### 1. *General Overview of Apps*

As mentioned, the Commission recommends developing mobile apps to help reduce the spread of COVID-19, complemented by other measures such as increased testing capabilities. Its legally non-binding App Guidance issued on April 17, 2020, addresses the development of voluntary apps to fight the COVID-19 pandemic. It does not cover mandatory apps or those enforcing quarantine requirements. In the opinion of the Commission, further analysis is needed for mandatory apps because of the “high degree of intrusiveness of such an approach,” and therefore recommends the use of voluntary apps.<sup>57</sup> The App Guidance deals with apps with one or several of the following characteristics:

- provides accurate information to individuals about the COVID-19 pandemic;
- has symptom-checker functionality;
- has contact tracing and warning functionality; or
- increases the use of telemedicine.<sup>58</sup>

---

<sup>56</sup> Id. Annex.

<sup>57</sup> App Guidance, *supra* note 4, at 2.

<sup>58</sup> Id.

The App Guidance states that symptom checker and contact tracing and warning functionalities are useful both for individuals and public health authorities.<sup>59</sup> Individuals that have been in contact with an infected person are informed about appropriate next steps, such as testing, self-quarantine, or treatment. Furthermore, the data may be useful in understanding transmission patterns and provide information on virus circulation.<sup>60</sup> The Commission recommends interoperability of IT solutions used by the different Member States to enable cross-border collaboration and to ensure contact detection between users of different apps.<sup>61</sup>

## 2. *Compatibility with Privacy and Data Protection Principles*

In a next step, the Commission lays out different elements that are meant to ensure that the mobile apps comply with the EU privacy and personal data protection framework.

### a. Designation and Role of Controllers

The Commission recommends the designation of national health authorities or other similar bodies as the controllers of data.<sup>62</sup> Controllers are charged with ensuring compliance with data protection rules and must inform individuals of how their data is going to be used.<sup>63</sup> Furthermore, as the processing of sensitive health data will likely result in a high risk to the rights and freedoms of individuals, the controller must conduct a prior data protection impact assessment (DPIA).<sup>64</sup> The European Data Protection Board (EDPB) recommends publication of the DPIAs.<sup>65</sup>

### b. Individual Control of Data

Secondly, the Commission emphasizes that individuals must remain in control of their data.<sup>66</sup> Being “in control” means that

- the download and installation of the app are voluntary and there are no negative repercussions for individuals who chose not to download it;
- consent is given for each individual functionality of the app;
- proximity data is stored on the device and will not be shared unless a person is infected with COVID-19 and consents to the data sharing;
- health authorities provide individuals with all necessary information about the processing of their data in line with the GDPR and the ePrivacy Directive;

---

<sup>59</sup> Id. at 3, para. 2.

<sup>60</sup> Id.

<sup>61</sup> Id.

<sup>62</sup> Id. at 3, para. 3.1.

<sup>63</sup> GDPR, art. 5, para. 2.

<sup>64</sup> Id. art. 35.

<sup>65</sup> EDPB, *supra* note 26, para. 39.

<sup>66</sup> App Guidance, *supra* note 4, at 4, para 3.2

- individuals are able to exercise their data protection rights, such as access, rectification, and deletion, among others;
- restrictions of rights are provided for in a necessary and proportionate law and satisfy the requirements set out in the GDPR and the ePrivacy Directive; and
- the app is automatically deleted from the mobile device once the pandemic is declared to be under control.<sup>67</sup>

c. Consent of the User

Furthermore, the Commission points out that contact tracing and warning apps generally require the storage of information on the device. According to the ePrivacy Directive, storing information or gaining access to information already stored on a device requires either consent of the user or must be necessary to provide the service.<sup>68</sup> The Commission explains that as the user may need to upload proximity data, which is not necessary for the operation of the app as such, consent is required.<sup>69</sup> Consent according to the GDPR is only valid if it is freely given,<sup>70</sup> specific, informed,<sup>71</sup> and an unambiguous indication of the data subject's wishes by which he or she signifies agreement to the processing of personal data relating to him or her.<sup>72</sup> That means that silence, pre-ticked boxes (checked by default), or inactivity do not constitute valid consent.<sup>73</sup> Furthermore, withdrawing consent needs to be as easy as giving consent.<sup>74</sup> The EDPB issued guidelines in May 2020 that provide more details on the requirements for valid consent.<sup>75</sup>

d. Processing for Reasons Other than Consent

The GDPR also allows processing of personal data when it is necessary to comply with a legal obligation to which the controller is subject or when such processing is necessary for the performance of a task carried out to further the public interest.<sup>76</sup> The Commission states that national laws that were already in place before the COVID-19 pandemic or laws enacted or amended in response to it can provide a valid legal basis for processing personal data in a mobile app if they meet the requirements of the GDPR.<sup>77</sup> The legal obligation or public interest task must

---

<sup>67</sup> Id.

<sup>68</sup> Id. at 4, para. 3.3; ePrivacy Directive, art. 5, para. 3.

<sup>69</sup> App Guidance, *supra* note 4, at 4, para. 3.3.

<sup>70</sup> GDPR, art. 7, para. 4; recital 43.

<sup>71</sup> Id. recital 42.

<sup>72</sup> Id. art. 4, point (11).

<sup>73</sup> Id. recital 32.

<sup>74</sup> Id. art. 7, para. 3.

<sup>75</sup> EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679* (May 4, 2020), <https://perma.cc/XG4F-YMBL>. These guidelines update guidelines previously issued by the Article 29 Working Party in 2018, which were endorsed by the EDPB. See EDPB, *Guidelines 05/2020*, at 3.

<sup>76</sup> GDPR, art. 6, para. 1(c), (e).

<sup>77</sup> App Guidance, *supra* note 4, at 5, para 3.3.

be codified in either EU law or Member State law to which the controller is subject, and that legal basis must identify the purpose of the processing or the processing must be necessary for the performance of the task.<sup>78</sup> Furthermore, the legal basis must “meet an objective of public interest and be proportionate to the legitimate aim pursued.”<sup>79</sup> In the opinion of the Commission, a generic purpose of “prevention of further COVID-19 infections” is not specific enough for an app with contact tracing and warning functionalities. Instead, it proposes “retaining of the contacts of the persons who use the app and who may have been exposed to infection by COVID-19 in order to warn those persons who could have been potentially infected.”<sup>80</sup>

The Commission recommends not bundling functionalities and only using the data for the fight against COVID-19. If Member States would like to use the data for additional purposes such as scientific research and statistics, such purposes should be clearly communicated to the user and included in the legal basis.<sup>81</sup>

The Commission emphasizes that even if there is a valid legal basis that allows the processing of personal data to fight epidemics by national authorities, individuals must remain free to install or de-install a contact tracing and warning app.<sup>82</sup>

e. Automated Individual Decision-making

If the warnings are issued directly by the app, national authorities also need to abide by the requirements codified in the GDPR for automated individual decision-making.<sup>83</sup> The GDPR establishes a general prohibition for decision-making based solely on automated processing that has legal or similarly significant effects. “Solely” means that the decision is totally automated and there is no human review.<sup>84</sup> “Legal or similarly significant effects” means that the decision either affects a person’s legal status or rights, such as the denial of a social benefit, or has equivalent impact on an individual’s circumstances, behavior, or choices, or leads to exclusion/discrimination of an individual, such as the denial of an online credit application or access to education.<sup>85</sup> However, as an exception, decision-making based solely on automated processing may be performed when it is necessary for the performance of or entering into a contract, is authorized by EU or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the user’s rights and freedoms and legitimate interests, or is based on the user’s explicit consent.<sup>86</sup> In addition, for sensitive data such as health

---

<sup>78</sup> GDPR, art. 6, para. 3.

<sup>79</sup> Id.

<sup>80</sup> App Guidance, *supra* note 4, at 8, para. 3.6.

<sup>81</sup> Id.

<sup>82</sup> Id. at 5, para 3.3.

<sup>83</sup> Id.; GDPR, art. 22.

<sup>84</sup> Article 29 Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679* 20 (Feb. 2018), <https://perma.cc/LAGP-26NN>.

<sup>85</sup> Id. at 21.

<sup>86</sup> GDPR, art. 22, para. 2.

data, the processing may only take place when the user has consented or when it is necessary for reasons of substantial public interest and there are sufficient safeguards in place.<sup>87</sup>

f. Data Minimization

The Commission emphasizes that the apps must abide by the principle of data minimization, meaning that the processing of personal data should be adequate, relevant, and limited to what is necessary.<sup>88</sup> For example, an app with symptom checking or telemedicine functionality does not need access to the contact list stored on the device.<sup>89</sup> Mobile apps with contact tracing and warning functionality will generally require proximity data from the user. The Commission recommends the use of Bluetooth Low Energy (BLE) communications data or data generated by equivalent technology for this purpose.<sup>90</sup> In the opinion of the Commission, BLE, unlike geolocation data, is more precise, thereby minimizing the risk of having false positives, and avoids the possibility of tracking.<sup>91</sup> It should only be recorded when there is an actual risk of infection.<sup>92</sup> The Commission advises against the use of location data as it is not necessary for contact tracing.

With regard to the warning of people who have been in close contact with an infected person, the Commission proposes two solutions, a centralized and a decentralized solution. When a user has tested positive and inputs that information into the app, where it is subsequently stored, an automatic alert is sent to the close contacts (decentralized processing). The Commission recommends that the alert message should be drafted by the health authorities. Under the second option, arbitrary temporary identifiers that cannot directly identify the user are stored on a backend server held by the health authorities. Users who have been in close contact with someone who has tested positive receive an alert on their phone through the identifiers (centralized processing). For contact via phone or text message, health authorities would need additional consent of those users.<sup>93</sup> The Commission prefers the first solution as it aligns better with the principle of data minimization.<sup>94</sup> There is no need to reveal the identity of the infected person to the individuals who have been in close contact with him or her.<sup>95</sup>

---

<sup>87</sup> Id. art. 22, para. 4.

<sup>88</sup> App Guidance, *supra* note 4, at 5, para. 3.4; GDPR, art. 5, para. 1(c).

<sup>89</sup> App Guidance, *supra* note 4, at 5, para. 3.4.

<sup>90</sup> Id. at 6, para. 3.4.

<sup>91</sup> Id. at 6, para. 3.4. & 9, para. 3.9.

<sup>92</sup> Id. at 6, para. 3.4.

<sup>93</sup> Id.

<sup>94</sup> Id. at 7, para. 3.5

<sup>95</sup> Id.

g. Data Storage Limitation

Data should not be kept longer than necessary for the specific functionality of the app based on medical relevance and administrative processing.<sup>96</sup> That means that proximity data for apps with contact tracing and warning functionalities should be deleted after a maximum of one month (incubation period plus margin) or after a negative test result. It may be kept longer in an anonymized form. Only data that is necessary to fulfill the purpose of the app should be uploaded to the server of the health authorities.<sup>97</sup>

h. Data Security

With regard to data security, the Commission emphasizes encryption and pseudonymization of the data. It advises that the data be stored on the user's device in an encrypted form with state-of-the-art cryptographic techniques.<sup>98</sup> Such techniques could be symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, and homomorphic encryption, among others.<sup>99</sup> Proximity data should be encrypted and pseudonymized. When proximity data is collected via BLE, the Commission recommends establishing and storing temporary device IDs that change regularly instead of the actual ID.<sup>100</sup> Temporary IDs offer more protection against hacking and tracking. Additional security measures proposed are automatic deletion or anonymization of data after a certain time. In general, the more sensitive the data is, the more security is required. The EDPB additionally recommends that a mechanism be established to verify the status of users who log a positive test result in the app—for example, by providing a single-use code linked to a test station or health care professional.<sup>101</sup>

Furthermore, the Commission states that the source code should be published and be made available for review.<sup>102</sup> In the opinion of the Commission and the EDPB, such a review of the algorithm by independent experts will ensure fairness, accountability, and compliance with the law.<sup>103</sup>

3. *Development of a CEN Technical Specification*

The European Committee for Standardization (CEN) has been asked by the Commission to develop a new CEN technical specification for “Quality and Reliability of Health and Wellness

---

<sup>96</sup> Id. at 8, para. 3.7.

<sup>97</sup> Id.

<sup>98</sup> Id. at 8, para. 3.8.

<sup>99</sup> EDPB, *supra* note 26, at 16, no. 8.

<sup>100</sup> App Guidance, *supra* note 4, at 8, para. 3.8.

<sup>101</sup> EDPB, *supra* note 26, at 16, no. 8.

<sup>102</sup> App Guidance, *supra* note 4, at 9, para. 3.8.

<sup>103</sup> EDPB, *supra* note 26, para. 37.

Apps.”<sup>104</sup> It is slated to be completed in 2020 and is meant to provide app developers with a consistent set of criteria for such apps. CEN states that such a quality standard will “giv[e] users and health professionals confidence that the apps are fit for purpose, and provid[e] app developers easier access to European markets.”<sup>105</sup> The specification will be compatible with the world health informatics standards from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

#### 4. *Pan-European Privacy-Preserving Proximity Tracing Initiative*

The Pan-European Privacy-Preserving Proximity Tracing Initiative (PEPP-PT) is a consortium made up of various European firms and research institutions that is in the process of developing a software for national contact or proximity tracing apps to fight the spread of COVID-19.<sup>106</sup> Several European countries had reportedly announced they would use the software as a basis for developing their own COVID-19 app.<sup>107</sup> However, after a controversy over whether a centralized or a decentralized approach should be used and concerns over transparency, several partners dropped out and governments withdrew support.<sup>108</sup>

### **B. Use of Mobility Data**

Furthermore, the Commission recommends developing a common approach for the use of anonymized and aggregated mobility data to inform measures and exit strategies.<sup>109</sup> The EDPB emphasizes that preference should be given to the processing of anonymized data rather than personal data.<sup>110</sup> The eHealth Network plans to release a plan for a common approach in June 2020.<sup>111</sup> In particular, such mobility data can be used to map and predict the diffusion of the disease and its impact on health system needs in the Member States, optimize the effectiveness of measures to contain the spread of COVID-19, and address its effects. The Commission advises Member States to exchange best practices on the use of mobility data, share and compare modelling and predictions of the spread of the virus, and monitor the impact of measures to limit its spread.<sup>112</sup> It emphasizes that the appropriate use of anonymized and aggregated mobility data for modelling needs to be addressed and the methodology that providers used for anonymizing

---

<sup>104</sup> *Quality & Reliability for Health and Wellness Apps*, CEN, <https://perma.cc/HB7W-G72Y>.

<sup>105</sup> *Id.*

<sup>106</sup> *Pan-European Privacy-Preserving Proximity Tracing*, PEPP-PT, <https://perma.cc/LA59-URUB>.

<sup>107</sup> Douglas Busvine, *European Coronavirus App Platform Gains Traction With Governments*, Reuters (Apr. 17, 2020), <https://perma.cc/Z27T-9Z6F>.

<sup>108</sup> Douglas Busvine, *Rift Opens Over European Coronavirus Contact Tracing Apps*, Reuters (Apr. 20, 2020), <https://perma.cc/AQM6-VCK3>.

<sup>109</sup> Commission Recommendation (EU) 2020/518, *supra* note 4, at 14, para. 18.

<sup>110</sup> EDPB, *supra* note 26, para. 14.

<sup>111</sup> EHealth Network, *Mobile Applications*, *supra* note 5, at 24, point V.c.

<sup>112</sup> Commission Recommendation (EU) 2020/518, *supra* note 4, at 14, para. 19.

data must be checked for plausibility. Furthermore, safeguards need to be put in place to prevent de-anonymization.<sup>113</sup> The EDPB points out that robust anonymization requires examining

- whether data can be singled-out, meaning whether an individual can be isolated in a larger group based on the data;
- linkability; and
- inference, meaning whether unknown information about an individual can be deduced with significant probability.<sup>114</sup>

Data that was accidentally processed must be immediately and irreversibly deleted. All other data should be deleted after 90 days or no later than the end of the pandemic. Lastly, the mobility data should only be used for the aforementioned purposes and not be shared with third parties.<sup>115</sup>

---

<sup>113</sup> Id. at 14, para. 20.

<sup>114</sup> EDPB, supra note 26, para. 16.

<sup>115</sup> Commission Recommendation (EU) 2020/518, supra note 4, at 14, para. 20.

# England

Clare Feikert-Ahalt  
Senior Foreign Specialist

**SUMMARY** The UK has been one of the hardest hit countries in Europe in both numbers of deaths and cases of infection from COVID-19. The use and sharing of data is regulated by the Data Protection Act, which implements the European Union's General Data Protection Regulation. England is developing an app that will operate via Bluetooth and use a centralized system to alert individuals who have been in close proximity to a user who later reports symptoms of COVID-19. England has also developed a Test and Trace Program, which involves a significant number of people to track and trace the contacts of people who report symptoms of COVID-19 either online, through the app, or via the telephone. There is no new legislation to introduce the app, the use of which is entirely voluntary. While the government has faced criticism for not introducing legislation to underpin the app, it claims that new legislation is not necessary as the use of the app is entirely voluntary and that data is protected under the Data Protection Act 2018 and the Human Rights Act 1998.

## I. Introduction

The UK has been one of the most severely hit countries in Europe from COVID-19 in terms of both infections and deaths. As of May 22, 2020, 254,195 people in the UK had tested positive for COVID-19 and there had been 36,393 deaths confirmed with COVID-19 positive test results.<sup>1</sup>

A significant percentage of the UK's population has cell phones, with a study from Deloitte reporting that 88% of people in the UK own a smartphone.<sup>2</sup> With the high number of smartphones in use across the UK, an app to help automate the process to trace the contacts of individuals with symptoms of COVID-19 could help to reduce the spread of the disease, but this will only work if a significant number of people who have smartphones install the app. A poll from the *Observer* reported that 52% of people would download an app that enables contact tracing to be conducted automatically via their cell phones<sup>3</sup> while another poll indicated that 65% of people are willing to download such an app.<sup>4</sup>

---

<sup>1</sup> Cabinet Office Briefing Room, *Reducing the Spread of COVID-19*, <https://perma.cc/GAC8-7GR5>. The Office of National Statistics reported 41,020 deaths as of May 8 where COVID-19 was mentioned in the death certificate. Id.

<sup>2</sup> Deloitte, *Global Mobile Consumer Survey: UK Cut* (2019), <https://perma.cc/B5V8-QJPG>.

<sup>3</sup> Michael Savage, *Only 50% of Britons Would Download NHS Tracing App – Poll*, *The Observer* (London) (May 10, 2020), <https://perma.cc/NH4F-5SE5>.

<sup>4</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST (May 14, 2020), <https://perma.cc/5P6A-GXMW>.

While aspects of this report touch upon the four countries of the UK—England, Wales, Scotland, and Northern Ireland—the electronic measures taken by England to prevent the spread of COVID-19 will be the main focus.

The team responsible for the contact tracing app currently under development in England has stated that 60% of the population needs to download the app in order for it to be effective, although even a 50% uptake will help reduce infections and prevent the health care system from being overwhelmed.<sup>5</sup> As a point of reference, approximately 67% of cell phone users have downloaded WhatsApp.<sup>6</sup> The models estimating required participation exclude persons over 70 years of age, because they have lower smartphone usage and it is assumed they will typically follow the government’s advice to minimize contact with other people.<sup>7</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The UK incorporated the European Union’s General Data Protection Regulation (GDPR) into its national law through the Data Protection Act 2018 (the 2018 Act).<sup>8</sup> The 2018 Act contains provisions relating to general data processing, and the processing of data by law enforcement and the intelligence services. The 2018 Act also provides for regulatory oversight and enforcement mechanisms to ensure it is implemented properly. It regulates how personal information may be processed, “requiring personal data to be processed lawfully and fairly, on the basis of the data subject’s consent or another specified basis.”<sup>9</sup> The 2018 Act also requires that any data collected should be limited in scope, collected only as necessary for the reasons it is processed, accurate, and kept up to date. Any personal data must be stored in a manner that enables the identification of the data subject and held for no longer than necessary. Personal data must be processed in a way that ensures the security of the data and protects against unauthorized processing, accidental loss, destruction, or damage. The 2018 Act places a duty on the data controller to ensure the principles of the Act are complied with and demonstrate how this compliance is achieved.<sup>10</sup>

Individuals have a number of rights under the 2018 Act, including the right to obtain information about how their personal data is processed along with the right to have any inaccurate personal data corrected.<sup>11</sup> Individuals also have the right to have personal data held on them erased in certain circumstances, including if the data held is no longer necessary for the purposes that it

---

<sup>5</sup> Savage, *supra* note 3.

<sup>6</sup> Eleanor Lawrie, *Coronavirus: How Does Contact Tracing Work and Is My Data Safe?*, BBC News (May 12, 2020), <https://perma.cc/3HZE-GNGZ>.

<sup>7</sup> *Id.*

<sup>8</sup> Data Protection Act 2018, c. 12, <https://perma.cc/39Y3-H34A>.

<sup>9</sup> *Id.* § 2(1)(a).

<sup>10</sup> *Id.* Pt. 2, ch. 2.

<sup>11</sup> *Id.* § 2(1)(b).

was originally collected, if the individual withdraws consent, or if the data was processed unlawfully.<sup>12</sup>

Article 6(1)(d) of the GDPR provides that data may be lawfully processed for public health purposes if it is necessary:

- to protect the vital interests of the data subject or another natural purpose;
- for the performance of a task carried out in the public interest; and
- for reasons of public interest in the area of public health.<sup>13</sup>

The 2018 Act further requires that any such processing must be necessary to perform a function conferred on a person by a law, with the Health Protection (Coronavirus) Regulations 2020 providing an additional legal basis for processing data relating to COVID-19.<sup>14</sup> For health data, such processing must also be “necessary for reasons of substantial public interest.”<sup>15</sup>

## **B. Location Tracking**

The interpretation of “identifiable living individuals” includes those who can be identified using location data; thus, location data is considered to be personal data and the protections of the 2018 Act in relation to processing, storing, using, and sharing such data apply.<sup>16</sup>

The Investigatory Powers Act 2016 (the 2016 Act) provides the legal framework for the investigatory powers of law enforcement, public authorities, and the security and intelligence agencies of the UK to obtain communications and communications data. The 2016 Act includes location data under the term “secondary data”<sup>17</sup> and allows law enforcement to intercept, acquire, and retain these types of data in specified circumstances, such as in the interests of public safety or to protect public health.<sup>18</sup>

The 2016 Act also provides the Secretary of State with the ability to require telecommunications operators to retain internet connection records, which enable “law enforcement to identify the communications service to which a device has connected online.”<sup>19</sup>

---

<sup>12</sup> Id. Pt. 3, ch. 3.

<sup>13</sup> General Data Protection Regulation (GDPR), art.6, 2016 O.J. (L 119) 1, <https://perma.cc/7T85-89ZQ>.

<sup>14</sup> Data Protection Act 2018, § 8(c) and the Health Protection (Coronavirus) Regulations 2020, SI 2020/129, <https://perma.cc/5GJU-XYQ8>.

<sup>15</sup> Data Protection Act 2018, sched. 1 Pt. 2(6).

<sup>16</sup> Id. § 3.

<sup>17</sup> Investigatory Powers Act 2016, c. 25, § 263(2), <https://perma.cc/AML3-UT2J>.

<sup>18</sup> Id. § 61(1).

<sup>19</sup> *Judgment in Investigatory Powers Legal Challenge*, Home Office (July 29, 2019), <https://perma.cc/3JU8-5F5L>.

### III. Electronic Measures to Fight COVID-19 Spread

#### A. Contact Tracing App

The government has noted that the potential number of asymptomatic carriers of COVID-19 “indicate[s] that the spread of COVID-19 is too fast to be contained by manual contact tracing alone, but containment would be possible using a more efficient method involving a mobile app.”<sup>20</sup> In April 2020, the government announced that the National Health Service User Experience<sup>21</sup> (NHSX), the technology and research arm of NHS England and the Department of Health and Social Care, and researchers at Oxford University had worked together to develop an app that works on mobile devices to help public health authorities to manage COVID-19.<sup>22</sup> It is currently testing the app and plans to release it in England in the beginning of June 2020.<sup>23</sup> The aim of the app is to

. . . automate key parts of public health contact tracing by offering a proximity cascade system that can help slow transmission of the COVID-19 virus. This will save lives, reduce pressure on the NHS, help return people to normal life and mitigate damage to the economy.

The app also aims to preserve individual and group privacy, be tolerant to various malicious users and minimise the risks of pseudonymous subgroup reidentification. Importantly, it is driven by and informs expert epidemiological modelling, which in turn drives public policy.<sup>24</sup>

In order for the app to be the most effective, the government has noted that it needs to be paired with manual contact tracing and widespread testing to ensure that the data is accurate.<sup>25</sup>

The app was designed not to interfere with other apps or drain phone batteries, and to protect users’ privacy and device security. The app does not work on some older-model cell phones, such as those that do not support Bluetooth Low Energy (BLE), leading to concerns that vulnerable groups may be excluded from using the app.<sup>26</sup> The app is also reportedly incompatible with the

---

<sup>20</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, supra note 4.

<sup>21</sup> Jess Morley, *All the Things We Like about the Centre for Data Ethics and Innovation’s New Strategy*, Technology in the NHS (Mar. 21, 2019), <https://perma.cc/83JW-65DC>.

<sup>22</sup> *Stop the Spread of Coronavirus*, NHS, <https://perma.cc/T7YQ-JVKC>. See also Hasan Chowdhury, Matthew Field & Margi Murphy, *NHS Contact Tracing App: How Does It Work and When Can You Download It?*, Telegraph (London) (May 12, 2020), <https://perma.cc/5Z9J-FMXS>; *Who We Are*, NHSX, <https://perma.cc/4EMD-JMXM>; Matthew Gould, *Digital Contact Tracing: Protecting the NHS and Saving Lives*, NHSX (Apr. 24, 2020), <https://perma.cc/B4C9-UG7R>.

<sup>23</sup> *Coronavirus: UK Track and Trace System in Place from June – PM*, BBC News (May 20, 2020), <https://perma.cc/Q97H-D5H4>.

<sup>24</sup> Dr. Ian Levy, *The Security Behind the NHS Contact Tracing App*, National Cyber Security Centre (May 4, 2020), <https://perma.cc/F7GT-VH5B>.

<sup>25</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, supra note 4.

<sup>26</sup> *UK Government Covid Tracking App: What We Found*, Privacy International (May 7, 2020), <https://perma.cc/UU8V-YSKR>.

operating system of newer Huawei phones.<sup>27</sup> The source code of the app has been made available to the public.<sup>28</sup>

### 1. Operation of the App

Once installed, the app creates an anonymous, fixed identifier for the user's cell phone.<sup>29</sup> The app generates anonymous tokens and records when two people who have installed the app on their mobile devices are within a certain distance from one another for longer than a specified period of time.<sup>30</sup> The app does not use location data, although it does prompt users to provide the first half of their postcode (zip code) to enable the NHS to use the data to see where hotspots are emerging.<sup>31</sup>

The government has decided to permit users to self-report symptoms as "self-diagnosis can reduce by days, the time it takes a potentially infectious person to isolate. This is critical to the management of the spread of the disease, under the assumptions in the UK's model."<sup>32</sup> The Parliamentary Office of Science and Technology (POST) has noted that while permitting such self-reporting can reduce the exposure of others to infection while test results are being processed, it could also lead to a number of false positive alerts and that fast testing will be key to ensuring public confidence in the advice provided by the app.<sup>33</sup>

The NHS has reiterated this, stating that the reason for allowing individuals to self-report symptoms on the app is because

[t]he epidemiological models tell us that any delay in isolating people who are showing symptoms has a real effect on the spread of the virus. The less delay there is, the better the NHS can manage the spread. No testing regime can give immediate results, so the public health professionals have taken the decision to ask people to declare symptoms that are likely to be coronavirus.<sup>34</sup>

The app asks self-reporting users a series of structured questions to determine if they have symptoms of COVID-19.<sup>35</sup> The app then "runs [any contact events with other users of the app] through a sophisticated risk model to work out the encounters that are high risk from a virus transmission point of view."<sup>36</sup> This appears to be based on users having prolonged close contact

---

<sup>27</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, supra note 4.

<sup>28</sup> Terence Eden, *The Code Behind the NHS Covid-19 App*, NHSX (May 8, 2020), <https://perma.cc/9GQ7-SMVM>.

<sup>29</sup> Chowdhury et al., supra note 22.

<sup>30</sup> National Cyber Security Centre, *High Level Privacy and Security Design for NHS COVID-19 Contact Tracing App* (May 2020), <https://perma.cc/RR3M-X5MH>.

<sup>31</sup> Chowdhury et al., supra note 22.

<sup>32</sup> National Cyber Security Centre, supra note 30, at 3.

<sup>33</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, supra note 4.

<sup>34</sup> Levy, supra note 244.

<sup>35</sup> Id.

<sup>36</sup> Id.

with one another.<sup>37</sup> The data is shared to a centralized health service database<sup>38</sup> and all users who were in “significant contact” within the past 28 days<sup>39</sup> of the user reporting symptoms are alerted. The app sends recommendations to these users that vary “depend[ing] on the evolving context and approach.”<sup>40</sup> The POST has stated that

[c]riteria used to determine whether a user is at risk are based on an understanding of how different levels of exposure (e.g. closeness and duration of contact) affect risk of infection. The app could also make recommendations to manage this risk, such as checking symptoms, reporting to a test centre or self-isolating.<sup>41</sup>

The identity of the person reporting symptoms is not revealed to other app users; the notification simply informs them that they have been in proximity to a person with symptoms of COVID-19<sup>42</sup> and to take certain measures.

In cases where the person reporting symptoms later receives a negative test, contacts are informed through the app that it was a false positive. If the user has a positive test result, the contacts are asked to self-isolate for 14 days and to get tested themselves. If the user reporting symptoms does not get a test and not many of his or her contacts report symptoms, it is considered that this “statistically suggests” the user was not positive and their contacts are informed they do not need to continue to self isolate. If the opposite is true, and a number of the user’s contacts report symptoms, it is considered that the person was probably infected and that their contacts should consider self-isolation.<sup>43</sup>

There are reports that the app is unable to work properly if another app is being actively used, as it will only start broadcasting its identifier if an identifier is broadcast from another phone. The result of this is that “two iPhone users [who] sat next to each other on a train, both playing the game Candy Crush, would fail to register as a contact, unless a third phone was nearby with the app open.”<sup>44</sup>

## 2. *Centralized Model*

The app uses a centralized model, which means the matching process occurs on a centralized computer server.<sup>45</sup> A decentralized model, which was proposed by Apple and Google, would have limited the data exchange to individual users’ cell phones and was rejected by the NHSX,

---

<sup>37</sup> Id. at 4.

<sup>38</sup> Chowdhury et al., *supra* note 222.

<sup>39</sup> Id.

<sup>40</sup> Gould, *supra* note 22.

<sup>41</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, *supra* note 4.

<sup>42</sup> Lawrie, *supra* note 6.

<sup>43</sup> Levy, *supra* note 24.

<sup>44</sup> Dan Sabbage, Alex Hern & Kate Proctor, *UK Racing to Improve Contact-tracing App’s Privacy Safeguards*, *The Guardian* (London) (May 5, 2020), <https://perma.cc/4UAM-MHN4>.

<sup>45</sup> Lawrie, *supra* note 6.

which stated the centralized system will provide it with more insight into how the disease spreads and improve the efficiency of the app.<sup>46</sup>

### 3. *Voluntary Uptake*

Installation and use of the app is entirely voluntary, although a document from the body established to consider the ethics of the app has noted that it is possible the app could be a requirement for individuals returning to work or using public transportation.<sup>47</sup> The app also allows people to voluntarily opt in to report their symptoms and when they started feeling unwell.<sup>48</sup>

### 4. *Trial*

The NHS's contact tracing app was tested on the Isle of Wight, where the island's 80,000 households were asked to download the app beginning May 5, 2020. The Isle of Wight was selected as the place for trial due to its elderly population and low numbers of cell phone users. The BBC reported that if the trial "is successful despite these challenges then that will show it can work across the UK."<sup>49</sup>

The app was downloaded 55,000 times within the first week of being launched, although, as the device does not track location, some downloads may have occurred outside the Isle of Wight.<sup>50</sup> By May 14, 2020, around half of the Island's population had reportedly downloaded the app.<sup>51</sup> Any person who voluntarily reports their symptoms during this trial will be brought a test for COVID-19 within 24 hours, according to the *Telegraph*.<sup>52</sup>

The test revealed that the app affected the battery power of certain iPhones.<sup>53</sup> Concerns have also been raised that delays of up to a week for people to receive test results may undermine the effectiveness of the app. The government has noted that using Bluetooth has both limitations and risks. Bluetooth may miss connections if phones are in bags or pockets that weaken the signal, which in turn can make the distance measurements unreliable.<sup>54</sup> Keeping Bluetooth turned on can also pose a security risk. The phone's unique identifier could be collected by third parties in

---

<sup>46</sup> Id.

<sup>47</sup> NHS COVID-19 App: Ethics Advisory Board Terms of Reference, NHSX, <https://perma.cc/7FDY-J8ND>.

<sup>48</sup> Chowdhury et al., *supra* note 22.

<sup>49</sup> Lawrie, *supra* note 6.

<sup>50</sup> *Coronavirus: NHS Virus-Tracing App Downloaded 55,000 Times*, BBC News (May 11, 2020), <https://perma.cc/LLF4-Q2XC>. See also Savage, *supra* note 3.

<sup>51</sup> Lawrie, *supra* note 6.

<sup>52</sup> Chowdhury et al., *supra* note 22.

<sup>53</sup> Savage, *supra* note 3.

<sup>54</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, *supra* note 4.

the area for malicious purposes and it may render phones vulnerable to hacking and malicious software uploading.<sup>55</sup>

## **B. Contact Tracing for People Without the App**

The app is only one part of the UK's approach to tackling COVID-19. The government has also established the COVID-19 Test and Trace Taskforce,<sup>56</sup> which is responsible for ensuring that people who develop symptoms of COVID-19 have fast access to a test to determine if they have the virus. The Test and Trace Taskforce will also conduct manual contact tracing, which was used at the start of the outbreak before the cases of COVID-19 became so widespread,<sup>57</sup> to alert people who have had close contact with the person. The aim of this is to

- identify who is infected more precisely, to reduce the number of people who are self-isolating with symptoms but who are not actually infected, and to ensure those who are infected continue to take stringent self-isolation measures; and
- ensure those who have been in recent close contact with an infected person receive rapid advice and, if necessary, self-isolate, quickly breaking the transmission chain.<sup>58</sup>

The government has noted that it is necessary for testing and contact tracing to

. . . operate quickly for maximum effect, because relative to other diseases (for example SARS) a proportion of COVID-19 sufferers almost certainly become infectious to others before symptoms are displayed; and almost all sufferers are maximally infectious to others as soon as their symptoms begin even if these are initially mild.<sup>59</sup>

The government is working to ensure that all components of contact tracing are

. . . fully joined up to make the system as seamless as possible for members of the public and to ensure the app complements more traditional measures. This coordinated approach will help protect vulnerable groups, including those who cannot or do not want to use digital tools.<sup>60</sup>

People with symptoms who see their doctor or receive a positive test result for COVID-19 are being referred by their doctor to the contact tracing team, and individuals will also be able to report their symptoms and order testing for COVID-19 over the phone or online.<sup>61</sup> The contact tracing team will then contact the person by phone or email to get a list of people who they have

---

<sup>55</sup> Id.

<sup>56</sup> Press Release, Department of Health and Social Care, New Chair of Coronavirus 'Test and Trace' Programme Appointed (May 7, 2020), <https://perma.cc/2B29-XX5K>.

<sup>57</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, *supra* note 4.

<sup>58</sup> HM Government, *Our Plan to Rebuild: The UK Government's COVID-19 Recovery Strategy*, CP 239, at 38 (May 2020), <https://perma.cc/6UDR-T8BY>.

<sup>59</sup> Id.

<sup>60</sup> *NHS COVID-19 App*, NHSX, <https://perma.cc/4P9R-MA52>.

<sup>61</sup> Lawrie, *supra* note 6.

been in close contact with and places they have visited over the days prior to displaying symptoms, or receiving the positive test result.<sup>62</sup> The contact tracer will then call or email individuals on the list and advise them to self-isolate for seven days and call the contact tracing team if they display any symptoms, at which point their contacts will be tracked and asked to self-isolate.<sup>63</sup> The design allows the notification that people self-isolate based on the self-reported symptoms of other users to be reversed at a later date if the person later tests negative for COVID-19.<sup>64</sup>

The app and contact tracing requires a significant amount of human resources to operate effectively. The government aims to have 25,000 people to trace the contacts of people testing positive for COVID-19, with the aim being to track the contacts of 10,000 COVID-19 cases per day by June 1, 2020.<sup>65</sup>

The UK is also planning to use the Joint Biosecurity Centre to provide analysis and assessment of outbreaks of COVID-19 at the community level in a manner that enables a rapid intervention before the outbreak grows further.<sup>66</sup>

### C. Compatibility of Measures with Privacy Rights

The government's COVID-19 Recovery Strategy states that the measures being taken "will involve an unprecedented degree of data-collection . . . [and] the government will enact robust safety measures."<sup>67</sup> These safety measures are not mentioned in the UK Government's COVID-19 Recovery Strategy. Information collected by the app and through the Test and Trace program will be compiled together and "form part of a core national COVID-19 dataset."<sup>68</sup>

The app does not collect any personally identifiable information about the user, nor is the location of the user collected. Users of the app are anonymous, and data collected by the app from users is used for "NHS care, management, evaluation and research."<sup>69</sup> As use of the app is not mandatory, the NHSX notes that it may be deleted at any time by its user<sup>70</sup> and any record stored on the user's phone is deleted after 28 days if the user, or his or her contacts, have made no reports of symptoms or contact with anyone with COVID-19.<sup>71</sup>

---

<sup>62</sup> Nick Phin, *Coronavirus (COVID-19) Expert Interview: What Is Contact Tracing?*, Public Health England (Feb. 13, 2020), <https://perma.cc/UUH8-5FRH>; Press Release, Department of Health and Social Care, *Coronavirus Test, Track and Trace Plan Launched on Isle of Wight* (May 4, 2020), <https://perma.cc/GE29-AUG8>.

<sup>63</sup> Press Release, *supra* note 62.

<sup>64</sup> Levy, *supra* note 244.

<sup>65</sup> *Coronavirus: UK Track and Trace System in Place from June – PM*, BBC News, *supra* note 28.

<sup>66</sup> HM Government, *Our Plan to Rebuild*, *supra* note 58, at 37.

<sup>67</sup> *Id.* at 39.

<sup>68</sup> *Id.*

<sup>69</sup> *NHS COVID-19 App*, NHSX, *supra* note 60.

<sup>70</sup> *Id.*

<sup>71</sup> Levy, *supra* note 244.

The centralized data collection point has also been designed to ensure security of the data held there, although this data is anonymous “and communicates out to other NHS systems through privacy preserving gateways, so data in the app data can’t be linked to other data the NHS holds.”<sup>72</sup> The government has noted that location data for each individual is unique and thus the individual may be able to be identified from their location data alone, even with the data being stored anonymously.<sup>73</sup>

Concerns have been raised the anonymized data in a centralized model “could be de-anonymized and used for surveillance purposes.”<sup>74</sup> The Ada Lovelace Institute and Parliament’s Joint Committee on Human Rights have recommended that primary legislation be introduced to “impose strict purpose and time limitations on technical solutions to support transition from the crisis”<sup>75</sup> and to “provide legal clarity about how data gathered by a contact-tracing app could be used, stored and disposed of . . . [to] increase confidence in the app, which would increase uptake and improve the app’s efficiency.”<sup>76</sup>

The National Cyber Security Centre has stated that the use of anonymized data collected by the app being used to re-identify users is very low. It notes that in other circumstances the re-identification of anonymized users can sometimes occur where information about an individual is available, such as their age, gender and location, and such data can only apply to a particular person. The National Cyber Security Centre says that that it does not collect enough information to enable such re-identification of users of the app to occur. It does note that users may have to be identified to the NHS, for example for them to take a test, but that “if that happens through the app, the system uses a privacy preserving gateway to be able to link a test to an app Installation ID anonymously”<sup>77</sup> and will not connect this information to the person’s identity or NHS record.

The Centre for Data Ethics and Innovation (CDEI) has noted issues arising as a result of the limited development time for the app:

The speed of development means that working transparently and enabling scrutiny is not straightforward. New decisions are taken every day, and sometimes changed a day later as new evidence or technical challenges emerge. Explaining this to the public without

---

<sup>72</sup> Id.

<sup>73</sup> *Contact Tracing Apps for COVID-19*, UK Parliament POST, supra note 4.

<sup>74</sup> Isobel Asher Hamilton, *170 Cybersecurity Experts Warn That British Government’s Contact Tracing App Could Be Used to Surveil People Even after Coronavirus Has Gone*, Business Insider (Apr. 29, 2020), <https://perma.cc/SJF4-DTHF>.

<sup>75</sup> Ada Lovelace Institute, *Exit Through the App Store?* (Apr. 20, 2020), <https://perma.cc/3X8E-YQZ4>.

<sup>76</sup> House of Lords Library, *Contact-tracing Apps: Legislating for Data Protection?* (May 13, 2020), <https://perma.cc/VFR2-CZQT>.

<sup>77</sup> Levy, supra note 244.

undermining confidence is hard—particularly at a time when people want to be reassured that their governments have the crisis in hand.<sup>78</sup>

While expressing concern over certain aspects of the app, the Joint Committee on Human Rights has noted that the benefit provided by the app may outweigh the risks to privacy:

The privacy concerns about the contact tracing app are certainly pertinent to human rights, especially Article 8, which protects the right to private and family life. However, Governments also have a responsibility to protect Article 2 ECHR, the right to life. If the app demonstrably protects lives and can help to ease the constraints of a lockdown, then this is a very relevant factor in assessing the proportionality of any interference with the right to a private life under article 8 ECHR.<sup>79</sup>

The Joint Committee on Human Rights, as noted above, has called for the government to introduce a legislative basis for the app to help create public trust and possible participation, along with requiring a formal human rights assessment to occur. It has noted that

this degree of formal rights balancing is lacking at present, being left to the NHSX team and its advisory bodies. In particular, Parliamentary scrutiny would allow for consideration as to whether the use of a centralised system, as opposed to a decentralised system, is reasonable and proportionate. The implementation and oversight of this app must, in our view, be urgently placed on a legislative footing; if rolled out without being governed by a clear legislative framework it risks not complying with the provisions of the ECHR.<sup>80</sup>

Despite calls for the app to be placed on a legislative basis, the government has maintained that this is not required because use of the app is voluntary and protections currently provided by the Data Protection Act and Human Rights Act are sufficient.<sup>81</sup>

#### D. Oversight Mechanisms

The NHS established an App Oversight Board and an independent Ethics Advisory Board<sup>82</sup> (EAB) to ensure that any questions about ethics, privacy, and security “are properly explored and addressed.”<sup>83</sup> The EAB provides advice, guidance, and recommendations on ethical issues raised by the use of the app to the App Oversight Board.<sup>84</sup>

---

<sup>78</sup> Centre for Data Ethics and Innovation, *The Ethics of Contact Tracing Apps: International Perspectives* (May 12, 2020), <https://perma.cc/TJG2-JB49>.

<sup>79</sup> House of Commons & House of Lords Joint Committee on Human Rights, *Human Rights and the Government's Response to Covid-19: Digital Contact Tracing*, (2019-21) HC 343 HL 59 ¶ 3, <https://perma.cc/8ECH-3L9P>.

<sup>80</sup> *Id.* at 3.

<sup>81</sup> *Id.* See also *Coronavirus: Security Flaws Found in NHS Contact-tracing App*, BBC News (May 19, 2020), <https://perma.cc/XR8R-GFMB>.

<sup>82</sup> NHS COVID-19 App, Ethics Advisory Board Terms of Reference, *supra* note 47.

<sup>83</sup> *NHS COVID-19 App*, NHSX, *supra* note 60.

<sup>84</sup> *NHS COVID-19 App*, Ethics Advisory Board Terms of Reference, *supra* note 47.

The CDEI has noted that this decision making should be “guided by an ethical approach, identifying the trade-offs and endeavouring to reflect the reasonable expectations of citizens.”<sup>85</sup> It has worked with the EAB to establish core principles that will help to guide the development of the app. The EAB has tentatively published a “Public Trust Matrix” that details “key components of trustworthy data use and set[s] out the issues to be addressed within them.”<sup>86</sup>

---

<sup>85</sup> Centre for Data Ethics and Innovation, *supra* note 78.

<sup>86</sup> NHS COVID-19 App, Ethics Advisory Board Terms of Reference, *supra* note 47, App. 1.

# France

*Nicolas Boring*  
*Foreign Law Specialist*

**SUMMARY** The right to privacy is enshrined in French law, but is now primarily governed by the European Union’s General Data Protection Regulation (GDPR). The GDPR’s provisions have been incorporated into the 1978 *Loi Informatique et Libertés*, France’s original information privacy law. Information technology must not infringe upon human identity, human rights, privacy, or individual or public freedoms. Furthermore, personal data must be processed lawfully and fairly, and data that falls under the GDPR should also be processed in a manner that is transparent for the data subject. Mishandling personal data is a criminal offense under the French Penal Code. The main enforcement authority for issues of technology and privacy is the *Commission nationale de l’informatique et des libertés* (CNIL), an independent agency.

As a general rule, data may not be retained in a manner that allows the data subjects’ identification beyond the time necessary to fulfill the purpose for which it was collected. Location tracking of individuals falls squarely in the GDPR’s definition of “personal data,” and may only be collected and processed under the conditions laid out by that regulation. The *Loi Informatique et Libertés* contains several provisions regarding the handling of personal data related to health care, which may be collected and used only for certain limited purposes.

The French government has developed two electronic databases to help in the fight against the spread of COVID-19. The SI-DEP database is a secure platform where all COVID-19 test results are recorded to ensure that all positive cases are taken care of by the French health care system. The “Contact COVID” database collects information on positive cases, such as where they live and work, and who they are in regular contact with, to facilitate contact tracing. Additionally, the French government is deploying a smartphone app, called StopCovid, to help with contact tracing. This app, which is used on a purely voluntary basis, relies on Bluetooth technology to notify its user if he or she has been in close proximity to a person infected by COVID-19 for 15 minutes or more. This app is controversial and has elicited concerns over whether it is lawful under French and European privacy laws. The CNIL has issued two opinions declaring it to be legal, so long as certain conditions are respected. The French Parliament approved the app’s deployment in a nonbinding vote on May 27, 2020.

## I. Introduction

France, like many other countries, has been hard-hit by the COVID-19 pandemic. According to the French government, there have been 149,071 confirmed cases of COVID-19 in France as of May 28, 2020, and a total of 28,662 deaths from that disease.<sup>1</sup> France has taken several important

---

<sup>1</sup> COVID-19, *Données au 28/05/2020*, Gouvernement.fr (May 28, 2020), <https://perma.cc/Q8PK-PTVD>.

measures to fight COVID-19's spread, including declaring a new type of state of emergency in March 2020.<sup>2</sup>

Contact tracing appears to be an important tool in the fight against COVID-19, and France is using some technological solutions to facilitate or supplement this process. One of these solutions is the deployment of a smartphone app, capitalizing on the broad penetration of smartphones in the French market. Indeed, about 95% of French residents had a mobile phone in 2019, including approximately 77% who had a smartphone.<sup>3</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The French Civil Code provides that all people have a right to privacy.<sup>4</sup> However, data protection in France is primarily governed by the European Union's (EU's) General Data Protection Regulation (GDPR),<sup>5</sup> and by the domestic *Loi Informatique et Libertés* (Law on Information Technology and Freedoms).<sup>6</sup> The latter was originally adopted in 1978, but has been amended many times since. For example, it was amended in 2004 to incorporate provisions from the EU's ePrivacy Directive,<sup>7</sup> and it was amended in 2018 to be consistent with the GDPR and the EU's Directive 2016/680 on processing of personal data.<sup>8</sup> The *Loi Informatique et Libertés* states that information technology "should not infringe upon human identity, human rights, privacy, or public or individual freedoms."<sup>9</sup> Personal data must be processed lawfully and fairly, and data that falls under the GDPR should also be processed in a manner that is transparent for the data

---

<sup>2</sup> Nicolas Boring, *France: Government Adopts Law Declaring and Defining a 'State of Health Emergency,'* Global Legal Monitor (Mar. 30, 2020), <https://perma.cc/22VB-CM6Z>.

<sup>3</sup> *Proportion d'individus disposant d'un téléphone mobile en France de 2005 à 2019*, Statista (Mar. 9, 2020), <https://perma.cc/RWG9-FJSM>; *Répartition de la population en France de 2011 à 2019, selon le type de téléphone mobile utilisé*, Statista (Mar. 5, 2020), <https://perma.cc/BM53-J67A>.

<sup>4</sup> Code civil, art. 9, <https://perma.cc/UPQ8-MH6K>.

<sup>5</sup> General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, <https://perma.cc/7T85-89ZQ>.

<sup>6</sup> Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (as amended) (*Loi Informatique et Libertés*), <https://perma.cc/N8EV-FZV9>.

<sup>7</sup> Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Aug. 6, 2004), <https://perma.cc/FPZ7-DBA6>.

<sup>8</sup> Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (June 20, 2018), <https://perma.cc/2Y25-G7ZW>; Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel (Dec. 12, 2018), <https://perma.cc/7U58-XB42>.

<sup>9</sup> *Loi Informatique et Libertés*, art. 1.

subject.<sup>10</sup> Data may not be used in a manner that is incompatible with the explicit and legitimate purposes for which it was collected.<sup>11</sup>

Mishandling personal data in or through a computerized system, whether intentionally or by negligence, is punishable under the French Penal Code.<sup>12</sup> Someone who violates the rules set out in the GDPR or the Loi Informatique et Libertés can be sentenced to a fine of up to €300,000 (about US\$327,300) and up to five years in jail.<sup>13</sup>

The Loi Informatique et Libertés set up the Commission nationale de l'informatique et des libertés (CNIL) (National Commission on Information Technology and Freedoms), an independent agency tasked with enforcing regulatory or legislative texts regarding the use of personal data.<sup>14</sup> The CNIL also provides advisory opinions to the government, and informs the public on data privacy issues.<sup>15</sup>

## **B. Data Retention**

As a general rule, data may not be retained in a manner that allows the data subjects' identification beyond the time necessary to fulfill the purpose for which it was collected.<sup>16</sup> The main exception is that data, even personal information, may be retained for archival purposes, for historical or scientific research, or for statistical purposes. Even within this exception, however, the data must be kept in a manner that complies with the GDPR, and it may not be used to make decisions concerning the data subjects.<sup>17</sup> Additionally, data must be kept in a manner that adequately protects personal information from being lost, destroyed, damaged, or used in an illegal or unauthorized manner.<sup>18</sup>

Data that is found to be inaccurate with regard to the purpose for which it was collected should be immediately corrected or erased.<sup>19</sup> Additionally, data subjects have a right to demand that their personal data be erased.<sup>20</sup> Furthermore, the CNIL has the authority to demand that data be corrected or erased if it finds that the GDPR or other legal requirements have not been respected.<sup>21</sup>

---

<sup>10</sup> Id. art. 4.

<sup>11</sup> Id.

<sup>12</sup> Code pénal, arts. 226-16 to 226-24, <https://perma.cc/UCG5-CHKV>.

<sup>13</sup> Id.

<sup>14</sup> Loi Informatique et Libertés, art. 8.

<sup>15</sup> Id.

<sup>16</sup> Id. art. 4.

<sup>17</sup> Id.

<sup>18</sup> Id.

<sup>19</sup> Id.

<sup>20</sup> Id. arts. 51, 106.

<sup>21</sup> Id. art. 20.

### C. Location Tracking

Location tracking of individuals falls squarely in the GDPR's definition of "personal data," and is in fact one of the criteria listed to define an "identifiable natural person."<sup>22</sup> Location tracking in France is therefore primarily governed by the GDPR and the Loi Informatique et Libertés. Location tracking data may only be processed if at least one of the following conditions is fulfilled:

- The data subject has explicitly given consent under conditions defined in the GDPR,
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- Processing is necessary for compliance with a legal obligation,
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person,
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular when the data subject is a child.<sup>23</sup>

### D. Data Related to Health Care

The Loi Informatique et Libertés contains several provisions regarding the handling of personal data related to health care. Personal health care data may only be collected and processed for a purpose of public benefit, such as ensuring high quality and safety standards for medication and health care practices.<sup>24</sup> Organizations that wish to collect or process personal health care data must either provide prior notice to the CNIL if the collection and processing fall within certain published guidelines, or request the CNIL's prior authorization if they fall outside these guidelines.<sup>25</sup> An exemption exists, however, for organizations that collect or process data for the sole purpose of responding to a health emergency.<sup>26</sup> This exemption only applies to organizations that have a public service mission and are on a list established by the Minister of Health, with the

---

<sup>22</sup> General Data Protection Regulation (GDPR), art. 4, point (1).

<sup>23</sup> Id. art. 6; Loi Informatique et Libertés, art. 5.

<sup>24</sup> Loi Informatique et Libertés, art. 66.

<sup>25</sup> Id.

<sup>26</sup> Id. art. 67.

CNIL's advice.<sup>27</sup> In any case, health care professionals who provide data from their patients to an organization authorized to collect this data must do so in a manner that guarantees confidentiality.<sup>28</sup> If the results of the data processing are made public, it must be in such a manner that the direct or indirect identification of the data subjects is impossible.<sup>29</sup> Furthermore, the data subjects must be informed in accordance with the requirements of the GDPR.<sup>30</sup> The Loi Informatiques et Libertés contains similar provisions for data collection and processing for the purposes of health-care-related research.<sup>31</sup>

### III. Electronic Measures to Fight COVID-19 Spread

#### A. Contact-COVID and SI-DEP Databases

On May 13, 2020, the French government deployed two electronic databases to help fight the spread of COVID-19.<sup>32</sup> These databases were authorized by Parliament two days before, as part of a law that extended the state of emergency related to the COVID-19 pandemic.<sup>33</sup> Indeed, this law authorized the implementation of a computerized database “for the sole purposes of fighting against the spread of the COVID-19 epidemic, and for the amount of time strictly necessary for this goal or, at most, a period of six months after the end of the state of emergency [related to the epidemic].”<sup>34</sup> As an exception to the legislation on the confidentiality of personal medical information, this database may include relevant personal information even without the data subject's consent.<sup>35</sup> The Constitutional Council, which judges the constitutionality of French laws, was asked to review the bill before it became law. In its opinion, the Council stated that while aspects of the proposed database violated the right to privacy, these violations were necessary for, and justified by, the fight against the COVID-19 pandemic.<sup>36</sup> The Council did warn, however, that “a particular vigilance must be observed” with regard to the use of personal data of a medical nature.<sup>37</sup>

---

<sup>27</sup> Id.

<sup>28</sup> Id. art. 68.

<sup>29</sup> Id.

<sup>30</sup> Id. art. 69.

<sup>31</sup> Id. arts. 72 to 77.

<sup>32</sup> Décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, May 13, 2020, <https://perma.cc/LY6U-U6NS>; *Coronavirus : le fichier de suivi des malades "Contact Covid" entre en vigueur*, L'Express (May 13, 2020), <https://perma.cc/5UBG-3GTT>.

<sup>33</sup> Loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, May 12, 2020, <https://perma.cc/EZD9-5MSP>.

<sup>34</sup> Id. art. 11.

<sup>35</sup> Id.

<sup>36</sup> Conseil constitutionnel, decision No. 2020-800DC, May 11, 2020, <https://perma.cc/ZP6Q-99XX>.

<sup>37</sup> Id.

The two databases that came out of this legislative authorization are called “Contact COVID” and SI-DEP.<sup>38</sup> SI-DEP, which stands for *Système d’Informations de DEPistage* (Screening Information System) is a secure platform where all COVID-19 test results are recorded to ensure that all positive cases are taken care of by the French health care system.<sup>39</sup> “Contact COVID” collects information on positive cases, and is meant to facilitate contact tracing. The information collected includes the data subject’s identity and contact information, the identity and contact information of people they are close to, their frequent contacts, their workplace, whether they display clinical symptoms, information on their general state of health, and whether they are homeless or in an otherwise vulnerable situation.<sup>40</sup>

Contact COVID is managed by the national health insurance organization, while SI-DEP is managed by a partnership between the Ministry of Health, the Paris public hospital system, the French public health agency, and medical laboratories throughout the country.<sup>41</sup> The data in both systems may only be accessed by medical professionals who are subject to duties of medical confidentiality: doctors, pharmacists, testing laboratory technicians, and other professionals accredited by the national health insurance organization, the national public health agency, or regional public health agencies.<sup>42</sup>

## B. StopCovid Smartphone App

The French government deployed a contact tracing app, called “StopCovid,” on June 2, 2020.<sup>43</sup> This app uses Bluetooth technology, rather than geolocation, to detect whether the user was, for a period of 15 minutes or more, within one meter of a person infected with COVID-19.<sup>44</sup> Installation and use of this app is on a purely voluntary basis.<sup>45</sup>

This app has been in development since April 2020, but was delayed by technical difficulties as well as legal uncertainties.<sup>46</sup> Unlike many other countries, France opted for a system in which data was stored on a central server controlled by the public health authorities. This led to

---

<sup>38</sup> *Contact-COVID et SI-DEP, les outils numériques du dépistage COVID-19*, Ministère des Solidarités et de la Santé (May 26, 2020), <https://perma.cc/8HR8-7XVA>.

<sup>39</sup> Id.

<sup>40</sup> Id.

<sup>41</sup> Id.

<sup>42</sup> Id.

<sup>43</sup> *Déconfinement: Edouard Philippe "invite" les Français à utiliser l'application de traçage StopCovid, disponible à partir du 2 juin*, France Info (May 28, 2020), <https://perma.cc/B5LD-BWX2>.

<sup>44</sup> Id.

<sup>45</sup> Fabien Soyez, *StopCovid: Ce qu'il faut savoir sur l'application de traçage du gouvernement*, CNET France (May 27, 2020), <https://perma.cc/T35T-LYSM>.

<sup>46</sup> Damien Leloup, *Application StopCovid: La France isolée dans son bras de fer avec Apple et Google*, Le Monde (Apr. 28, 2020), <https://perma.cc/N3DZ-S82W>.

disagreements with both Google and Apple, the designers of the two most common operating systems for smartphones, who favored a more decentralized concept.<sup>47</sup>

The legal uncertainties around the StopCovid app mostly had to do with whether it is an illegal infringement of the right to privacy. To clarify this issue, the government sought advice from the CNIL twice. The CNIL issued one opinion on April 24, 2020, and the second on May 25, 2020.

In its April 24th opinion, the CNIL found that the proposed app did not infringe the GDPR or other privacy legislation, so long as it is truly useful to deal with the COVID-19 crisis and certain privacy guarantees are built in.<sup>48</sup> The CNIL stated that use of the app needed to be purely voluntary, and that there should be no negative repercussion for not using it.<sup>49</sup> Furthermore, according to the CNIL, this app must be temporary, and the data gathered must be preserved only for a limited amount of time.<sup>50</sup> The CNIL also made some recommendations to ensure the security of the data collected, including the advice that only state-of-the-art cryptographic algorithms should be used to ensure the integrity and confidentiality of the app and database.<sup>51</sup> In its May 25th opinion, the CNIL found that the recommendations that it had issued on April 24 appeared to have been followed, and that the app could be legally deployed.<sup>52</sup> However, the CNIL required that the app's actual utility be evaluated after its deployment, and stated that the continued use of StopCovid should be contingent on the results of regular evaluations.<sup>53</sup> The CNIL also recommended that the app's source code be made public in its entirety, though details of the security measures and software parameters should remain secret.<sup>54</sup>

In an effort to quell the controversies and promote public acceptance of StopCovid, the government submitted its deployment to a nonbinding vote by Parliament on May 27.<sup>55</sup> In defending the app before the National Assembly, the government specified that StopCovid was only one tool out of several to fight against the COVID-19 epidemic, and that its purpose was to complement rather than replace the work of contact tracing teams.<sup>56</sup> The National Assembly

---

<sup>47</sup> Id.

<sup>48</sup> CNIL, Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » (Apr. 24, 2020), <https://perma.cc/99NP-H5WU>.

<sup>49</sup> Id. at 5.

<sup>50</sup> Id. at 7.

<sup>51</sup> Id. at 10.

<sup>52</sup> CNIL, Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (May 25, 2020), <https://perma.cc/SU5V-3F7A>.

<sup>53</sup> Id. at 4.

<sup>54</sup> Id at 12.

<sup>55</sup> Elsa Bembaron, *L'application StopCovid approuvée à l'Assemblée et au Sénat*, Le Figaro (May 27, 2020), <https://perma.cc/3JPX-6PUG>.

<sup>56</sup> Assemblée Nationale, *Compte rendu intégral, Séance du mercredi 27 mai 2020* (May 27, 2020), <https://perma.cc/WU3C-QRXG>.

approved the deployment of StopCovid by 338 votes against 215.<sup>57</sup> The Senate also expressed its approval.<sup>58</sup>

---

<sup>57</sup> Id.

<sup>58</sup> Elsa Bembaron, *supra* note 55.

# Iceland

*Elin Hofverberg*  
*Foreign Law Specialist*

**SUMMARY** Privacy is a constitutionally protected right under Icelandic law. As a European Economic Area member, Iceland is bound by some EU legislation, and has implemented both the General Data Protection Regulation (GDPR) and the Directive on Privacy and Electronic Communications. Under the GDPR, Iceland permits the collection, storage, and sharing of personal data (including location data) in a limited number of cases, such as when there is public interest or following consent.

As of May 22, 2020, Iceland only had two active cases of COVID-19 infection, with 1,791 patients recovered and ten fatalities, making it one of the countries globally that has most successfully managed to stem the spread of the disease. Iceland has launched a COVID-19 transmission app to contact trace infections. The app tracks and saves the location of users on their smartphones. If a user is later confirmed infected with COVID-19, the Icelandic Contact Tracing Team requests access to the location data from the phone. While the app has been downloaded by 40% of the population, it has mainly served to complement ordinary contact tracing methods.

## I. Introduction

### A. COVID-19 in Numbers

Iceland is one of the world's smallest independent nations. It is an island in the North Atlantic sea with approximately 350,000 inhabitants.<sup>1</sup>

Iceland is considered one of the countries that have, so far, successfully limited the spread of COVID-19 within its populace.<sup>2</sup> Iceland reported its first COVID-19 case on February 28, 2020.<sup>3</sup> Iceland has, as of May 22, 2020, reported 1,803 confirmed cases and 10 fatalities from COVID-19.<sup>4</sup> Of the total confirmed cases, 1,791 patients have recovered.<sup>5</sup> Currently, there are only two active cases, and the country has not recorded any new cases since May 12, 2020.<sup>6</sup> There are currently

---

<sup>1</sup> *The World Factbook: Iceland*, CIA, <https://perma.cc/PES2-Y39T>.

<sup>2</sup> Thomas K. Grose, *What Iceland Can Teach the World About Minimizing COVID-19*, US News (May 4, 2020), <https://perma.cc/628Z-NTG3>.

<sup>3</sup> *COVID-19 in Iceland – Statistics*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., <https://perma.cc/E967-55UV>.

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

no patients with COVID-19 treated in hospitals or intensive care units.<sup>7</sup> Also as of May 22, 2020, 58,295 persons have been tested for COVID-19 in Iceland.<sup>8</sup> Only the Faroe Islands (part of Denmark) and Gibraltar (part of the United Kingdom) have tested more residents per capita.<sup>9</sup>

## B. Smartphone Use

Smartphone use is widespread in Iceland, with the number of Icelandic cell phone subscriptions outnumbering the total population.<sup>10</sup> With 238,395 contract subscriptions, about 80% of all cell phone users are using the 4G network.<sup>11</sup> It is unclear how willing the population is to share the data.

## C. The *Rakning C-19* App

On April 19, 2020, Iceland introduced a mobile app to trace people with COVID-19.<sup>12</sup> The app, *Rakning C-19*,<sup>13</sup> is available via the Apple Store,<sup>14</sup> as well as Google Play.<sup>15</sup> The app was designed on behalf of the Contingency, Department of Civil Protection and Emergency Management.<sup>16</sup> Reportedly, close to 40% of all Icelanders have downloaded the COVID-19 app, making it the most widely downloaded app in any one country as measured per capita.<sup>17</sup> However, some commentators claim that it has not been a “game changer.”<sup>18</sup> Reportedly, the purpose of the app is to help users refresh their memory, and representatives from Iceland treat the app more as a complement to ordinary contact tracing than as a stand-alone approach.<sup>19</sup> There is no requirement to use the app for either infected or uninfected persons. Persons in quarantine are also not required to use the app. Persons in quarantine and isolation are, however, required to check in

---

<sup>7</sup> Id.

<sup>8</sup> Id.

<sup>9</sup> *COVID-19 Coronavirus Pandemic*, Worldometer (May 22, 2020), <https://perma.cc/93LJ-8FNK>.

<sup>10</sup> *Tölfræði um íslenska fjarskiptamarkaðinn Fyrri helmingur ársins 2019* [Statistics on the Icelandic Telecommunications Market: The First Half of 2019] (Nov. 2019), PFS, <https://perma.cc/4VVP-2JNW>.

<sup>11</sup> Id. at 18; see also *Statistics Report on the Icelandic Telecommunications Market in 2019*, Iceland Post & Telecom Admin. (May 14, 2020), <https://perma.cc/TE9N-KJCF>.

<sup>12</sup> *Contagion Tracing Is a Community Affair*, Directorate of Health Iceland and Dep’t of Civ. Protection & Emergency Mgmt., <https://perma.cc/4DDX-ADMM>.

<sup>13</sup> *Rakning C-19 appið*, Directorate of Health Iceland and Dep’t of Civ. Protection & Emergency Mgmt., <https://perma.cc/V55B-9SNG>. *Rakning* means tracking/counting in Icelandic.

<sup>14</sup> *Rakning C-19*, Apple Store, <https://perma.cc/V4SY-LHZP>.

<sup>15</sup> *Rakning C-19*, Google Play, <https://perma.cc/KE5D-TDWH>.

<sup>16</sup> *Contagion Tracing Is a Community Affair*, Directorate of Health Iceland and Dep’t of Civ. Protection & Emergency Mgmt., *supra* note 12.

<sup>17</sup> Covid Tracing Tracker – Read Only, MIT Tech. Rev., [https://docs.google.com/spreadsheets/d/1ATaIASO8KtZMx\\_zJREoOvFh0nmB-sAqJ1-CjVRSCow/edit#gid=0](https://docs.google.com/spreadsheets/d/1ATaIASO8KtZMx_zJREoOvFh0nmB-sAqJ1-CjVRSCow/edit#gid=0); Bobbie Johnson, *Nearly 40% of Icelanders Are Using a Covid App – and It Hasn’t Helped Much*, MIT Tech. Rev. (May 11, 2020), <https://perma.cc/G22G-FQAK>.

<sup>18</sup> Id.

<sup>19</sup> *How Iceland Handles Contact Tracing*, NPR (May 17, 2020), <https://perma.cc/EBW8-2QQZ>.

with their local health care providers daily.<sup>20</sup> Iceland started testing about four weeks before it had a confirmed case.<sup>21</sup> Reportedly, Iceland remains one of the countries with the lowest COVID-19 fatalities measured per capita.<sup>22</sup>

#### D. Travel Restrictions in Force

Iceland, as a Schengen Area nation, normally allows European Union citizens to enter the country without border checks.<sup>23</sup> Nevertheless, on April 24, 2020, it closed its borders to noncitizens and currently requires everyone arriving in Iceland, regardless of nationality, to self-quarantine for 14 days.<sup>24</sup> If subject to self-quarantine, a person must stay home for 14 days but may use a taxi to visit a doctor or a dentist.<sup>25</sup> A person in quarantine may not, however, shop for groceries in person or take public transport.<sup>26</sup> Quarantine is not a total isolation, but a person in quarantine should limit contacts with others to a minimum.<sup>27</sup> In addition to international travelers, persons who have come in contact with a person with COVID-19 also must self-quarantine.<sup>28</sup> As of May 22, 2020, a total of 20,194 persons have completed a self-quarantine in Iceland, and another 886 are currently self-quarantining.<sup>29</sup> Self-quarantining is less restrictive than isolation, but persons must follow the guidelines.<sup>30</sup> Under Icelandic law, persons who have COVID-19 must isolate for the duration of their illness, meaning they must stay at home alone or together with a person who is also isolating.<sup>31</sup> Persons who are not sick may isolate together with the sick individual but should not come within one meter (three feet) of the sick person, and if another person in the household

---

<sup>20</sup> Directorate of Health Iceland, *Instructions for Persons Under Home-Based Quarantine*, <https://perma.cc/7LAH-VLJH>; Directorate of Health Iceland, *Instructions for Persons Under Home-Based Isolation*, <https://perma.cc/V5TQ-MRPG>.

<sup>21</sup> Todd Bishop, COVID-19 Lessons from Iceland: How One Nordic Country Has All but Stopped the Virus in Its Tracks, *GeekWire* (May 17, 2020), <https://perma.cc/RKS6-LG4G>.

<sup>22</sup> *Id.*

<sup>23</sup> *Schengen Area*, Eur. Commission, Migration & Home Aff., <https://perma.cc/5SVB-B68C>.

<sup>24</sup> Press Release, Government of Iceland, *Iceland Introduces Temporary Schengen Border Controls and 14-Day Quarantine for International Arrivals* (Apr. 22, 2020), <https://perma.cc/3XV2-GJ9T>.

<sup>25</sup> *How Does Quarantine Work?*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., <https://perma.cc/35QE-7C5M>; Directorate of Health Iceland, *Instructions for Persons Under Home-Based Quarantine*, *supra* note 20.

<sup>26</sup> Directorate of Health Iceland, *Instructions for Persons Under Home-Based Quarantine*, *supra* note 20.

<sup>27</sup> *Id.*

<sup>28</sup> *How Does Quarantine Work?*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., *supra* note 25.

<sup>29</sup> *COVID-19 in Iceland – Statistics*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., *supra* note 3.

<sup>30</sup> Directorate of Health Iceland, *Instructions for Persons Under Home-Based Quarantine*, *supra* note 20.

<sup>31</sup> *How Does Isolation Work?*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., <https://perma.cc/KE53-E625>; Directorate of Health Iceland, *Instructions for Persons Under Home-Based Quarantine*, *supra* note 20.

contracts the disease, the isolation will be prolonged.<sup>32</sup> For the duration of their isolation, the person's primary care provider will be in contact with the person daily.<sup>33</sup> As of May 22, 2020, two persons are currently in isolation.<sup>34</sup> Violating quarantine and isolation rules is punishable by monetary fines of between ISK50,000 (about US\$370) and ISK500,000 (about US\$3,700), depending on the severity of the violation.<sup>35</sup> In addition, under the General Penal Code:

causing a danger that a communicable disease will break out or be spread between people by violating the provisions of law on preventive measures against communicable diseases, or precautionary rules on these matters issued by the authorities, shall be [punishable by imprisonment] for up to 3 years. The punishment may take the form of up to 6 years' imprisonment in the case of diseases which the authorities have taken special measures to contain or to prevent their entering the country.<sup>36</sup>

Currently, the *Rakning C-19* app is not used to monitor compliance with the quarantine or isolation rules.

## II. Legal Framework

### A. Privacy and Data Protection

Iceland regulates privacy rights and data protection. The Icelandic Constitution guarantees the right to privacy in article 71.<sup>37</sup> However, such rights may be limited "by statutory provisions if this is urgently necessary for the protection of the rights of others."<sup>38</sup> Iceland is also a signatory to the European Convention on Human Rights, which guarantees the right to privacy in article 8.<sup>39</sup> As a European Economic Area (EEA) member, Iceland is bound by the General Data Protection Regulation (GDPR).<sup>40</sup> Moreover, because of its EEA membership, Iceland must also

---

<sup>32</sup> Id.

<sup>33</sup> Id.

<sup>34</sup> *COVID-19 in Iceland – Statistics*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., supra note 3.

<sup>35</sup> Ríkissáksóknari, Brot gegn sóttvarnarlögum og reglum settum samkvæmt þeim, sbr. 19. gr. sóttvarnalaga nr. 19/1997, vegna heimsfaraldurs COVID-1 (Mar. 27, 2020), <https://perma.cc/3S5X-N94P>.

<sup>36</sup> General Penal Code 1940 No. 19 (12 February) as amended, art. 175 [hereinafter General Penal Code], <https://perma.cc/6HDC-XYNU>.

<sup>37</sup> Constitution of the Republic of Iceland (No. 33, 17 June 1944, as amended 30 May 1984, 31 May 1991, 28 June 1995 and 24 June 1999), <https://perma.cc/HFS6-A3DL> [in English].

<sup>38</sup> Id.

<sup>39</sup> European Convention on Human Rights, 213 U.N.T.S. 221 (entered into force Mar. 9, 1953), <https://perma.cc/XP8C-Z7HJ>.

<sup>40</sup> EEA Joint Committee No. 154/2018 of 6 July 2018 Amending Annex XI (Electronic Communication, Audiovisual Services and Information Society) and Protocol 37 (Containing the List Provided for in Article 101) to the EEA Agreement [2018/1022], 2018 O.J. (L 183) 23, <https://perma.cc/W5ZR-BZ5P> (in English); <https://perma.cc/VV5M-CBRL> (in Icelandic); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal

follow all of the EU legislation on electronic communications.<sup>41</sup> Iceland transposed the GDPR into Icelandic law through the Act on Data Protection and Processing of Personal Data (Act No. 90/2018) in 2018.<sup>42</sup> The purpose of the Act on Data Protection and Processing of Personal Data is to “promote that personal data be treated in accordance with fundamental principles and rules on the protection of personal data and respect for private life, and to ensure the reliability and quality of such data and their free flow within the EEA single market.”<sup>43</sup>

Personal data is defined in article 3.2 as:

“Information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

Sensitive personal data is defined in article 3.3 as data that reveals racial or ethnic origin, political opinions, philosophical beliefs, trade union membership; data related to physical or mental health (including substance abuse); data on a person’s sex life or sexual orientation; genetic data; and biometric data.<sup>44</sup>

Both personal and sensitive data may be processed on the basis of consent.<sup>45</sup> Consent (to the treatment of personal data) is defined as: “A freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative

---

Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), [2018/1022], 2016 O.J. (L 119) 1, <https://perma.cc/9TR8-YS5R>.

<sup>41</sup> Decision of the EEA Joint Committee No 80/2003 of 20 June 2003 Amending Annex XI (Telecommunication Services) to the EEA Agreement, 2003 O.J. (L 257) 31 [hereinafter Decision of the EEA Joint Committee No 80/2003], <https://perma.cc/2UWT-AKPS>; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) 2002 O.J. (L 201) 37 [hereinafter Directive 2002/58/EC], <https://perma.cc/YCY4-M68Z>.

<sup>42</sup> Act on Data Protection and the Processing of Personal Data (No. 90 of 27 June 2018), <https://perma.cc/T52A-NWPB> (unofficial English translation by the Data Protection Authority). For an overview of the Icelandic implementation of the GDPR, see Ingvi Snær Einarsson, *Iceland – National GDPR Implementation Overview*, DataGuidance (Nov. 2019), <https://perma.cc/8L97-RW3G>. According to article 2 of the implementing legislation (Act on Data Protection and Processing of Personal Data (Act No. 90/2018)), “as it is incorporated into the Agreement on the European Economic Area, shall apply in Iceland with the adaptations resulting from the Decision of the EEA Joint Committee amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement.”

<sup>43</sup> Act on Data Protection and the Processing of Personal Data art. 1.

<sup>44</sup> Id. art. 3.3.

<sup>45</sup> Id. arts. 9 and 10.

action, signifies agreement to the processing of personal data relating to him or her.”<sup>46</sup> A person must be at least 13 years of age to give consent.<sup>47</sup>

In addition to processing based on consent, personal data may also be processed if it is necessary for the performance of a contract, compliance with a legal obligation, protecting a vital interest of the person the data pertains to or of another person, or a task undertaken in the public interest.<sup>48</sup> Article 52 specifically states that personal data may be used to fight or prevent contagious diseases.<sup>49</sup> Article 14, which deals with electronic surveillance, states that it must be carried out for an objective purpose.<sup>50</sup>

## **B. Data Retention and Location Tracking**

Data retention is authorized by a number of Icelandic statutes, including the Telecommunications Act,<sup>51</sup> Patients’ Rights Act (medical records),<sup>52</sup> and contagious diseases legislation.<sup>53</sup> Moreover, as an EEA member, Iceland has an obligation to implement the Directive on Privacy and Electronic Communications.<sup>54</sup> This obligation was carried out by implementation of the Telecommunications Act.<sup>55</sup>

Location tracking and electronic surveillance is regulated in law, specifically in the Law on Electronic Communications and the Rules on Electronic Surveillance.<sup>56</sup> Typically, the tracking of individuals is restricted. Tracking may only be used if there is a legitimate need, such as “significant security factors, by consent of the data subject, or according to other specific authorization, e.g. by wage contracts or provisions of law.”<sup>57</sup> In addition, tracking a vehicle

---

<sup>46</sup> Id. art. 3.3.

<sup>47</sup> Id. art. 10.

<sup>48</sup> Id. art. 9.

<sup>49</sup> Id. art. 52.

<sup>50</sup> Id. art. 14.

<sup>51</sup> Electronic Communications Act No. 81, 26 March 2003, art. 43 [hereinafter Electronic Communications Act], <https://perma.cc/74QZ-7PNT>.

<sup>52</sup> Patients’ Rights Act, No. 74/1997, as amended by Act No. 77/2000, No. 40/2007, No. 41/2007, No. 112/2008, No. 55/2009, No. 162/2010, No. 126/2011, No. 34/2012 and No. 44/2014, <https://perma.cc/QQ6V-J4EN> (unofficial English translation by the Ministry of Justice).

<sup>53</sup> Act on Health Security and Communicable Diseases, No. 19/1997, as amended by Act No. 90/2000, No. 93/2002, No. 164/2002, No. 55/2004, No. 43/2007, No. 167/2007, No. 88/2008, No. 112/2008, No. 162/2010, No. 126/2011 and No. 117/2016 [hereinafter Act on Health Security and Communicable Diseases], <https://perma.cc/3785-TYNX>.

<sup>54</sup> Decision of the EEA Joint Committee No 80/2003; Directive 2002/58/EC.

<sup>55</sup> Electronic Communications Act.

<sup>56</sup> Electronic Communications Act art. 43; Rules No. 837/2006 on Electronic Surveillance, <https://perma.cc/2FQG-UWCV>.

<sup>57</sup> Rules No. 837/2006 on Electronic Surveillance art. 8.

requires a lawful and reasonable objective for needing to track the location of the driver.<sup>58</sup> Monitoring attendance either at school or at work (such as a work schedule) is typically not restricted by this legislation.<sup>59</sup> Electronic surveillance must only “be carried out for specified, explicit and legitimate purposes, such as security or property protection.”<sup>60</sup> The police may also share and use data under a limited set of circumstances.<sup>61</sup> For example, the police may use electronic surveillance of persons who are suspected of having committed a crime that carries a sentence of at least one year.<sup>62</sup> Personal information that pertains to a person’s medical records is regulated by the Patients’ Rights Act.<sup>63</sup>

Responses to epidemics are regulated by the Act on Health Security and Communicable Diseases.<sup>64</sup> Article 3 states that the Chief Epidemiologist is responsible for maintaining a record of persons with communicable diseases and also has a right to access health record information in accordance with the Medical Act.<sup>65</sup> However, the information must be made unidentifiable.<sup>66</sup> Retaining personal data is one of the main duties of the Chief Epidemiologist, “in order to monitor the spread of communicable diseases, by gathering detailed data on their diagnosis from laboratories, hospitals and physicians.”<sup>67</sup> Article 7 of the Act on Health Security and Communicable Diseases regulates the individual’s responsibility in a pandemic, which includes tracing.<sup>68</sup> However, there is no obligation on behalf of the individual, or right on behalf of the authorities, to go through the person’s phone to trace the person’s whereabouts.<sup>69</sup> The Chief Epidemiologist may, however, request help from the police if the person does not comply with measures to stop the spread, but measures that may be taken by the police include only isolation measures, not measures focused on tracing the spread.<sup>70</sup>

---

<sup>58</sup> Id.

<sup>59</sup> Id. art. 1.

<sup>60</sup> Id. art. 4.

<sup>61</sup> Regulation on Management of Personal Information by the Police, No. 322 9 April 2001 with Amendment No. 926/2004, arts. 6 and 7 [hereinafter Regulation on Management of Personal Information by the Police], <https://perma.cc/NV5K-SX44> (unofficial translation by Ministry of Justice of Iceland), as well as Amendment No. 926/2004, <https://perma.cc/W4VK-GJQF>.

<sup>62</sup> Rules No. 837/2006 on Electronic Surveillance. See also Regulation on Management of Personal Information by the Police, as well as Amendment No. 926/2004, and the General Penal Code.

<sup>63</sup> Patients’ Rights Act, No. 74/1997, as amended by Acts No. 77/2000, No. 40/2007, No. 41/2007, No. 112/2008, No. 55/2009, No. 162/2010, No. 126/2011, No. 34/2012 and No. 44/2014, <https://perma.cc/qq6V-J4EN> (unofficial English translation by the Ministry of Justice).

<sup>64</sup> Act on Health Security and Communicable Diseases.

<sup>65</sup> Id. art. 3.

<sup>66</sup> Id.

<sup>67</sup> Id. art. 5.

<sup>68</sup> Id. art. 7.

<sup>69</sup> Id.

<sup>70</sup> Id. art. 14.

### C. Enforcement

Enforcement of data protection rules is carried out by the Icelandic Data Protection Authority.<sup>71</sup> The Authority is independent and oversees the implementation and compliance with the GDPR.<sup>72</sup> It also issues daily as well as administrative fines for noncompliance.<sup>73</sup> Daily fines can be up to ISK200,000 (about US\$1,480) for each day that a party violates an Authority order.<sup>74</sup> Administrative fines range from ISK100,000 (about US\$740) to ISK1.2 billion (about US\$8.9 million), and are typically issued to the designated data controller of the corporation or institution that handles personal data in breach of the personal data legislation.<sup>75</sup> Both physical persons and legal entities can be fined.<sup>76</sup>

On May 19, 2020, the Authority issued a comment regarding the sharing of health information, asking the Icelandic Parliament to define the scope of the legal protection.<sup>77</sup>

### III. Electronic Measures to Fight COVID-19 Spread

As discussed in section I.C. above, Iceland has developed a smartphone app, the *Rakning-19* app, to respond to the COVID-19 pandemic. The app has received international recognition as being one of the least invasive apps from a privacy perspective.<sup>78</sup>

The app collects location data and retains it for 30 days on the user's smartphone.<sup>79</sup> To use the app, the smart phone must allow GPS tracking.<sup>80</sup> It does not track who you have been in contact with, as the data is only saved on the user's phone, and the Department of Civil Protection and Emergency Management's Contact Tracing Team sends a request to users who have been diagnosed with COVID-19 to share its previously recorded data with the Contact Tracing Team Database.<sup>81</sup> To share the data, an individual must type his or her ID number into the app.<sup>82</sup> Once

---

<sup>71</sup> Act on Data Protection and the Processing of Personal Data art. 1.

<sup>72</sup> Id. art. 38.

<sup>73</sup> Id. arts. 45 and 46.

<sup>74</sup> Id. art. 45.

<sup>75</sup> Id. art 46.

<sup>76</sup> Id.

<sup>77</sup> *Álit um skrár Embættis landlæknis*, Personuvernd (May 19, 2020), <https://perma.cc/E66E-FVTV>; *Álit um skrár Embættis landlæknis: Mál nr. 2020010064*, Personuvernd (May 19, 2020), <https://perma.cc/VM9E-LZ86>.

<sup>78</sup> Patrick Howell O'Neill et al., *A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them*, MIT Tech. Rev. (May 7, 2020), <https://perma.cc/GH99-JWER>.

<sup>79</sup> *Contagion Tracing Is a Community Affair*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., supra note 12.

<sup>80</sup> Id.

<sup>81</sup> Id.

<sup>82</sup> Id.

shared, the Contact Tracing Team will store the data for 14 days.<sup>83</sup> According to the privacy statement for the app, the data controller is the Icelandic Department of Health.<sup>84</sup>

Although the Contingency Agency developed the *Rakning-19* app with the purpose of tracing the spread of COVID-19 in Iceland, it is not the primary source for contact tracing. Use of the app remains voluntary, whereas daily calls with the local health care provider are mandatory.<sup>85</sup> Iceland has focused on tracking persons who are confirmed as infected with COVID-19 or who have been in direct contact with a person who has been confirmed as infected with COVID-19.<sup>86</sup>

---

<sup>83</sup> *Id.*

<sup>84</sup> *Privacy Statement*, Directorate of Health Iceland and Dep't of Civ. Protection & Emergency Mgmt., <https://perma.cc/U4L8-J95F>.

<sup>85</sup> Directorate of Health Iceland, *Instructions for Persons Under Home-Based Quarantine*, *supra* note 20; Directorate of Health Iceland, *Instructions for Persons Under Home-Based Isolation*, *supra* note 20.

<sup>86</sup> *How Iceland Handles Contact Tracing*, NPR (May 17, 2020), *supra* note 19.

# Italy

*Dante Figueroa*  
*Senior Legal Information Analyst*

**SUMMARY** Since the breakout of the COVID-19 pandemic, Italy has put in place a number of initiatives to trace, store, and share information on traffic and location data of telephone users in order to alleviate the effects of the pandemic. A national task force composed of different professionals is currently reviewing a national plan with proposals that would be implemented by legislation. The proposed measures include the use of apps on a voluntary and anonymous basis by citizens, as well as tracing and data-sharing technologies. Issues concerning respect for European Union law and Italian constitutional standards are being weighed in the decision to implement new technological measures.

## I. Introduction

### A. Current Statistics on COVID-19

According to Italy's Health Ministry, as of May 22, 2020, the current situation in the country with respect to COVID-19 is as follows:<sup>1</sup>

- Currently positive: 59,322 cases.
- Dead from COVID-19: 32,616 cases.
- Recovered from COVID-19: 136,720 cases.

### B. Mobile Phone Statistics

As of 2020, about 44 million Italians are smartphone users.<sup>2</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The Italian Constitution<sup>3</sup> guarantees the inviolable freedom and confidentiality of correspondence and of every other form of communication. Other legislation and regulations protect privacy rights and data. The main legislative instruments are the EU Code on Protection

---

<sup>1</sup> *Coronavirus: La Situazione Attuale*, Ministero della Salute (last updated May 22, 2020), <https://perma.cc/B3Q2-QWTY>.

<sup>2</sup> Statista, *Mobile Data Consumption in Italy*, <https://perma.cc/2742-UWCF>.

<sup>3</sup> Costituzione Italiana art. 15, <https://perma.cc/UJ8M-F2GS> (in Italian), <https://perma.cc/69KR-A7L8> (English translation).

of Personal Data, which was adapted by Italy's national legislation in 2003,<sup>4</sup> and Legislative Decree No. 101 of 2018,<sup>5</sup> which implemented the EU's General Data Protection Regulation (GDPR)<sup>6</sup> and which broadly provides that personal data processed for public interest purposes or pursuant to official authority may be disseminated or communicated to entities that process such data for other purposes only under qualified criteria.<sup>7</sup>

Legislative Decree No. 101 of August 10, 2018, generally states that personal data may be collected provided that certain guarantees are undertaken considering the purposes for the gathering of the data—specifically, identification of encryption and security techniques including pseudonymization, minimization measures, specifications for selective access to data, and any other measures necessary to guarantee the rights of interested parties.<sup>8</sup> In general, Italian legislation and regulations applicable to the collection and use of personal data mandate that personal data must be treated in a correct and lawful manner according to the express and legitimate purposes for which it was collected and must be preserved in a manner that allows interested parties full access to it and the opportunity to update it when necessary, and that an adequate level of safety and protection from unauthorized access and use must be guaranteed.<sup>9</sup>

In addition, Italy's Personal Data Protection Code provides that in the case of a personal data breach, providers of electronic communication services that are accessible to the public must give notice of such breach to the authorities without delay.<sup>10</sup> When the breach entails prejudice to the

---

<sup>4</sup> The EU Code on Protection of Personal Data was made directly applicable in Italy by the Codice in Materia di Protezione dei Dati Personali, approved by Decreto Legislativo 30 Giugno 2003, n.196 recante il "Codice in materia di Protezione dei Dati Personali", G.U., July 29, 2003, <https://perma.cc/AGJ9-3V84>, <https://perma.cc/3MYV-A3KN> (English translation).

<sup>5</sup> Decreto Legislativo 10 Agosto 2018, n. 101, Disposizioni per l'Adeguamento della Normativa Nazionale alle Disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla Protezione delle Persone Fisiche con riguardo al Trattamento dei Dati Personali, nonche' alla Libera Circolazione di tali Dati e che Abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati), G.U. Sept. 4, 2018, no. 205, <https://perma.cc/37DP-TWY6>.

<sup>6</sup> General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, <https://perma.cc/7T85-89ZQ>.

<sup>7</sup> Decreto Legislativo 10 agosto 2018, no. 101, art. 2 para. 1(f) (adding art. 2-ter (3)).

<sup>8</sup> Decreto Legislativo 10 agosto 2018, n. 101, art. 2 para. 1(f) (adding art. 2-septies(5)).

<sup>9</sup> Decreto Legislativo 18 maggio 2018, n. 51, Attuazione della Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativa alla Protezione delle Persone Fisiche con Riguardo al Trattamento dei Dati Personali da parte delle Autorita' Competenti a fini di Prevenzione, Indagine, Accertamento e Perseguimento di Reati o Esecuzione di Sanzioni Penali, nonche' alla Libera Circolazione di tali Dati e che Abroga la Decisione Quadro 2008/977/GAI del Consiglio, art. 3(1), G.U. May 24, 2018, no.119, <https://perma.cc/E6T2-X657>.

<sup>10</sup> Decreto Legislativo 28 Maggio 2012, n. 69, Modifiche al Decreto Legislativo 30 Giugno 2003, n. 196, recante Codice in materia di Protezione dei Dati Personali in Attuazione delle Direttive 2009/136/CE, in materia di Trattamento dei Dati Personali e Tutela della Vita Privata nel Settore delle Comunicazioni Elettroniche, e 2009/140/CE in materia di Reti e Servizi di Comunicazione Elettronica e del Regolamento (CE) n. 2006/2004 sulla Cooperazione tra le Autorita' Nazionali Responsabili dell'Esecuzione della Normativa a Tutela dei Consumatori, art. 1(3), G.U. May 31, 2012, <https://perma.cc/8N5Z-R5NU>.

personal data or the confidentiality of a party, the provider must also give prompt notice to such party.<sup>11</sup>

The Italian Data Protection Authority (DPA),<sup>12</sup> an independent administrative authority established by Law No. 675 of December 31, 1996, is the supervisory authority responsible for monitoring application of the General Data Protection Regulation.<sup>13</sup> The DPA is regulated by the Personal Data Protection Code.

## B. Data Retention and Location Tracking

Law No. 167 of 2017 regulates data retention in Italy.<sup>14</sup> That law implements EU directives and amends provisions of the Italian Criminal Procedure Code and other legislation to state that telecommunication operators must retain “telephone and telematic traffic data as well as data relating to unanswered calls” for a period of 72 months.<sup>15</sup> The requirement that such voluminous data be retained for this length of time has been criticized on privacy grounds.<sup>16</sup>

The European Data Portal contains information on the portions of Italian territory for which specific COVID-19 containment measures have been adopted.<sup>17</sup> In the case of Italy,<sup>18</sup> mobile carriers are reportedly sharing data with health authorities to fight the coronavirus by monitoring whether people are complying with lockdowns or other movement restrictions.<sup>19</sup> This data is said to be “anonymous and aggregated,” and “make[s] it possible to map concentrations and movements of customers in ‘hot zones’ where COVID-19 has taken hold.”<sup>20</sup> Italians mobile carriers Telecom Italia, Vodafone, and WindTre have offered to gather and deliver aggregated data to the authorities in order to monitor people’s movements.<sup>21</sup>

---

<sup>11</sup> Id.

<sup>12</sup> *Coronavirus: Information from the Italian Supervisory Authority*, Garante per la Protezione dei Dati Personali, <https://perma.cc/6UEJ-TDZ7>.

<sup>13</sup> Regulation No. 2016/679, art. 51.

<sup>14</sup> Legge 20 novembre 2017, n. 167 Disposizioni per l’Adempimento degli Obblighi Derivanti dall’Appartenenza dell’Italia all’Unione Europea - Legge Europea 2017, G.U., Nov. 27, 2017, <https://perma.cc/JNG6-MPV6>.

<sup>15</sup> Id. art. 24(1).

<sup>16</sup> Luigi Garofalo, *Data Retention a 6 Anni, OK dal Parlamento (Nonostante la Privacy)*, Key4Biz (Nov. 8, 2017), <https://perma.cc/KDC4-NPAW>.

<sup>17</sup> COVID-19 Monitoring of the Italian Situation (RNDDT – Series), European Data Portal, <https://perma.cc/A4Z3-MZUV>.

<sup>18</sup> Costica Dumbrava, European Parliamentary Research Service, *Tracking Mobile Devices to Fight Coronavirus 6* (EPRS Briefing, Apr. 2020), <https://perma.cc/87WG-82CL>.

<sup>19</sup> Elvira Pollina & Douglas Busvine, *European Mobile Operators Share Data for Coronavirus Fight*, Reuters, <https://perma.cc/7UCG-P96K>.

<sup>20</sup> Id.

<sup>21</sup> Id.

The Lombardy region has used such data to determine observance of lockdown measures; movements exceeding 300 to 500 yards are reportedly down by around 60% from late February when the first case was discovered in the Codogno area.<sup>22</sup>

### III. Electronic Measures to Fight COVID-19 Spread

According to the Italian Health Ministry, a surveillance network on new COVID-19 cases, controls, and screening is currently active under the coordination of a national task force established to regulate the use of technology to fight the spread of COVID-19.<sup>23</sup> Since January 31, 2020, when a state of emergency was declared, a Special Commissioner for the emergency has been appointed and a technical-scientific committee has been established to deal with emergencies.<sup>24</sup> The national task force is soon to announce potential technological solutions to trace and isolate those who have tested positive for COVID-19.<sup>25</sup> Tech companies and research institutions have provided suggestions to the Italian government, including one proposal “that would analyze user data from Facebook to determine the mass movement of people.”<sup>26</sup> Facebook’s Data for Good unit “has been sharing aggregated data collected from location tracking software on mobile phones with researchers at the University of Pavia,” while an extant proposal would also review ways to use from Facebook’s GeoInsights portal.<sup>27</sup>

A broadly used and voluntary application adopted by the government of Lombardy requests users “to fill out a questionnaire with their symptoms to build a map indicating the risk of contagion.”<sup>28</sup> The app, called “AllertaLOM,” captures “a phone’s IMEI code, the unique serial number that all smartphones carry, and the user’s IP address.”<sup>29</sup> The app is available from the Apple, Google Play, and Huawei stores.<sup>30</sup> It enables all users, whether symptomatic or not, to fill in an integrated questionnaire enabling the collection of data, in an anonymous format, and to make it available to the regional crisis unit and other authorities monitoring the spread of the pandemic in the Lombardy region.<sup>31</sup> The app was developed by the digital company ARIA S.p.A. in collaboration with the San Matteo Hospital and the University of Pavia.<sup>32</sup> It allows the authorities to compile statistic and epidemiological information that can be used to calculate the

---

<sup>22</sup> Id.

<sup>23</sup> *Coronavirus: La Situazione Attuale*, Ministero della Salute, supra note 1, “Sorveglianza e Controlli.”

<sup>24</sup> Id.

<sup>25</sup> Cecilia Butini, *Italy Looks to Tech to Limit the Spread of the Coronavirus*, *Authoritarian Tech* (Apr. 10, 2020), <https://perma.cc/4VNR-GR8J>.

<sup>26</sup> Id.

<sup>27</sup> Id.

<sup>28</sup> Id.

<sup>29</sup> Id.

<sup>30</sup> *AllertaLOM: L’App dell’Emergenza Covid-19*, Regione Lombardia, <https://perma.cc/2QHH-G7JP>.

<sup>31</sup> Id.

<sup>32</sup> Id.

potential “level of risk contagion, thus reinforcing the protection of all citizens, whether or not symptomatic.”<sup>33</sup>

These and other proposals have triggered an ongoing discussion in Italy as to the level of privacy rights and data protection that these new technologies would afford to citizens.<sup>34</sup> Some argue that, based on the extent of the pandemic in Italy, “concerns about user privacy and data sharing should be temporarily put on hold.”<sup>35</sup> The national Constitution allows for measures aimed at protecting the health of a whole nation.<sup>36</sup>

In April, a company called Webtek released an app called “StopCovid19.” The app traces the movements of users using GPS by having users connect their phone numbers to the app, which in turn uploads their location into a database, so only health authorities may determine the contacts a person who has tested positive with COVID-19 has had in a determined period of time and venue.<sup>37</sup> In particular, the app “would record when the user came into proximity with another smartphone user with the app, for how long and at what distance and if a person tested positive for the coronavirus, authorities would be able to trace the contacts and alert them.”<sup>38</sup> The system would make “it possible to warn someone who comes into close contact with someone who then tests positive for COVID-19, even if they then travel on to another EU country.”<sup>39</sup>

Some observers have raised important issues of privacy and data control.<sup>40</sup> In this context, on April 30, 2020, the Italian government issued Decree-Law No. 28, which creates the COVID-19 Alert System, which is designed to alert people who have had close contact with those who have tested positive for COVID-19 in order to protect their health through preventive measures.<sup>41</sup> The Alert System is based on an application to be installed voluntarily by citizens on their mobile telephones.<sup>42</sup> All data is compiled by several layers of government authorities coordinated by the Ministry of Health, which must ultimately adopt all the measures necessary to guarantee an adequate level of security, considering the risks involved and the rights and freedoms of the

---

<sup>33</sup> Id.

<sup>34</sup> Id.

<sup>35</sup> Id.

<sup>36</sup> Chiara De Cuia, *How Is Italy Handling the Coronavirus*, Lawfare (Mar. 6, 2020) (referring to article 16 of the Constitution, which “provides for its [freedom of movement] restriction for public health and security reasons”), <https://perma.cc/YG9F-YGXH>.

<sup>37</sup> *Coronavirus Is Spreading Fast and Quietly*, Webtek, <https://perma.cc/MPQ6-BYAE>.

<sup>38</sup> Id.

<sup>39</sup> Id.

<sup>40</sup> Elvira Pollina & Kirsten Donovan, *Italy Working on Coronavirus Tracing App to Help Lockdown Exit*, Reuters (Apr. 8, 2020), <https://perma.cc/EX6K-7MS9>.

<sup>41</sup> Decreto-Legge 30 Aprile 2020, n. 28 Misure Urgenti per la Funzionalità dei Sistemi di Intercettazioni di Conversazioni e Comunicazioni, Ulteriori Misure Urgenti in materia di Ordinamento Penitenziario, nonché Disposizioni Integrative e di Coordinamento in materia di Giustizia Civile, Amministrativa e Contabile e Misure Urgenti per l’Introduzione del Sistema di Allerta Covid-19 (D.L. No. 28), art. 6(1), G.U. Apr. 30, 2020, no. 111, <https://perma.cc/6B6V-NB86>.

<sup>42</sup> Id.

concerned parties.<sup>43</sup> Decree-Law No. 28 also makes explicit reference to all the guarantees and safeguards established for the use and protection of personal data by the EU GDPR.<sup>44</sup> The use of the app and of each piece of personal data acquired through it will cease when the state of emergency declared by the Council of Ministers on January 31, 2020, is lifted, and in any case the app cannot be used beyond December 31, 2020, when all personal data must be cancelled or classified as definitively anonymous.<sup>45</sup> The app, “which uses Bluetooth, won’t geo-localize users, and data will only be mined for purposes of containing the virus or for epidemiological study.”<sup>46</sup>

According to Decree-Law No. 28 the process to alert persons potentially contacted by infected individuals is based on the processing of proximity data of the devices, on an anonymous basis or, when not possible, pseudonymized, but at any rate the geolocation of individual users is forbidden.<sup>47</sup> The data collected through the app may only be processed for the purposes stated in Decree-Law No. 28, which includes the possibility of aggregation in an anonymous form, exclusively for public health, prevention, statistical or scientific research purposes.<sup>48</sup>

Italy has also signed a deal with telecoms operators to collect anonymized location data.<sup>49</sup>

The Italian government has stated that ultimately any movement-tracing technological solutions would have to comply with EU regulations and be sanctioned through legislation in the country,<sup>50</sup> and has reiterated that all data gathered during the pandemic will be discarded afterwards.<sup>51</sup>

The Italian Civil Aviation Authority (Ente Nazionale per l’Aviazione Civile, ENAC) has approved the use of drones by local police to monitor social distancing.<sup>52</sup> Drones can be used in urban areas or “where there are small populations exposed to the risk of impact.”<sup>53</sup>

---

<sup>43</sup> Id. art. 6(2).

<sup>44</sup> Id. art. 6(2)(a), (b) & (f), (3).

<sup>45</sup> Id. art. 6(6).

<sup>46</sup> *Italy Says App Tracing Contacts of People Infected with COVID-19 Will Be Anonymous*, Time (Apr. 29, 2020), <https://perma.cc/9VY9-FFEZ>.

<sup>47</sup> D.L. No. 28, art. 6(2)(c).

<sup>48</sup> Id. art. 6(3).

<sup>49</sup> Isobel Asher Hamilton, *Compulsory Selfies and Contact Tracing*, Business Insider (Apr. 14, 2020), <https://perma.cc/7GX7-ZCEE>.

<sup>50</sup> Id.

<sup>51</sup> Id.

<sup>52</sup> Matthew Holroyd, *Coronavirus: Italy Approves Use of Drones to Monitor Social Distancing*, Euronews (Mar. 23, 2020), <https://perma.cc/8EXJ-GHC3>.

<sup>53</sup> Id.

# Norway

*Elin Hoføerberg*  
*Foreign Law Specialist*

**SUMMARY** Norway protects the right to privacy in its Constitution and, following a European Economic Area (EEA) Joint Committee Decision in 2018, is bound by the European Union General Data Protection Regulation. Personal data may typically be stored for purposes of a public need and may specifically be used and shared to prevent the spread of contagious diseases.

Norway has launched a physical location tracking app, Smittestopp, to locate and prevent the spread of COVID-19. The app, which is available for download to Android, Google, and Huawei smartphones, uses both Bluetooth technology and GPS to track users who are in close proximity, defined as within two meters (about six feet) of each other for at least fifteen minutes. Downloading the app is voluntary, and once downloaded the app requires consent in order for the Norwegian Institute of Public Health to track the location of the person. The information is deleted after thirty days.

The Norwegian Data Protection Authority, Datatilsynet, is currently investigating whether the app complies with Norwegian and international data protection rules. An expert committee has recommended that changes be made to the app to enable further anonymization and prevent individual identification.

## I. Introduction

### A. COVID-19 Infections

Norway has a low rate of infection and deaths related to COVID-19 and a high rate of testing.<sup>1</sup> As of May 22, 2020, it had 8,309 confirmed cases and 235 fatalities from COVID-19,<sup>2</sup> the equivalent of 43 deaths per million residents.<sup>3</sup> Norway reported its first confirmed case of COVID-19 on February 24, 2020.<sup>4</sup> On March 12, 2020, it reported its first fatality.<sup>5</sup> On May 22, 2020, it reported no new deaths from COVID-19.<sup>6</sup> During the prior week a total of 15 persons were reported to have died from COVID-19.<sup>7</sup>

---

<sup>1</sup> On May 22, 2020, Norway ranked below the world average for both deaths per million and number of total infections. *Coronavirus*, Worldometers (last updated May 22, 2020), <https://perma.cc/93LJ-8FNK>.

<sup>2</sup> Press Release, FHI, Dagsrapport og statistikk om koronavirus og COVID-19 (May 22, 2020), <https://perma.cc/ZU6X-LUCY>.

<sup>3</sup> *Coronavirus*, Worldometers, supra note 1.

<sup>4</sup> *Status koronaviruset*, NRK, <https://perma.cc/C69M-55T9>.

<sup>5</sup> Halvor Bjørntvedt et al., *Første coronadødsfall i Norge*, VG (Mar. 13, 2020), <https://perma.cc/235F-ZPHN>.

<sup>6</sup> *Coronavirus*, Worldometers, supra note 1.

<sup>7</sup> FHI, *COVID-19 Ukerapport – uke 20* (May 19, 2020), <https://perma.cc/5EVJ-2F5M>.

## B. Smartphone Use

The use of smartphones is widespread in Norway. In 2019, Statistics Norway (Statistisk Sentralbyrå, SSB) reported that close to 100% of Norwegians age 9 to 79 have a cellular phone, and 95% have a smartphone,<sup>8</sup> not counting any smartphone access persons may have via their work.<sup>9</sup> Most users use either Telenor or Telia; Telenor has the largest market share of account subscribers with almost half of the market (48.9%), with Telia at 37.2%.<sup>10</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The Norwegian Constitution guarantees the right to privacy in article 102, which states that “[e]veryone has a right to respect for his or her personal life and family life, as well as his or her home and communication. House searches may not be conducted, except during criminal investigations. State authorities shall ensure the protection of personal integrity.”<sup>11</sup> In addition, Norway is a signatory to the European Convention on Human Rights, which guarantees the right to privacy in article 8.<sup>12</sup>

Norway regulates privacy rights and data protection in its Personal Information Act.<sup>13</sup> Though not a European Union (EU) Member State, it is bound by the EU legislation on personal data, namely the General Data Protection Regulation (GDPR),<sup>14</sup> because of its obligations as a member of the European Economic Area (EEA) and European Free Trade Agreement (EFTA). In 2018 the EEA Joint Committee signed on to the GDPR legislation in order to ensure harmonized rules on

---

<sup>8</sup> *Fakta om Internet tog mobil, Andel som har tilgang til ulike elektroniske tilbud, personer 9-79 år*, SSB, <https://perma.cc/A8GD-7VL6>; Statistisk sentralbyrå, *Norsk mediebarometer 2019* at 5 (May 19, 2020), <https://perma.cc/XQL3-7NYL>; see also *Number of Mobile Phone Users in Norway from 2011 to 2019*, Statista, <https://perma.cc/8K84-DZLJ>; *Forecast of Smartphone User Numbers in Norway from 2018 to 2024*, Statista, <https://perma.cc/L4E6-LUGH>.

<sup>9</sup> *Fakta om Internet tog mobil*, supra note 8.

<sup>10</sup> Marius Lorentzen, *Ferske mobiltall: Ice vokser – Telenor og Telia faller*, E24 (May 13, 2019), <https://perma.cc/97QE-9YUG>.

<sup>11</sup> § 102 Grunnloven [Norwegian Constitution] (LOV-1814-05-17), <https://perma.cc/M2JC-N95A> (translation by author).

<sup>12</sup> Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, <https://perma.cc/XP8C-Z7HJ>; see also NIM, «Smittestopp» og retten til privatliv (May 4, 2020), <https://perma.cc/2DWB-USXN>.

<sup>13</sup> Lov om behandling av personopplysninger (Personopplysningsloven) (LOV-2018-06-15-38) (hereinafter Personal Information Act), <https://perma.cc/BK6V-66KK> (in English translations, also known as the “Protection of Data Act”).

<sup>14</sup> General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, <https://perma.cc/7T85-89ZQ>.

data protection within the EEA.<sup>15</sup> The Personal Information Act incorporates the EU GDPR.<sup>16</sup> Thus, the same rules for the collection of data apply in Norway as in the EU Member States.<sup>17</sup>

In accordance with the GDPR as implemented in the Personal Information Act, “personal data” is defined as

any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.<sup>18</sup>

Data may only be collected in the following situations:

- a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- c. processing is necessary for compliance with a legal obligation to which the controller is subject;
- d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.<sup>19</sup>

---

<sup>15</sup> EEA Joint Committee Decision 154/20182018 O.J. (L 183, 23), <https://perma.cc/W5ZR-BZ5P>.

<sup>16</sup> Prop. 56 LS (2017–2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke tildeltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen, <https://perma.cc/CE8N-UN6R>; *Ny personopplysningslov*, Regjeringen (Oct. 30, 2019), <https://perma.cc/W9Y7-S4VL>. For an overview of Norway’s implementation of GDPR see Detlev Gabel & Tim Hickman, *GDPR Guide to National Implementation: Norway*, White & Case (Norway 13, 2019), <https://perma.cc/AS6S-3EYE>. For more on the implementation process in EEA countries generally see Line Coll & Rolf Riisnæs, *Implementing the GDPR in Norway*, Wikborg Rein (June 29, 2018), <https://perma.cc/6EFX-H45W>.

<sup>17</sup> For additional information on the EU see the EU survey in this report.

<sup>18</sup> GDPR art. 4(1).

<sup>19</sup> Id. art. 6(1).

Thus, the general basis for the collection of information is informed, adequate, and voluntary consent.<sup>20</sup> Specifically, consent is defined in article 4 of the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”<sup>21</sup> Moreover, as specified in article 7, such consent must “be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.”<sup>22</sup> A person’s consent remains revocable at all times.<sup>23</sup> In addition, a person must be at least 13 years old to provide consent under Norwegian law.<sup>24</sup> As implemented in Norwegian law, consent can also be given for the collection and processing of all sensitive data, as Norway has not provided additional provisions to further limit the sharing of sensitive information.<sup>25</sup> Thus, there is no data that cannot be shared provided that prior adequate and voluntary consent has been given during the collection phase.<sup>26</sup>

Legally, information may be stored without the consent of the data subject, if needed for a public purpose.<sup>27</sup> However, in such cases the public interest in processing the data must clearly exceed the disadvantages to the person whom the data is about (the data subject) and must be approved by the Norwegian Data Protection Agency.<sup>28</sup> The storage and sharing of data typically requires anonymization and pseudonymization.<sup>29</sup> In accordance with the Personal Information Act the Personal Data Authority may allow the handling of personal data in individual cases, if in the public interest.<sup>30</sup> Similarly, the government may issue specific regulations pertaining to data retention.<sup>31</sup> The collection of personal data, allowing use also without consent, is regulated in a number of legal acts, including the Criminal Procedures Act and the Health Registry Act.<sup>32</sup> The lawfulness of measures that may be used to contain contagious diseases is regulated in the Control of Communicable Diseases Act.<sup>33</sup> The law allows for the collection and sharing of

---

<sup>20</sup> Id. arts. 4, 6(1), 7.

<sup>21</sup> GDPR art. 4(1).

<sup>22</sup> Id. art. 7(2).

<sup>23</sup> Id. art. 7(3).

<sup>24</sup> Personal Information Act § 5.

<sup>25</sup> GDPR arts. 9(2)(a), 54; Personal Information Act, e contrario.

<sup>26</sup> GDPR arts. 6(1)(a), 7.

<sup>27</sup> GDPR art. 89(1); Personal Information Act § 9.

<sup>28</sup> Personal Information Act § 9.

<sup>29</sup> GDPR art. 25(1).

<sup>30</sup> Personal Information Act § 7.

<sup>31</sup> Id.

<sup>32</sup> See, e.g., § 216(b) Straffeprosessloven [Criminal Procedures Act] (LOV-1981-05-22-25), <https://perma.cc/RL46-GHG8>; § 11 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)[Health Registry Act] (LOV-2014-06-20-43), <https://perma.cc/DD4Q-F8XX>.

<sup>33</sup> Lov om vern mot smittsomme sykdommer [smittevernloven] (LOV-1994-08-05-55), <https://perma.cc/W4LS-D4YR>.

personal data in order to prevent disease.<sup>34</sup> The permissibility of using personal data to trace contagious disease is specifically mentioned in the GDPR, and was also mentioned in the bill implementing the GDPR into Norwegian law.<sup>35</sup> The GDPR allows for the use and sharing of personal information when needed for disease tracing.<sup>36</sup>

## **B. Data Retention and Location Tracking**

The telecommunications sector is regulated by the Electronic Communication Act.<sup>37</sup> However, location tracking is primarily regulated through the Personal Information Act as, per the GDPR, the definition of personal data includes location data.<sup>38</sup> As mentioned above, the Personal Information Act authorizes the Personal Data Authority to handle and retain personal data in individual cases, if in the public interest.<sup>39</sup> Similarly, the government may issue specific regulations pertaining to data retention.<sup>40</sup> Telecommunication service providers may store data, including location data, but only for as long as needed; they must delete or anonymize the data when no longer needed.<sup>41</sup>

## **C. Enforcement**

Datatilsynet, the Norwegian Data Protection Authority, is the supervisory authority for the collection and use of personal data in Norway.<sup>42</sup> Violations are subject to monetary fines, including compulsory fulfillment fines that run until the violation has been corrected.<sup>43</sup> Violations are also subject to damages for nonmonetary losses caused by the breach of the data protection rules.<sup>44</sup>

## **D. COVID-19 Tracing Legislation**

On March 27, 2020, the Norwegian Ministry of Health and Care Services issued a regulation on tracing and epidemic contagion related to COVID-19.<sup>45</sup> The regulation was adopted with the

---

<sup>34</sup> Id. §§ 3-6.

<sup>35</sup> Prop. 56 LS (2017–2018) at 264.

<sup>36</sup> GDPR recital 112.

<sup>37</sup> Lov om elektronisk kommunikasjon (Ekomloven) (LOV-2003-07-04-83), <https://perma.cc/8ZCY-MCZU>.

<sup>38</sup> GDPR art. 4(1).

<sup>39</sup> Personal Information Act § 7.

<sup>40</sup> Id.

<sup>41</sup> Ekomloven § 2-7.

<sup>42</sup> Personal Information Act § 20.

<sup>43</sup> Id. §§ 26, 29.

<sup>44</sup> Id. § 30.

<sup>45</sup> Forskrift om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19 (FOR 2020-03-27-475), <https://perma.cc/UKS8-5Y5W>.

purpose of making it easier to track COVID-19 cases and prevent community spread<sup>46</sup> based on authorization provided by temporary emergency legislation pertaining to COVID-19, known as the Corona Act.<sup>47</sup> The regulation gives the FHI power to establish an electronic system for tracking COVID-19 infections.<sup>48</sup> Participation in the system must be voluntary and must include “comprehensive, understandable, and easily accessible information, including on the processing of personal data.”<sup>49</sup>

### III. Electronic Measures to Fight COVID-19 Spread

#### A. Smittestopp Voluntary COVID-19 Tracing App

On April 16, 2020, Norway introduced a mobile app, called Smittestopp (which means infection stop), to trace persons infected with COVID-19.<sup>50</sup> Interest in the app was initially high, but usage has since waned. On April 17, 2020, close to a million users were reported as having downloaded the app.<sup>51</sup> As of April 30, 2020, the Norwegian Public Health Agency (Folkehelseinstituttet, FHI) reported that about 900,000 Norwegians were actively using the app (about 20.5% of the population age 16 and above).<sup>52</sup> On May 7, the FHI reported that they needed more users to use the app for it to work properly.<sup>53</sup> As of May 19, 2020, the FHI reported that 641,824 users actively used the app.<sup>54</sup> Most of the users are located in the Norwegian capital, Oslo, with about 100,000 users.<sup>55</sup> Oslo has a population of about 680,000. As of May 20, 2020, no municipality had more than 20% of active Smittestopp app users.<sup>56</sup>

Smittestopp<sup>57</sup> traces the movements of users with the explicit purpose of determining whether a user has been in close contact with another user who later developed COVID-19.<sup>58</sup> “Close contact”

---

<sup>46</sup> Id. § 1.

<sup>47</sup> Midlertidig lov om forskriftshjemmel for å avhjelpe konsekvenser av utbrudd av Covid-19 mv. (koronaloven) (LOV- 2020-03-27-17), <https://perma.cc/WKH3-YX9G> (to be repealed on May 27, 2020).

<sup>48</sup> FOR 2020-03-27-475 § 2.

<sup>49</sup> Id.

<sup>50</sup> See Elin Hofverberg, *Norway: Government Launches Mobile App to Track and Stem Spread of COVID-19*, Global Legal Monitor (Law Library of Congress, May 6, 2020), <https://perma.cc/FE5G-KKEQ>.

<sup>51</sup> Louise Krüger et al., *Nesten en million har lastet ned smitteapp*, NRK (Apr. 17, 2020), <https://perma.cc/FX97-NEWP>.

<sup>52</sup> *1 av 5 deler data fra Smittestopp-appen med Folkehelseinstituttet*, FHI (Apr. 30, 2020), <https://perma.cc/G5YU-PYUS>.

<sup>53</sup> *Vi treng fleire Smittestopp-brukarar*, FHI (May 7, 2020), <https://perma.cc/SB28-58EN>.

<sup>54</sup> *Antall nedlastinger og antall brukere av Smittestopp*, FHI (May 20, 2020), <https://perma.cc/RD9J-Z4L8>.

<sup>55</sup> Id.

<sup>56</sup> Id.

<sup>57</sup> FHI, *Informational Brochure on Smittestopp App*, <https://perma.cc/XA7F-SWMM> (in Norwegian) <https://perma.cc/2A3W-GUMD> (in English).

<sup>58</sup> See generally *Together We Can Fight Coronavirus – Download the Smittestopp App*, Helse Norge, <https://perma.cc/FGR3-6BMB>.

is defined as within two meters (about six feet) for a minimum of fifteen minutes.<sup>59</sup> Initial reporting suggests that it is possible that locations on separate sides of a wall may erroneously be recorded as within close contact, because they are registered as within two meters.<sup>60</sup>

The app records the movements of users, provided that the user actively chooses to share its location data with FHI.<sup>61</sup> The data obtained and stored is reportedly pseudonymized but the location of a user may nevertheless be identifiable, which is why, according to the developer, no analysts may look directly at the data.<sup>62</sup> According to Helse Norge, the Norwegian Health Network that services all e-health resources for Norwegians, the data is stored on the smartphone and uploaded to the app once every hour, provided that there is an internet connection.<sup>63</sup> The app also has a number of privacy protection features.<sup>64</sup> For example, stored data is automatically deleted after 30 days.<sup>65</sup> Smittestopp has a 16-year-old age requirement for use.<sup>66</sup>

Persons who have been in close proximity to another user who develops the disease will get a text message instructing them to take additional measures to determine if they have contracted COVID-19.<sup>67</sup> However, users who are notified are not required to self-isolate.

## **B. Supervisory Authority Investigation of the App**

On April 27, 2020, Datatilsynet announced that it was about to launch an investigation into the use of the Smittestopp app because the central registration and collection of users' location data may be an infringement of privacy.<sup>68</sup> Datatilsynet, is the supervisory authority for the collection and use of personal data in Norway.<sup>69</sup> It explained that the purpose of the investigation is to ensure that the app complies with the Norwegian regulation on tracing and epidemic contagion related to COVID-19.<sup>70</sup> As noted above, the regulation requires that the system be voluntary and include "comprehensive, understandable and easily accessible information, including on the processing of personal data."<sup>71</sup>

---

<sup>59</sup> *Sammen kan vi knekke korona – last ned Smittestopp*, Helse Norge, <https://perma.cc/Z4XG-AL3Y>.

<sup>60</sup> Id.

<sup>61</sup> Id.

<sup>62</sup> Helse Norge, Informational Brochure on Smittestop App, <https://perma.cc/8JQE-KBBB>.

<sup>63</sup> Id.

<sup>64</sup> *Bruk av Smittestopp og personvern*, FHI (Mar. 31, 2020), <https://perma.cc/ESY4-6WJ8>.

<sup>65</sup> HelseNorge, *supra* note 59

<sup>66</sup> Id; FHI, *supra* note 64.

<sup>67</sup> Helse Norge, *supra* note 592.

<sup>68</sup> Press Release, Datatilsynet, Starter kontroll av FHIs Smittestopp-app (Apr. 27, 2020), <https://perma.cc/87XW-SYDH>.

<sup>69</sup> Personal Information Act § 20.

<sup>70</sup> Id.

<sup>71</sup> § 2 FOR 2020-03-27-475.

On May 12, 2020, Datatilsynet initiated the investigation.<sup>72</sup> On May 20, 2020, it asked the FHI to provide additional information no later than June 1, 2020,<sup>73</sup> on how the FHI has balanced the need for the app (presumably the public need for contact tracing during a pandemic) with the protection of users' personal data.<sup>74</sup> Datatilsynet noted in its press release that, "[i]f you do not have an overview of which personal data is used for what purpose, one cannot determine if it necessary to use that personal data to achieve each of these goals."<sup>75</sup>

Following the announcement of the investigation, an expert group suggested improvements to the Smittestopp app, particularly the use of non-static Bluetooth IDs.<sup>76</sup> The expert group also suggested using privacy differentiation for analytical purposes.<sup>77</sup>

### C. Privacy & and Other Critiques of the App

In addition to the supervisory authority investigation mentioned above, concerns have also been raised internationally that the current design of the app is problematic in relation to the international framework for collecting personal data, even though using the app is voluntary. Specifically, the European Data Protection Board, which oversees compliance with the GDPR and the Data Protection Law Enforcement Directive, has voiced concerns that apps that collect and store information in the way the Norwegian app does violate those privacy protections.<sup>78</sup>

Another critique of the app is that it was launched too soon, before municipalities were ready to use it.<sup>79</sup> As of May 10, 2020, only three municipalities had the technology available to send notification texts to their residents, Drammen, Tromsø, and Trondheim.<sup>80</sup> Reportedly, as of May 16, no case had been discovered with the help of the app, as notifications of potential exposure was limited to users in these areas.<sup>81</sup>

---

<sup>72</sup> Datatilsynet, *supra* note 68; *Varsel om pålegg til Smittestopp*, Datatilsynet (May 12, 2020), [perma.cc/9W9T-2CUS](https://perma.cc/9W9T-2CUS).

<sup>73</sup> *Etterspør mer informasjon om Smittestopp*, Datatilsynet (May 20, 2020), <https://perma.cc/NA8K-ZJHR>.

<sup>74</sup> *Id.*

<sup>75</sup> *Id.* (translation by author).

<sup>76</sup> *Ekspertgruppe foreslår forbedringer i Smittestopp-appen*, Regjeringen (May 20, 2020), <https://perma.cc/4FQA-SHSX>; Jeanine Lilleng et al., *Ekspertgruppen for kodegjennomgang av løsning for digital smittesporing, Endelig rapport for kildekodegjennomgang av løsning for digital smittesporing av koronaviruset* (May 18, 2020), <https://perma.cc/8DZU-5THM>; see also Caroline Simonsen, *Rapport: Sikkerhet og personvern ikke godt nok ivaretatt i Smittestopp-appen*, NKR (May 20, 2020), <https://perma.cc/2JKJ-K3N9>. *FHI har mottatt rapport fra ekspertgruppen om Smittestopp*, FHI (May 20, 2020), <https://perma.cc/4XK5-8AQZ>.

<sup>77</sup> *Id.*

<sup>78</sup> European Data Protection Board Letter to EC, Ref: OUT2020-0028 (Apr. 14, 2020), <https://perma.cc/F8XT-LEBS>.

<sup>79</sup> NTB, *FHI trosset ekspertgruppen da de lanserte Smittestopp-appen*, Aftenposten (May 10, 2020), <https://perma.cc/225G-QLSA>.

<sup>80</sup> *Id.*

<sup>81</sup> Line Fransson, *Har ikke oppdaget coronasmitte*, Dagbladet (May 16, 2020), <https://perma.cc/7UFC-NJNX>.

On the other hand, the app has also been criticized by IT experts for not collecting and sharing enough data—specifically the app’s establishment of a 15-minute contact requirement for information sharing—on the ground that contact for shorter intervals of time may also result in the spread of COVID-19, and that such information must be recorded in order to better develop the app.<sup>82</sup>

#### D. Use of Telecommunication Data for Determining Travel Restriction Compliance

Norway implemented travel restrictions, both to and from the country as well as domestically within Norway, during the month of March 2020.<sup>83</sup> The travel restrictions were coupled with monetary fines or prison of up to six months, including for persons breaching the domestic travel restrictions.<sup>84</sup> Telecommunications data was used to measure compliance with these restrictions.<sup>85</sup> Initial reports on how many Norwegians were present outside their home municipality were based on numerical data from the telecommunications systems,<sup>86</sup> reporting the number of mobile users in a given area compared to the number of permanent residents, but there were no reports of people being individually targeted by that approach.<sup>87</sup> Instead, as described by the telecommunications company Telenor, the data only provides information on how many mobile users are present in a given area (connected to a given cellular tower), not who or how close from each other they are.<sup>88</sup>

---

<sup>82</sup> Julie Kalveland, *IT-ekspert bekymret for at Smittestopp-appen vil finne for få smittede*, Dagens Medisin (Apr. 28, 2020), <https://perma.cc/PX93-BPMR>.

<sup>83</sup> Press Release, Ministry of Justice and Public Security & Ministry of Foreign Affairs, Stricter Border controls Being Introduced – Norwegian Airports Not Closing (Mar. 15, 2020), <https://perma.cc/KK6H-8E5C>. For example, only Norwegian citizens and residents were allowed to enter the country, and the government asked all travelers to spend two weeks in quarantine following any international travel. In addition, Norwegians were also not allowed to travel to vacation properties outside their home municipality between March 16, 2020, and April 20, 2020. Forskrift om karantene, isolasjon og forbud mot opphold på fritidseiendommer mv. i anledning utbrudd av Covid-19 (FOR-2020-03-15-294), <https://perma.cc/8NMX-GMUE>; see also Elin Hofverberg, *Norway: Government Prohibits Staying in Vacation Properties Outside of Home Municipality over Coronavirus Spread*, Global Legal Monitor (Law Library of Congress, Mar. 19, 2020), <https://perma.cc/QH5K-BRB9>; *Koronasituasjonen: Hytteforbudet*, Regjeringen (Apr. 14, 2020), <https://perma.cc/28MZ-C9TZ>.

<sup>84</sup> FOR-2020-03-15-294 § 6.

<sup>85</sup> See, e.g., Lone Lohne, *Hyttefolket forlater ikke fjellet: – Fryktelig skuffende*, VG (Mar. 14, 2020), <https://perma.cc/W2YM-KTBK>.

<sup>86</sup> Id.

<sup>87</sup> Id.

<sup>88</sup> *Nordmenns mobilbruk kan bidra til å forhindre spredningen av koronaviruset*, Telenor, <https://perma.cc/45D8-4JKL>.

# Portugal

*Eduardo Soares*  
*Senior Foreign Law Specialist*

**SUMMARY** The General Data Protection Regulation issued by the European Union in 2016 was implemented in Portugal's domestic legislation in 2019 and applies to the processing of personal data carried out in the national territory. A law enacted in 2004 determines that companies offering electronic communications networks and or services must guarantee the inviolability of communications. The preservation and transmission of traffic and location data relating to persons and legal entities, as well as related data necessary to identify the subscriber or registered user, for the purposes of investigation, detection, and prosecution of serious crimes by the competent authorities is regulated by a law enacted in 2008.

Notwithstanding several legal measures taken to fight the pandemic, Portugal has yet to adopt electronic means to help in the fight against the spread of COVID-19.

## I. Introduction

As of May 22, 2020, Portugal had registered 30,200 confirmed cases of COVID-19 and 1,289 related deaths.<sup>1</sup> According to the National Authority of Communications (Autoridade Nacional de Comunicações, ANACOM), in 2019 Portugal had 12.4 million active cell phones in the country.<sup>2</sup> However, Portugal has not yet developed a contact tracing app for the pandemic.

## II. Legal Framework

### A. Privacy and Data Protection

On April 26, 2016, the European Union issued the General Data Protection Regulation (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.<sup>3</sup> To implement the GDPR into its domestic legislation, Portugal enacted Law No. 58 of August 8, 2019, which regulates the processing of personal data carried out in the national territory, regardless of the public or private nature of the controller or the subcontractor, even if it is carried out in compliance with legal obligations or in pursuit of missions of public interest, applying all the exclusions provided for in article 2 of the GDPR.<sup>4</sup> Under the GDPR the processing of personal data must comply with the principles of lawfulness, fairness and

---

<sup>1</sup> *Ponto de Situação Atual em Portugal*, Direção Geral de Saúde, <https://covid19.min-saude.pt/ponto-de-situacao-atual-em-portugal/>.

<sup>2</sup> *Serviços móveis - 2019*, Autoridade Nacional de Comunicações, <https://perma.cc/HPB9-CBFR>. For comparison purposes, on May 5, 2020, the Portuguese population was estimated to be 10,259,625 persons. Pordata, Base de Dados Portugal Contemporâneo, <https://perma.cc/2SR3-P222>.

<sup>3</sup> General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, <https://perma.cc/4HPB-DXKW>.

<sup>4</sup> Lei No. 58/2019, de 8 de Agosto, arts. 1, 2(1), <https://perma.cc/4KXC-HX8J>.

transparency; limitation of purpose; data minimization; accuracy; storage limitation; and integrity and confidentiality.<sup>5</sup>

## **B. Data Retention and Location Tracking**

### *1. Law No. 41 of August 18, 2004*

Law No. 41 of August 18, 2004, transposed into domestic law the EU's 2002 ePrivacy Directive on the processing of personal data and the protection of privacy in the electronic communications sector.<sup>6</sup> Exceptions to the application of Law No. 41 that are strictly necessary for the protection of activities related to public security; defense; state security; and the prevention, investigation, and prosecution of criminal offenses are defined in special legislation.<sup>7</sup>

Companies offering electronic communications networks and/or services must guarantee the inviolability of communications and respective traffic data carried out through public communications networks and publicly available electronic communications services.<sup>8</sup>

The use of electronic communications networks for the storage of information or to obtain access to information stored in the terminal equipment of a subscriber or any user is only permitted when the following conditions are met:

- a) Clear and complete information must be provided to the subscriber or user concerned, namely on the purposes of processing, in accordance with the provisions of the Personal Data Protection Law;
- b) The subscriber or user has the right to refuse such processing.<sup>9</sup>

#### **a. Traffic Data**

Traffic data relating to subscribers and users that is processed and stored by companies offering electronic communications networks and or services must be deleted or made anonymous when they are no longer needed for the purpose of transmitting the communication.<sup>10</sup> Companies offering electronic communications services may process the data to the extent and for the time necessary for the commercialization of electronic communications services or the provision of value-added services, provided that the subscriber or user to whom the data refers has given prior consent, which can be withdrawn at any time.<sup>11</sup>

---

<sup>5</sup> GDPR art. 5. For an in-depth discussion of the GDPR and other EU instruments, see the European Union survey in this report.

<sup>6</sup> Lei No. 41/2004, de 18 de Agosto, art. 1(1), <https://perma.cc/3Y5A-G8LS>.

<sup>7</sup> Id. art. 1(4).

<sup>8</sup> Id. art. 4(1).

<sup>9</sup> Id. art. 5(1) (translation by author).

<sup>10</sup> Id. art. 6(1).

<sup>11</sup> Id. art. 6(4).

b. Location Data

The processing of location data that relates to subscribers or users of public communications networks or publicly available electronic communications services is permitted only if the data is anonymized.<sup>12</sup> Organizations with legal competence to receive emergency calls may register, process, and transmit location data for the purpose of responding to those calls.<sup>13</sup> The processing of location data is also permitted to the extent and for the time necessary for the provision of value-added services, provided that prior consent is obtained from subscribers or users.<sup>14</sup> Before obtaining such consent, companies offering electronic communications services to the public must inform users or subscribers about the type of location data that will be processed, the duration and purposes of the processing, and the eventual transmission of data to third parties for the purpose of providing value-added services.<sup>15</sup> These companies must also guarantee subscribers and users the possibility, through simple and free means, to withdraw their consent for the processing of location data, and to temporarily refuse to authorize such processing “for each connection to the network or for each transmission of a communication.”<sup>16</sup>

The processing of location data must be limited to the employees and contractors of companies that offer electronic communications networks and/or services accessible to the public or third parties that provide value-added services, and must be restricted to what is necessary for the purposes of providing such service.<sup>17</sup>

2. *Law No. 32 of July 17, 2008*

Law No. 32 of July 17, 2008, regulates the preservation and transmission of traffic and location data relating to persons and legal entities, as well as related data necessary to identify the subscriber or registered user, for the purposes of investigation, detection, and prosecution of serious crimes by the competent authorities. It transposes into national law the EU Data Retention Directive of 2006 on the conservation of data generated or processed in the context of the offer of communication services publicly available or public communications networks.<sup>18</sup>

The preservation of data that reveal the content of communications is prohibited without prejudice to the provisions of Law No. 41 of August 18, 2004, and criminal procedural legislation regarding the interception and recording of communications.<sup>19</sup>

---

<sup>12</sup> Id. art. 7(1).

<sup>13</sup> Id. art. 7(2).

<sup>14</sup> Id. art. 7(3).

<sup>15</sup> Id. art. 7(4).

<sup>16</sup> Id. art. 7(5).

<sup>17</sup> Id. art. 7(6).

<sup>18</sup> Lei No. 32/2008, de 17 de Julho, art. 1(1), <https://perma.cc/T34T-CUVF>. The EU Data Retention Directive was declared invalid by the Court of Justice of the European Union (CJEU) on April 8, 2014. See European Union survey in this report.

<sup>19</sup> Id. art. 1(2).

### III. Electronic Measures to Fight COVID-19 Spread

On March 13, 2020, the government enacted Decree-Law No. 10-A, which established exceptional and temporary measures associated with the epidemiological situation of COVID-19.<sup>20</sup> The Decree-Law applies to the prevention, containment, mitigation, and treatment of COVID-19.<sup>21</sup> Among other things, it suspended classes<sup>22</sup> and travel,<sup>23</sup> and limited access to spaces frequented by the public.<sup>24</sup>

Several other legal measures were taken by the government to fight the pandemic. However, it seems that so far none of them have addressed electronic means to stop the spread of the virus.<sup>25</sup> Nor has any entity developed a contact tracing app for Portugal.

---

<sup>20</sup> Decreto-Lei No. 10-A/2020, de 13 de Março, <https://perma.cc/8TAX-SCQM>.

<sup>21</sup> Id. art. 1(2).

<sup>22</sup> Id. art. 9.

<sup>23</sup> Id. art. 11.

<sup>24</sup> Id. arts. 12, 13.

<sup>25</sup> Legislação Compilada - COVID-19, Diário da República Eletrónico, <https://perma.cc/AP5T-BZS3>.

# Russian Federation

*Peter Roudik  
Director of Legal Research*

**SUMMARY** The Federal Government has adopted austerity measures to minimize the economic consequences of the COVID-19 pandemic. However, the right to apply specific measures aimed at enforcement of policies to combat the pandemic, including the employment of new technologies to monitor the community spread of COVID-19 and trace the contacts of infected people, has been given to the governors of the constituent components of the Russian Federation. Some regions have amended their provincial laws in order to ensure the legality of newly implemented policies. Most of the time, the use of technology has extended to tracing contacts, monitoring one's location, and fining people for disobeying the isolation orders. Several regions have required the registration of the total population in order to obtain electronic Quick Response codes that serve as digital passes allowing individuals to leave their primary residences. Legal observers have noticed that these measures are not in line with Russian privacy and data protection legislation. As a follow-up to the pandemic, the Government introduced new federal legislation aimed at defining the legal regime for the forced quarantining of the population and building a nationwide population database.

## I. Introduction

According to information from Johns Hopkins University, on May 22, 2020, Russia officially reported around 326,000 confirmed cases of Covid-19 and 3,250 deaths from the infection.<sup>1</sup> The infection was most widely spread in Moscow, St. Petersburg, and other major industrial cities in the center of the country. A full-scale nationwide quarantine was not introduced in Russia. In late March, Russian President Vladimir Putin announced the closure of nonessential businesses for one week and "asked the Russians to stay at home without outlining penalties for disregarding the request."<sup>2</sup>

The national legislature adopted austerity measures aimed at fighting COVID-19. The legislative package mainly addressed economic difficulties of the pandemic experienced by individuals and territories. These measures included amendments to the federal budget, new fines for violation of quarantine rules and distribution of fake news about COVID-19, and other specific actions, for example, deferral of loan payments, postponement of state inspections for cars, increased sick leave coverage, a simplified procedure for applying for child subsidies, allowing the online purchase and delivery of medicines, and new rules for airfare refunds.<sup>3</sup> However, the power to

---

<sup>1</sup> COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE), Johns Hopkins U. (May 22, 2020), <https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6>.

<sup>2</sup> Isabelle Khurshudyan, *Putin Postpones Russian Vote on Constitutional Amendments That Would Let Him Run for President Again*, Wash. Post (Mar. 25, 2020), <https://perma.cc/22TU-N5WJ>.

<sup>3</sup> Federal Law No. 98-FZ of Apr. 1, 2020, on Amending Legislative Acts Related to Preventing and Eliminating Emergency Situations, Pravo.gov.ru (official publication), <https://perma.cc/WK8J-LFB7> (in Russian).

make decisions concerning the implementation and enforcement of stay-at-home policies was delegated to the heads of the 85 regional administrations that constitute the Russian Federation.<sup>4</sup> Most of the time, smart phone applications aimed at tracing the contacts of infected persons and identifying their location were used to enforce the established measures, mainly because of the availability of smartphones. Reportedly, 95.3 million out of the 144 million people living in Russia have smartphones.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The right to privacy is incorporated in articles 23 and 24 of the Russian Constitution.<sup>6</sup> Article 137 of the Criminal Code, entitled “Invasion of Personal Privacy,” provides for a monetary fine of up to RUB200,000 (approximately US\$3,380) and up to two years of deprivation of liberty for the illegal collection or spreading of information about the private life of a person, without the person’s consent, where the information concerns personal or family secrets.<sup>7</sup>

Federal Law of the Russian Federation No. 152-FZ on Personal Data is the main legal act in the field of collecting, handling, and protecting information deemed personal.<sup>8</sup> Under this Law, “any information directly or indirectly related to a physical person or that allows a physical person to be identified” is recognized as personal data.<sup>9</sup> State and municipal authorities, legal entities, and individuals are required to obtain a person’s consent in order to process personal data.<sup>10</sup>

The Law does not include an exhaustive list of information that is considered personal. Some examples of what should be treated as personal information can be found in various implementing regulations. For example, Government Regulation No. 125 of March 4, 2010, on the List of Electronically Recorded Personal Data Included in Identification Documents, states that one’s passport or other ID number, personal name, date of birth, citizenship, gender, and digital photographic image constitute personal data.<sup>11</sup>

---

<sup>4</sup> Robyn Dixon, *In Russia, Facial Surveillance and Threat of Prison Being Used to Make Coronavirus Quarantines Stick*, Wash. Post (Mar. 25, 2020), <https://perma.cc/Y44A-4TGF>.

<sup>5</sup> *By 2020, the Number of Russians with Smartphones Will Reach 95.3 Million*, Gazeta.ru, Dec. 23, 2019, <https://perma.cc/WQ4U-LHP3> (in Russian).

<sup>6</sup> Konstitutsiia Rossiiskoi Federatsii [Constitution of the Russian Federation] Dec. 12, 1993 (in Russian), <https://perma.cc/A5C7-HSJW>.

<sup>7</sup> Ugolovnyi Kodeks Rossiiskoi Federatsii [Criminal Code of the Russian Federation] No. 63-FZ, June 13, 1996, *Sobranie Zakonodatel'stva Rossiiskoi Federatsii* [SZRF] June 17, 1996, No. 25, item 2954, <https://perma.cc/N8FX-NZJX> (in Russian), <https://perma.cc/43WT-78TJ> (unofficial English translation).

<sup>8</sup> *Sobranie Zakonodatel'stva Rossiiskoi Federatsii* [Collection of Russian Federation Legislation] (official gazette), 2006, No. 31(1), Item 3451, <https://perma.cc/SX8U-ZJCV> (in Russian).

<sup>9</sup> *Id.* art. 3(1).

<sup>10</sup> *Id.* arts. 6(1), 9.

<sup>11</sup> Government Regulation No. 125 of Mar. 4, 2010, on the List of Electronically Recorded Personal Data Included in Identification Documents, *Rossiiskaia Gazeta* (official publication), Mar. 10, 2010, No. 48, <https://perma.cc/4W52-GKTH> (in Russian).

It is not clear, however, if each separate component of this information is recognized as personal data or only in combination with other information if such a combination would allow an individual to be identified. Russian lawyers are generally of the opinion that a person's name (first, middle, and last), date and place of birth, address, family and social status, education, profession, income, and other information may constitute personal data if this information or its combinations would allow an individual to be identified.<sup>12</sup>

Regarding other forms of identification, it appears that there is agreement among Russian lawyers that a computer IP address cannot be considered personal data because it does not allow a person to be directly identified. A person's telephone number is viewed as personal data only if it is firmly associated with an individual through an agreement with a service provider. Similar principles apply to the recognition of an individual's email address as personal information.<sup>13</sup>

## **B. Data Retention and Location Tracking**

Every organization involved in processing personal data sets its own time frame and rules for handling personal data based on principles established by the Law and guidance issued by the Federal Service for Oversight in the Field of Communications and Information Technologies.<sup>14</sup> The retention term is no less than six months for the messages and transmitted files, and no less than three years for information about the fact of communication.<sup>15</sup>

The Law established a general prohibition on taking any actions involving personal data without the consent of the data subject, except for a few specific situations when such consent may not be required. These may occur when personal data actions are necessary for any of the following purposes:

- To perform obligations under an international treaty,
- To conduct judicial proceedings and ensure the enforcement of a judgment,
- To secure legal rights and interests of third persons,
- To perform the activities of government institutions, and
- To protect the life, health, and other interests of the data subject if the subject's consent cannot be obtained.<sup>16</sup>

---

<sup>12</sup> *What Is Included in Personal Data and Under Which Conditions*, 101 Million.com, <https://perma.cc/W5Z8-EB7X>.

<sup>13</sup> *Id.*

<sup>14</sup> Law on Personal Data, art. 5.

<sup>15</sup> Federal Law No. 374 of July 6, 2016, on Amendments to the Federal Law on Countering Terrorism and Other Legislative Acts, *Rossiiskaia Gazeta* (official publication), July 8, 2016, <https://perma.cc/SR95-SAUH> (in Russian).

<sup>16</sup> Law on Personal Data, arts. 7, 9.

Tracking and identification of one's geographic location by using electronic devices is not regulated by Russian legislation. This information is not included in article 10 of the Personal Data Law, which defines what information can be recognized as personal. A 2014 government regulation ordered provincial and municipal emergency services to develop tools that would allow the identification of the location of a person who calls for assistance in an emergency such as a fire or roadway traffic accident.<sup>17</sup> In 2019, Russian legislators decided that geolocation information is information about services provided to customers by telecom operators. The new law protects the right of law enforcement to receive this information from mobile communications providers when a search for a missing child is conducted. Law enforcement authorities are required to receive judicial approval within 48 hours for the usage of geolocation information.<sup>18</sup> Later, the legislature discussed a proposal to expand the right of police to use geolocation information in all search and rescue operations and allow the mobile phone users to transfer this information to third persons, however, this bill did not advance beyond the first reading.<sup>19</sup> In 2016, a court found that when a telecom company shares with third persons information about its customers, including their geolocation information, it commits a violation of the licensing agreement.<sup>20</sup>

### III. Electronic Measures to Fight COVID-19 Spread

The Russian health care system is based on a strong governmental role in ensuring the country's sanitary and epidemiologic well-being. Combating epidemics and responding to emergencies are included in the joint jurisdiction of federal and provincial authorities.<sup>21</sup> Government policy in the area of protection against medical emergencies is formulated in a number of federal and provincial legislative acts, presidential decrees, government regulations, and government programs. There is no special legislation aimed at the regulation of issues related to public health emergencies and epidemics. The outbreak of epidemics is considered an emergency situation, and depending on the outbreak's severity, rules under a state of emergency may be declared.<sup>22</sup>

While the federal legislation was amended with provisions introducing criminal responsibility for violation of quarantine rules and stricter punishments for distribution of fake news about the pandemic, most of the measures for countering the pandemic were introduced by regional authorities. On March 23, 2020, the Prime Minister of Russia ordered the federal Ministry of Communications to develop, within the next three days, a guidance for regional authorities on how to build contact tracing systems based on transferring customers' geolocation information

---

<sup>17</sup> Government of the Russian Federation, Regulation No. 2446 of Dec. 3, 2014, on Approving the Complex Development Program "Safe City," Pravo.gov.ru (official publication), <https://perma.cc/D73Q-7SBK> (in Russian).

<sup>18</sup> Federal Law No. 311 of Aug. 2, 2019, on Amending Article 8 of the Federal Law on Operational and Investigative Activities, Consultant+ database, <https://perma.cc/Q92R-5SUJ>.

<sup>19</sup> *The State Duma Adopted the Bill on Using Geolocation In Search for Missing Persons*, Tass.ru, Sept. 25, 2019, <https://perma.cc/EVP2-YAWU>.

<sup>20</sup> Ruling of the Arbitration Appeals Court for the 9th Circuit No. 09AP-17574 of May 23, 2016, <https://perma.cc/25R4-JRM9>.

<sup>21</sup> Constitution of the Russian Federation art. 72.

<sup>22</sup> Federal Constitutional Law No. 3-FKZ of May 30, 2001, Legislationline.org, <https://perma.cc/2MY4-KDTK>.

by mobile phone operators to regional authorities in charge of fighting COVID-19. Transportation employees became subject to additional control and extended contact tracing.<sup>23</sup>

The introduction of digital passes that would allow individuals to go outside of their residences and the consequent surveillance of people's movements has turned out to be the most controversial point of the quarantine measures implemented. Most of the Russian regions required the self-isolated population to use tracking technology and install a system of downloadable matrix barcodes called Quick Response (QR) codes, which serve as digital passes. These QR codes are required to use public transportation. They are linked to prepaid transportation tickets, while individual public transit tickets usually available for purchase by cash at any point of sale were canceled.

As described in a Washington Post article, "as soon as the digital code is created on a cellphone, the clock is ticking. It allows three hours to shop at the nearest grocery store or pharmacy or to visit a doctor. One hour is allotted to walk the dog. Taking out the trash should take no more than 30 minutes. Street surveillance cameras are watching for anyone trying to skirt the rules."<sup>24</sup>

A concern has been reported that these efforts will require "building up an entirely new huge database and then getting all people living in Moscow to provide their personal data to that database."<sup>25</sup>

A separate app called Social Monitoring and built with the purpose of tracking patients who have tested positive for COVID-19 but were allowed to undergo treatment at home, as well as people who have been in contact with them, has been implemented in Moscow since April 3, 2020. A request to install the app is sent as a text message to all people identified as those who were in contact with an infected individual. The Deputy Mayor of Moscow has said this may include relatives, coworkers, passengers on a flight used by the infected person, cab drivers, couriers, etc.<sup>26</sup> Reportedly, the Moscow City Government has an agreement with all Russian airlines operating international flights, and they share information with the authorities about all individuals arriving from abroad, including their phone numbers and addresses. Similar agreements exist with mobile services providers who report to the government instances when a customer uses a SIM card purchased abroad.<sup>27</sup> The app is based on using the Global Positioning System (GPS) function for geolocation or the user's network connections in order to determine his or her location if the GPS function is not available.<sup>28</sup> The app monitors the location of the

---

<sup>23</sup> *The Russian Federation Will Begin to Track by Phone Everyone Who Had Contact with Coronavirus Patients*, Interfax, Mar. 23, 2020, <https://perma.cc/LE5H-KND6>.

<sup>24</sup> Isabelle Khurshudyan, *Coronavirus Is Testing the Limits of Russia's Surveillance State*, Wash. Post, Apr. 5, 2020, <https://perma.cc/7VYE-9NWQ>.

<sup>25</sup> *Id.*

<sup>26</sup> *About One Thousand Contacts with COVID-19 Cases Were Identified in Moscow*, M24.ru, Mar. 11, 2020, <https://perma.cc/QE8J-RS54>.

<sup>27</sup> Daria Kozlova, *Big Med Brother: How Big Data Is Used to Fight COVID-19 and Whether Total Surveillance Is Justified in the Face of a Pandemic*, Nezavisimaia gazeta, Mar. 20, 2020, <https://perma.cc/Q9R4-AXY9> (in Russian).

<sup>28</sup> Khurshudyan, *supra* note 24.

person automatically and periodically requests the smart phone holder to submit a selfie taken inside his or her home. If a person has not registered within 24 hours after being required to do so, has not responded to the request for identification within one hour, or has moved away from the location designated for the person's isolation, the app reports the violation to the city authorities. If people refuse to install the app on their phones, they receive text messages with reminders during the first three days after an installation request is made, and then fines are issued. Individuals who have no smartphones receive special devices with a preinstalled Social Monitoring app.<sup>29</sup>

Confirming popular concerns about weak protection of data collected by government agencies, it was reported that the names and passport numbers of people fined for violation of the isolation rules can be found on the website for making fine payments by using ticket numbers. The city government stated that disclosure of this information does not constitute a violation of data protection rules. While lawyers disagree with this government position, they believe that individuals have no chance for remediation and compensation.<sup>30</sup> Formally, government institutions can receive personal information from private companies under the court order only. Law enforcement may be allowed to have access to this information during investigative operations based on a special request. It appears that such information is shared most of the time regardless of the legal arrangements. Authorities also have information to all the personal data of individuals who have been registered on the web portal for state services because such a registration requires the customer's consent for transfer of information to the third persons. Russian experts say that even when information includes nonpersonal data, there are possibilities for full identification of a person.<sup>31</sup>

Similar apps and monitoring systems were developed and established in other regions. All the regionally introduced systems are not connected with each other, and regional governments were free to select local solutions. For example, in the largest East Siberian region, employers and self-employed individuals are supposed to send requests for passes by email to the regional digital development agency and then receive codes through text messages after verification of the requester's identification through the database of residents registered at the regional web portal for state services. Reasons for pass requests are, for example, visiting relatives, traveling to summer homes in the country, meeting with an attorney or a notary, and accompanying minors, among other things. Each pass is valid for two 60-minute trips.<sup>32</sup> In another region, the local administration partnered with a regional bank in which the regional government is a major stakeholder and asked all residents applying for the digital passes to consent to the processing of their personal information by the bank.<sup>33</sup>

---

<sup>29</sup> Bela Liauw & Valery Kodachigov, *Social Monitoring Users Were Fined More Than 200 Million Rubles*, *Vedomosti*, May 20, 2020, <https://perma.cc/5S55-KKXN>.

<sup>30</sup> *Open Access to Passport Data of Muscovites Fined for Violation of Isolation Rules*, *Newsru.com*, May 18, 2020, <https://perma.cc/2VTZ-TCAF> (in Russian).

<sup>31</sup> Kozlova, *supra* note 27.

<sup>32</sup> Anna Vilisova & Ilya Shevelev, *Digital Pass Systems Are Being Introduced Throughout Russia. We Checked Some of Them with Security Experts – and This Is What Happened*, *Meduza.io*, Apr. 27, 2020, <https://perma.cc/TK5B-HW9N>.

<sup>33</sup> *Id.*

Cybersecurity experts expect leaks of personal data and violation of data protection requirements because these regional systems were built in a rush and were not certified by federal cybersecurity authorities. They are concerned that mobile applications require access to sound, video, pictures, and records of movements stored in the phones.<sup>34</sup>

The implementation of these measures met with two major problems: the difficulties of actual enforcement and technical glitches in computer systems. It was reported that 60,000 people in the city of Moscow installed the Social Monitoring app on their smartphones. About 54,000 fines were issued to about one-third of those who were under surveillance. Some people were fined several times. People complain that they are fined for not sending a selfie on time or when the GPS erroneously shows that a person has left his or her residence. About 400 people were fined for not responding to self-identification requests received at nighttime. Later, the nighttime self-identification requests were terminated and fines were canceled. The city government allows a person to dispute a fine but the procedure is reportedly long and complicated. Each person who allegedly violates the house quarantine rules is fined in the amount of RUB4,000 (approximately US\$70) under the city law.<sup>35</sup> While federal legislation provides for 10 times higher fines for approximately the same violations, it is the regional laws, which were quickly amended with detailed norms regulating the behavior of different categories of the population during the pandemic,<sup>36</sup> that are enforced.<sup>37</sup>

#### IV. Related Legislative Developments

On May 21, 2020, Russian media reported that the upper chamber of the legislature discussed a bill that would amend the Federal Law on Protection of People and Territories in Emergency Situations, which would define the regime of self-isolation and allow federal and regional authorities to impose varied restrictions on individuals' rights. Presently, Russian law differentiates between an emergency situation and a state of emergency. The Law on Emergency Situations emphasizes that additional measures undertaken by government authorities to mitigate the consequences of the emergency cannot restrict the rights and freedoms of people. These rights, specifically the right to free movement, were limited by isolation rules recently imposed by regional governments to fight the pandemic. These regional measures appeared to be in contradiction with federal legislation. The amendment appears to be able to bring the practice in line with legislation and create legal grounds for restriction of rights in the future.<sup>38</sup>

Also, a new Federal Law on Unified Federal Information Registry was passed by the legislature on May 21, 2020. The Law provides for the creation of a single comprehensive database run by

---

<sup>34</sup> Id.

<sup>35</sup> Liauw & Kodachigov, *supra* note 29.

<sup>36</sup> See, for example, City of Moscow Law No. 6 of Apr. 1, 2020 on Amending Select Legislative Acts of the City of Moscow, Mos.ru, <https://perma.cc/K976-XJJS>.

<sup>37</sup> Denis Dmitriev, *Sobyanin and Putin Introduced Different Fines for Self-Isolation Violations*, Meduza.io, Apr. 4, 2020, <https://perma.cc/929Z-XZS6>.

<sup>38</sup> *Russia Wants to Pass a Law on Forced "Self-Isolation" Giving the Authorities the Right to Restrict the Freedoms of Citizens*, Newsru.com, May 21, 2020, <https://perma.cc/K264-QZ5J>.

the National Tax Service that would collect data on all Russian citizens and residents and keep records of their personal life. Data will be collected from the police and other ministries and government organizations, including information on one's family status, education, employment, military service, citizenship and migration information, civil registration records, etc. All individual records will be linked to profiles of one's parents, spouses, and children. Legislators who introduced the Law stated that no medical or biometric information will be collected, although a person's social security and health insurance information shall be included in the database. The Law allows individuals to request information from the database and provides for the creation of a secure part of the database for information on persons placed under state protection. The Law will enter into force as soon as it is published, and a transition period will be established through December 31, 2026. The Law makes it possible for the collected information to be shared among government agencies and institutions.<sup>39</sup> Legislators from the opposition parties said that the Law contradicts the Constitution and violates the privacy rights of citizens. They stated that, presently, there are no technical means in Russia to guarantee the safety of the collected information.<sup>40</sup>

---

<sup>39</sup> Federal Law on the Unified Federal Information Registry of the Russian Federation Population, State Duma of the Russian Federation, May 21, 2020, <https://perma.cc/R6UW-WNFL>.

<sup>40</sup> *The State Duma Passed on Third Reading the Law on the Registry with Information About All Russians*, Newsru.com, May 21, 2020, <https://perma.cc/B7KR-UCB8>.

# Spain

*Graciela Rodriguez-Ferrand*  
*Senior Foreign Law Specialist*

**SUMMARY** Spain declared a state of alarm due to COVID-19 on March 14, 2020, and adopted a mandatory lockdown that was extended to May 24, 2020. The application of data protection regulations in health emergencies allows the data controller to adopt decisions necessary to protect the vital interests of individuals while safeguarding essential interests in the field of public health. Under the state of alarm, the government is empowered to take all measures necessary to protect the health and safety of citizens and strengthen the public health system, in addition to preventing and containing the virus and mitigating the health, social, and economic impacts. The Ley General de Sanidad also empowers health authorities, in epidemic situations, to establish extreme measures to protect public and individual health. Among these measures, the National Institute of Statistics has developed an app called "DataCovid," which is based on data provided by the main telecommunications operators. It uses positioning data from mobile devices, anonymized and aggregated, guaranteeing strict compliance with data protection standards.

## I. Introduction

Spain declared a state of alarm due to COVID-19 on March 14, 2020.<sup>1</sup> A mandatory lockdown was imposed, and it has been extended several times since then, the latest being an extension through May 24, 2020 (although gradual easing of restrictions began in early May).<sup>2</sup>

Spain has 47 million residents. Under the lockdown, people were allowed out only to go to work, shop for groceries, seek medical care, and briefly walk their dog.

As of May 21, 2020, there were 233,037 COVID-19 cases in the country, and 27,940 persons had died.<sup>3</sup>

---

<sup>1</sup> Real Decreto 463/2020, de 14 de marzo, por el que Se Declara el Estado de Alarma para la Gestión de la Situación de Crisis Sanitaria Ocasionada por el COVID-19, Boletín Oficial del Estado [B.O.E.] Mar. 14, 2020, <https://perma.cc/4WL5-NK2T>.

<sup>2</sup> Real Decreto 514/2020, de 8 de mayo, por el que se Prorroga el Estado de Alarma Declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se Declara el Estado de Alarma para la Gestión de la Situación de Crisis Sanitaria Ocasionada por el COVID-19, B.O.E. May 8, 2020, <https://perma.cc/W3X2-K32R>; *Spain Begins 4-Phase Easing of COVID Restrictions*, VOA News, May 2, 2020, <https://perma.cc/Z4D9-ZNRA>.

<sup>3</sup> Centro Nacional de Epidemiología, Ministerio de Sanidad, updated daily as of May 21, 2020, <https://perma.cc/8TRG-BVCK>.

Ninety-seven percent of households in Spain have a mobile phone.<sup>4</sup> Among six countries affected by the pandemic—the United States, United Kingdom, Germany, Spain, Australia, and Singapore—Spain has the largest number of people willing to share their health data to help fight the epidemic, according to a survey on “Data Preferences in Times of Corona” by the consulting firm Oliver Wyman, which found that only 15% of Spanish respondents would be unwilling to share such information.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

On March 12, 2020, the Agencia Española de Protección de Datos (AEPD) released a legal advisory report on measures affecting data privacy because of the COVID-19 emergency.<sup>6</sup>

The report states that EU General Data Protection Regulation (GDPR)<sup>7</sup> and Organic Law 3/2018 of December 5 (LPDP) on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)<sup>8</sup> constitute the legal framework applicable in the current COVID-19 emergency situation.

The GDPR allows data controllers to process personal data during health emergencies in a manner that protects the vital interests of individuals while safeguarding essential interests in the field of public health.<sup>9</sup>

In this regard, recital 54 of the GDPR provides that the processing of special categories of personal data, without the consent of the data subject, may be necessary for reasons of public interest in the field of public health. Such processing must be subject to appropriate and specific measures in order to protect persons’ rights and freedoms. This processing of health-related data for reasons of public interest should not result in third parties, such as employers, insurance companies, or banks, using personal data for other purposes.<sup>10</sup>

---

<sup>4</sup> Adrian Raya, *Todos los Móviles de España Serán Rastreados Durante Ocho Días*, *Espanol*, Oct. 29, 2019, <https://perma.cc/E585-HXYK>.

<sup>5</sup> Santiago Millán Alonzo, *Oliver Wyman: “Los Españoles Son los más Dispuestos a Dar sus Datos para las Apps Frente al Covid-19,”* *Cinco Días*, Apr. 15, 2020, <https://perma.cc/8J32-QJJ8>.

<sup>6</sup> AEPD, *Informe 017/2020 on the Treatment of Data Derived from the Present COVID-19 Virus Situation* (Mar. 12, 2020), <https://perma.cc/Z8GA-655Y>.

<sup>7</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [GDPR], 2016 O.J. (L119), <https://perma.cc/JU3K-S9JE>.

<sup>8</sup> Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales [LOPDGDD], B.O.E. Dec. 6, 2018, <https://perma.cc/7P49-UFAK>.

<sup>9</sup> AEPD, *supra* note 6, at 4; GDPR art. 9.2 (g) and (i).

<sup>10</sup> GDPR, recital 54.

In addition, all the data protection principles under the GDPR and the LOPDGDD are applicable in the current situation, including the principles of legality, trustworthiness and transparency, restrictive purpose (in this case, the safeguarding of vital and essential interests of natural persons), accuracy, and data minimization.<sup>11</sup>

The processing of personal data must be limited to that which is necessary for its intended purpose, because the fundamental right to data privacy protection remains effective, despite the fact that under the emergency situation, the necessary health data may be processed to prevent the spread of the disease that has caused the health emergency.<sup>12</sup>

In the current health emergency situation, initiatives are being developed that involve the processing of personal data including sensitive data such as health data.<sup>13</sup>

While the emergency is not necessarily a ground for the suspension of the fundamental right to the protection of personal data, data protection standards cannot be applied in such a way as to restrict the effectiveness of the measures adopted by the competent authorities, such as health authorities, in dealing with the health emergency.<sup>14</sup> Therefore, the authorities have to guarantee the lawful use of personal data compatible with the necessary measures to effectively guarantee the common good. To do this, the AEPDP is assisting health authorities, providing them with criteria that make these aims compatible.<sup>15</sup>

The AEPDP has established the criteria that must be applied for the processing of personal data under the current circumstances.<sup>16</sup> The data processed under this emergency may only be used for control of an epidemic, such as public agencies using information on the use of self-assessment applications, or geolocation data being used to create maps of areas of greater or lesser risk.<sup>17</sup>

The data so accessed and used must be limited to what the competent public authorities consider necessary to fulfill the goal of epidemic management and control.<sup>18</sup> Data may only be collected from those who are over 16 years of age, unless authorization of parents or legal representatives is received.<sup>19</sup>

---

<sup>11</sup> AEPD, *supra* note 6, at 7; GDPR art. 5.

<sup>12</sup> AEPD, *supra* note 6, at 7.

<sup>13</sup> *Comunicado de la AEPD Sobre Apps y Webs de Autoevaluación del Coronavirus*, AEPD (Mar. 26, 2020), <https://perma.cc/LAX3-6WTS>.

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

Under Orden SND/297/2020, the National Institute of Statistics (INE) is responsible for the processing of data and reporting on the movement of people during confinement, guaranteeing statistical secrecy and compliance with data privacy requirements.<sup>20</sup>

## B. Location Tracking

Organic Law 4/1981 on the State of Alarm, Exception, and Siege allows exceptional measures restricting the full enjoyment of certain rights and freedoms in cases of epidemics and health emergencies.<sup>21</sup> Among others, these measures include restricting the movement of people or vehicles at specific times and places, or requiring them to fulfill certain conditions.<sup>22</sup>

Applying the state of alarm provisions of LO 4/1981, Real Decreto 463/2020 empowers the Ministries of Health, Defense, Interior and Transportation, Mobility and Urban Agenda to take all necessary measures to protect the health and safety of citizens, contain the progression of the disease and strengthen the public health system, in addition to preventing and containing the virus and mitigating the health, social, and economic impacts.<sup>23</sup> These measures include the issuance of orders, resolutions, provisions and instructions necessary to guarantee the provision of all services, ordinary or extraordinary, to protect people, property and places, under the authority granted within the state of alarm declaration in compliance with article 11 of LO 4/1981.<sup>24</sup>

In addition, Organic Law 3/1986 of April 14, on Special Measures in the Field of Public Health, provides that health authorities may adopt measures specified in this Law when necessary to protect public health.<sup>25</sup> These measures are directed at illness detection, treatment, hospitalization, and control when confronting a risk to public health.<sup>26</sup>

In order to control communicable diseases, health authorities, in addition to carrying out general preventive actions, may adopt appropriate measures for the control of patients and people who are or have been in contact with them and their environment, as well as those deemed necessary in the event of a transmissible risk.<sup>27</sup>

---

<sup>20</sup> INE, *Análisis de la Movilidad de la Población Durante el Estado de Alarma por COVID-19 a Partir de la Posición de los Teléfonos Móviles* (Mar. 2020), <https://perma.cc/3YJM-Y349>, and Orden SND/297/2020, por la que se Encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el Desarrollo de Diversas Actuaciones para la Gestión de la Crisis Sanitaria Ocasionada por el COVID-19 art. 2, para. 3, B.O.E. Mar. 27, 2020, <https://perma.cc/C8YN-XYZF>.

<sup>21</sup> Ley Orgánica 4/1981, de los Estados de Alarma, Excepción y Sitio art. 4.b, B.O.E. June 5, 1981, <https://perma.cc/AGL2-G88D>.

<sup>22</sup> Id. art. 11.b.

<sup>23</sup> Real Decreto 463/2020 art. 4.

<sup>24</sup> Id. art. 4.3.

<sup>25</sup> Ley Orgánica 3/1986, de Medidas Especiales en Materia de Salud Pública, B.O.E. Apr. 29, 1986, <https://perma.cc/TSZ7-KFKV>.

<sup>26</sup> Id. art. 2.

<sup>27</sup> Id. art. 3.

The General Health Law also empowers health authorities, in epidemic situations, to establish extreme measures to protect public and individual health.<sup>28</sup> It provides for the adoption of preventive measures deemed appropriate in the event of an imminent and extraordinary risk to health, including seizures of property, restrictions of activity, and closure of businesses and facilities.<sup>29</sup>

In this regard, Orden SND/234/2020 establishes the obligation to send information to the Ministry of Health by the Autonomous Communities, public hospital centers and certain private hospital centers.<sup>30</sup> In furtherance of these orders, Orden SND 297/2020 provides for the development of technological solutions and mobile applications for data collection in order to improve the operational efficiency of health services, as well as better care and accessibility by citizens.<sup>31</sup> It creates the legal basis for the tracing of persons' movements within the restrictions imposed by data protection laws.<sup>32</sup>

### III. Electronic Measures to Fight COVID-19 Spread

The Ministerio de Asuntos Económicos y Transformación Digital has been working on new mobility analysis tools to support the fight against COVID-19. All data collected in an aggregated and anonymous manner by the INE has been made available to the governments of the Autonomous Communities.<sup>33</sup> In addition, some information prepared by the INE, and by the Ministerio de Transporte, Movilidad y Agenda Urbana, is now available on their websites.<sup>34</sup>

Mobile phone location data is used to track people's movements and verify how closely a nationwide lockdown is being respected.<sup>35</sup> Information will enable verification that users' area of residence match their actual location, thus enabling measurement of compliance with containment measures.<sup>36</sup>

The app, called "DataCovid" and managed by INE, is based on data provided by the main telecommunications operators.<sup>37</sup> Data received from these operators does not include personal

---

<sup>28</sup> Ley General de Sanidad art. 26, B.O.E. Apr. 29, 1986, <https://perma.cc/Y6C8-F5T2>.

<sup>29</sup> Id.

<sup>30</sup> Orden SND/234/2020, Sobre Adopción de Disposiciones y Medidas de Contención y Remisión de Información al Ministerio de Sanidad ante la Situación de Crisis Sanitaria Ocasionada por el COVID-19, B.O.E. Mar. 15, 2020, <https://perma.cc/W43B-XGRC>.

<sup>31</sup> Id. art. 1.

<sup>32</sup> Orden SND/297/2020.

<sup>33</sup> *El Gobierno Avanza en Nuevas Herramientas de Análisis de la Movilidad para Apoyar la Lucha Contra el COVID-19*, Ministerio de Asuntos Económicos y Transformación Digital (Apr. 16, 2020), <https://perma.cc/V9WX-YEMG>.

<sup>34</sup> Id.

<sup>35</sup> Id.

<sup>36</sup> Id.

<sup>37</sup> Id.

information allowing individual identification.<sup>38</sup> The use of positioning data from mobile devices, anonymized and aggregated, guarantees strict compliance with data protection standards under the LPDP.<sup>39</sup>

INE has concluded that, in general, since the state of alarm was adopted, 85% of people have not moved from their area of residence.<sup>40</sup> The Data COVID mobility study, which is updated daily, allows an estimate of the mobility of the Spanish population during the period of application of the containment measures in relation to a normal situation.<sup>41</sup> The information so collected lets the government know whether, after the entry into force of the containment measures, the movements of the population between territories increase or decrease, if there are areas with greater crowds, or if there are areas with a high density of people relative to their health care capacity.<sup>42</sup>

In addition, the app allows a coronavirus self-assessment that will only use geo-localization.<sup>43</sup> The app will be used for self-evaluation of coronavirus symptoms, providing practical advice and recommendations for health care resources.<sup>44</sup>

The official self-diagnosis mobile application is already being used in Asturias, the Canary Islands, Cantabria, Castilla-La Mancha and Extremadura, in addition to Madrid.<sup>45</sup>

Spain has also joined the Pan-European Proximity Tracking Project (PEPP-PT) through the Secretary of State for Digitization and Artificial Intelligence, to track mobile phones with an app after quarantine.<sup>46</sup> The PEPP-PT is a consortium that will develop a protocol to trace contacts without violating privacy, in order to prevent COVID-19 infections.<sup>47</sup>

The PEPP-PT is a nonprofit organization in Switzerland with more than 130 members from 8 countries, including scientists, psychologists, communicators, epidemiologists,

---

<sup>38</sup> Id.

<sup>39</sup> Id.

<sup>40</sup> Id.

<sup>41</sup> Id.

<sup>42</sup> Id.

<sup>43</sup> Orden SND/297/2020 art. 1.

<sup>44</sup> Id.

<sup>45</sup> La 'App' Oficial del Covid-19 Está Ya en Seis Comunidades Autónomas, *Economía Digital*, Apr. 6, 2020, <https://perma.cc/VJ4S-3LLV>.

<sup>46</sup> Jorde Pérez Colomé, *España Se Suma a un Proyecto Europeo de Rastreo de Móviles para Después de la Cuarentena*, *País*, Apr. 14, 2020, <https://perma.cc/6NWX-WZRL>.

<sup>47</sup> Alberto R. Aguiar, *España Tendrá una App para que Puedas Vigilar Contagios de Coronavirus Entre tus Vecinos, pero no Será Efectiva Hasta que se la Descarguen 23 Millones de Personas*, *Business Insider*, Apr. 14, 2020, <https://perma.cc/D8EP-W4ZM>.

telecommunications operators, universities and information technology experts in encryption, cybersecurity, and data protection.<sup>48</sup>

---

<sup>48</sup> Id.

# Turkey

*Kayahan Cantekin*  
*Foreign Law Specialist*

**SUMMARY** As of May 22, 2020, Turkey had 154,500 cases of COVID-19 and 4,276 COVID-19 related deaths. The country has wide smartphone possession and a high rate of mobile internet use, with 75% of the population using the internet and 89% of internet users 16 to 64 years of age owning a smartphone in 2019. The Turkish Ministry of Health employs electronic systems implemented via mobile applications to inform the populace of the risks, track the spread of the virus, and implement isolation measures. To date, the Ministry of Health has launched two mobile applications; one primarily for warning users when they approach areas with a high risk of infection and preventing high-risk individuals from using public vehicles for intercity travel, and the other for assigning positive cases and their possible contacts to members of contact tracing teams. Personal health data collected by these applications appear to be processed under a special rule allowing sensitive health data to be processed without the explicit consent of data subjects for purposes of the protection of public health.

In Turkish law, the general personal data protection framework is set by the Law on the Protection of Personal Data (LPPD). The Turkish personal data protection framework is largely harmonized with EU data protection law, albeit there exist certain divergences. In the electronic communications sector, the retention of traffic data, including certain categories of personal data, and the processing of location data by service providers are governed by the Regulation on the Processing and Protection of the Privacy of Personal Data in the Electronic Communications Sector (ECommDPR). The ECommDPR allows the use of location data without the consent of the data subject in cases of disasters, emergencies, and emergency calls.

## I. Introduction

According to the Turkish Ministry of Health, by May 22, 2020, Turkey had 154,500 cases of COVID-19 and 4,276 COVID-19 related deaths with 116,100 patients recovered and 1.77 million tests administered; 800 patients remained in ICUs, of which 401 were intubated.<sup>1</sup> Turkey was ninth in the list of countries with the most COVID-19 cases on May 22nd, according to the John Hopkins University Coronavirus Resource Center.<sup>2</sup>

In response to the outbreak, the Turkish government has deployed an array of electronic measures aimed at informing the populace of the risks, tracking the spread of the virus, and implementing isolation measures. These measures are mainly implemented with mobile applications running on smartphones or tablet computers, which citizens can install on their

---

<sup>1</sup> COVID-19 Situation Report, Turkish Ministry of Health (May 22, 2020), <https://perma.cc/4PDQ-WMRR> (in Turkish).

<sup>2</sup> COVID-19 Dashboard, John Hopkins U. Coronavirus Resource Ctr., <https://coronavirus.jhu.edu/map.html>.

devices on a voluntary basis. The Ministry of Health appears to process the personal data collected through these applications under a public health related exception regime that exists under the Turkish personal data protection framework.

Turkey has wide smartphone possession and a high rate of mobile internet use. According to data released by the Turkish Statistical Institute, 98.7% of households in Turkey had a mobile phone (including smartphones) in 2019, with 88.3% of households having internet access and 75.3% of the population using the internet.<sup>3</sup> According to the *Digital 2020* report published by We Are Social, a UK-based digital marketing agency, of the 62.07 million internet users in Turkey—74% of the population—58.23 million (93.8%) were also mobile internet users.<sup>4</sup> The report found that 74.8% of web traffic (websites served to web browsers) is attributable to mobile phone use, and 89% of internet users 16 to 64 years of age own a smartphone.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

Article 20 of the Constitution of Turkey enshrines a person's right to protection of his or her privacy and personal data, providing that "[p]ersonal data can be processed only in cases envisaged by law or by the person's explicit consent."<sup>6</sup> Turkish personal data protection law is largely harmonized with the European Union's data protection framework. The main national legal framework that provides the general rules and principles of personal data protection in Turkish law is set forth in the Law on the Protection of Personal Data (LPPD) and the various relevant secondary legislation that governs certain aspects of personal data protection law such as the processing of personal health data, the protection of personal data in electronic communications, and the erasure, destruction, or anonymization of personal data.<sup>7</sup> These are complemented by personal data protection statutes in numerous laws that regulate the provision of services in the public and private sectors. The protection of privacy and personal data in the electronic communications sector is governed by the Regulation on the Processing and Protection of the Privacy of Personal Data in the Electronic Communications Sector (ECommDPR).<sup>8</sup>

---

<sup>3</sup> TurkStat, *Availability of Devices in Households, 2004-2019*, <https://perma.cc/MK2Z-74VA>; TurkStat, *Information Society Statistics, 2004-2019*, <https://perma.cc/4XM2-BRAN>.

<sup>4</sup> Simon Kemp, *Digital 2020: Turkey*, We Are Social (Feb. 18, 2020), <https://perma.cc/NF3B-9BBL>.

<sup>5</sup> *Id.*

<sup>6</sup> Constitution of Turkey, Law No. 4121, as amended, art. 20, <https://perma.cc/4EEX-3DM8> (in English).

<sup>7</sup> Law on the Protection of Personal Data, Law No. 6698, Official Gazette No. 29677 (Apr. 7, 2016), <https://perma.cc/EWS6-NN77> (unofficial English translation); Regulation on Personal Health Data, Official Gazette No. 30808, (June 21, 2019), <https://perma.cc/7GX5-457G> (in Turkish); Regulation on the Processing and Protection of the Privacy of Personal Data in the Electronic Communications Sector (ECommDPR), Official Gazette No. 28363 (July 24, 2012), <https://perma.cc/ZL5E-38RL> (in Turkish); Regulation on the Erasure, Destruction, or Anonymization of Personal Data, Official Gazette No. 30224 (Sept. 28, 2017), <https://perma.cc/JY8Z-DBPG> (in Turkish).

<sup>8</sup> ECommDPR, *supra* note 7.

### 1. *Law on the Protection of Personal Data*

The LPPD sets forth the principles that govern the processing of personal data, providing that any processing of data must be done in conformity with the law and in good faith, that the data must be accurate and up to date, that the data must be processed for a specified, explicit, and legitimate purpose and the processing must be relevant, limited, and proportionate to the purposes of processing, and that the data must be stored only for the duration that is necessitated by law or by the purpose for which the data was collected.<sup>9</sup> The LPPD sets forth the explicit consent of the data subject as the principal condition for the processing of personal data, and provides an additional list of conditions under which personal data may be processed without the explicit consent of the data subject.<sup>10</sup>

Similar to the scheme under EU law, the LPPD applies a special protection regime to “special categories of personal data,” namely, data relating to “race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics.”<sup>11</sup> These categories of personal data, except data relating to health and sexual life, may be processed without the explicit consent of the data subject only if prescribed by law.<sup>12</sup> On the other hand, according to the exception regime provided under article 6(3) of the LPPD, data relating to health and sexual life may only be processed without explicit consent “for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by persons under the obligation of secrecy or authorized institutions and organizations.”<sup>13</sup> Personal data processed in accordance with the law must be erased, destroyed, or anonymized ex officio by the data controller or upon request from the data subject when the reasons necessitating the processing cease to exist.<sup>14</sup> The rules and principles that govern the erasure, destruction, and anonymization process are provided in a regulation and guidelines issued by the Turkish Data Protection Authority (DPA).<sup>15</sup>

### 2. *Regulation of Personal Data Processing and Privacy in the Electronic Communications Sector*

The ECommDPR governs the specialized personal data protection regime that electronic communications service providers operating under the Law on Electronic Communications (LEC) must comply with.<sup>16</sup> The ECommDPR sets forth rules regarding the management of data

---

<sup>9</sup> LPPD art. 4(2).

<sup>10</sup> Id. art. 5.

<sup>11</sup> Id. art. 6(1).

<sup>12</sup> Id. art. 6(3).

<sup>13</sup> Id.

<sup>14</sup> Id. art. 7(1).

<sup>15</sup> Regulation on the Erasure, Destruction, or Anonymization of Personal Data, *supra* note 7.

<sup>16</sup> Law on Electronic Communications, Law No. 5809, Official Gazette No. 27050 (Nov. 10, 2008), <https://perma.cc/P4K3-NQ5J> (in Turkish).

safety, notification of risks and data breaches to data subjects, the processing and retention of data, including traffic data and location data, and certain privacy services that electronic communication service providers must provide to their customers.<sup>17</sup>

The ECommDPR prohibits the listening, tapping, storage, termination, or surveillance of communication without the consent of all parties to the communication, except in cases prescribed by law or in accordance with a court decision.<sup>18</sup> Moreover, service providers may not process traffic data, defined as “data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof,” for purposes that are not within the scope of the services they provide.<sup>19</sup> Traffic data may be processed by service providers only for purposes such as traffic management, interconnection, billing, fraud prevention, and dispute resolution.<sup>20</sup> ECommDPR provides the purposes for which certain categories of traffic data may be retained by service providers and prescribes the mandatory retention duration of certain traffic data.

## **B. Data Retention and Location Tracking**

### *1. Data Retention*

According to article 4(2)(d) of the LPPD, personal data may be retained for no longer than is provided in special laws or is necessary for the purposes for which the personal data are processed. Rules regarding the retention of personal data processed in the context of the provision of electronic communications are provided in the ECommDPR and based on the authority delegated by article 51 of the LEC, which is the special law regulating the electronic communications sector.

The ECommDPR provides a list of categories of data that electronic communications service providers are required to retain; the categories fall under data necessary for the following purposes: to trace and identify the source of a communication, to identify the destination of a communication, to identify the date, time, and duration of a communication, to identify the type of communication, to identify users’ communication equipment or what purports to be their equipment, and to identify the location of mobile communication equipment. Service providers are required to retain this data for one year from the date the communication occurred, and for three months for calls that are not connected.<sup>21</sup> The retained data must be stored in Turkey, and it must be destroyed or anonymized within one month after the date on which the mandated retention period ends.

Additionally, the ECommDPR requires service providers to retain personal data related to criminal investigations, inspections, audits, and disputes until the relevant process has ended,

---

<sup>17</sup> ECommDPR arts. 5, 6, 8-15, and 17-20, respectively.

<sup>18</sup> ECommDPR art. 7(1).

<sup>19</sup> *Id.* art. 8(1).

<sup>20</sup> *Id.* art. 8(2).

<sup>21</sup> *Id.* art. 14(1).

and retain records regarding access to personal data and relevant systems for four years. Service providers must also retain records on the consent provided by the users regarding the processing of their personal data at least until the subscription of the user is terminated.

## 2. Location Tracking

The LEC and the ECommDPR echo the same principle set forth in the EU ePrivacy Directive concerning the processing of location data,<sup>22</sup> providing that location data may only be processed if it is made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value-added electronic communication service.<sup>23</sup> Location data is defined as “data processed in an electronic communications network or via an electronic communications service, indicating the geographical position of the terminal equipment of a user.”<sup>24</sup> The ECommDPR further provides that service providers must offer users means to temporarily disallow the use of location data (data that is not traffic data), and means to withdraw their consent for the use of location data easily, immediately, and free of charge.<sup>25</sup> ECommDPR also provides for an exception to the consent rule, stipulating that location data may be processed without the consent of the user only “in cases of disasters, emergency, or in the context of emergency calls.”<sup>26</sup>

### III. Electronic Measures to Fight COVID-19 Spread

In response to the need for employing technological solutions to track and limit the spread of COVID-19, the Turkish Ministry of Health has launched several projects incorporating mobile applications that run on smartphones or tablet computers. These projects are complemented by the regular Turkish public digital health data management platform called *E-Nabız* (E-Pulse). Also, the DPA has issued two guidelines specific to the processing of personal data by the Ministry of Health and authorized institutions within the context of public health measures deployed to counter the outbreak.

#### A. Guidelines of the Turkish Data Protection Authority

The DPA issued two guidance statements relevant to electronic measures that could be deployed to fight the COVID-19 outbreak. On March 27, 2020, the DPA issued guidance on the processing of personal data, especially health data, in the context of the COVID-19 outbreak.<sup>27</sup> The DPA noted that employers were authorized to share the relevant personal data of persons who contracted COVID-19 with public authorities based on article 8 of the LPPD, which authorizes

---

<sup>22</sup> Consolidated Version of the Directive on Privacy and Electronic Communications (ePrivacy Directive), 2002 O.J. (L 201) 37, <https://perma.cc/YHA5-EFXV>.

<sup>23</sup> LEC art. 51(8); ECommDPR art. 11(1).

<sup>24</sup> ECommDPR art. 3(1)(j).

<sup>25</sup> Id. art. 11(1) and (2).

<sup>26</sup> Id. art. 11(3).

<sup>27</sup> Turkish Data Protection Authority, *On Protection of Personal Data During the Fight Against COVID-19* (Mar. 27, 2020), <https://perma.cc/42BX-U6JM> (in English).

the transfer of health data for purposes of the protection of public health.<sup>28</sup> The statement further explained that the LPPD would not apply to the processing of health data by the Ministry of Health and other public institutions for the purposes of fighting the outbreak, citing the derogation stipulated in article 28(1)(ç) providing that the LPPD will not apply to the “[p]rocessing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organizations who are assigned and authorized for providing national defence, national security, public safety, public order or economic safety.”

The DPA issued a second guidance issued on April 9, 2020, regarding the use of location data in connection with COVID-19 measures.<sup>29</sup> The DPA explained that location data, as defined in ECommDPR, is a type of personal data that would normally be protected under the LPPD. However, the DPA reiterated its position that the processing of data by the Ministry of Health and other public institutions and persons authorized by law for the purpose of fighting the outbreak would fall under the article 28(1)(ç) derogation of the LPPD, thus concluding that public institutions could process location data under the derogation as well. The DPA reiterated that although such processing would be within the scope of the derogation, the institutions and persons undertaking such processing must take all technical and administrative measures necessary to ensure the security and privacy of the data and must erase or destroy the data once the reasons necessitating the processing cease to exist.

## **B. Electronic Measures Deployed by the Ministry of Health Against the COVID-19 Outbreak**

Before the outbreak, the Turkish public health system already employed an extensive electronic health data management system called *Sağlık-NET*, with patient access to the system provided via the online portal *E-Nabız*.<sup>30</sup> The use of this portal is voluntary; users sign up to the system with their names and Turkish ID numbers and may access the system via website or mobile application. The Ministry of Health requires all healthcare providers to upload patients’ medical test results, diagnoses, and prescriptions to the centralized system, and the data remain in storage with the Ministry of Health without being anonymized, which has caused concerns among numerous commentators, including the Turkish Medical Association.<sup>31</sup> Patients can view their health data uploaded in the system through their *E-Nabız* accounts, and they have some control over the extent of access that healthcare providers have to the data, by giving or withholding consent electronically on the platform.<sup>32</sup> The Regulation on Personal Health Data provides standard rules for the access of healthcare providers to the health data of patients who

<sup>28</sup> LPPD art. 8(2), by reference to LPPD art. 6(3).

<sup>29</sup> *Covid-19 ile mücadelede konum verisinin işlenmesi ve kişilerin hareketliliklerinin izlenmesi hakkında bilinmesi gerekenler*, Turkish Data Protection Authority (Apr. 9, 2020), <https://perma.cc/KD38-E3AL>.

<sup>30</sup> Gov’t of Turkey, *About e-Nabız*, <https://perma.cc/W6RF-EKMB> (in English). The Ministry of Health bases the legality of the *Sağlık-NET* system on art. 3(f) of the Health Services Code, Law No. 3359, Official Gazette No. 19461 (May 15, 1987), <https://perma.cc/9FGR-76HZ> (in Turkish).

<sup>31</sup> See, e.g., Turkish Med. Ass’n, *e-Nabız çöktü!* (Sept. 13, 2019), <https://perma.cc/CU8C-5VSD>; for the administrative order governing the integration of all healthcare providers with the system, see Turkish Ministry of Health, *Sağlık.Net Online ve e-Nabız*, Circular No. 67189002 – 2016/6 (Apr. 26, 2016), <https://perma.cc/ZR4T-872D>.

<sup>32</sup> *Id.*

are not *E-Nabız* users.<sup>33</sup> *E-Nabız* users who have taken COVID-19 tests can see their results in their *E-Nabız* accounts.<sup>34</sup>

Besides *E-Nabız*, the Ministry of Health has set up two digital systems specific to the COVID-19 containment effort, addressing contact tracing and isolation.

On April 8, 2020, the Ministry of Health launched the “Pandemic Isolation Tracking Project” (*Pandemi İzolasyon Takip Projesi – PİTP*).<sup>35</sup> The PİTP incorporates the mobile application “Life Fits Home” (*Hayat Eve Sığar*), which users can download.<sup>36</sup> The application collects health data from users who voluntarily respond to questions about their age, how they feel physically, whether they are experiencing symptoms, and whether they have preexisting medical conditions. This information is then used for assigning a risk factor to the user and populating an epidemic heat map that can be viewed by application users, if the user shares his or her location data with the application. Users may also track the risk status and location of their consenting family members by adding them to their profile. The application warns the user if he or she, or a family member who was added to the profile, enters a high-risk zone. The application shows the user the nearest essential facilities such as hospitals, pharmacies, markets, and public transportation on a map.<sup>37</sup>

The application incorporates a module for creating a 10 or 12 digit code that includes information regarding the user’s infection risk status. On May 30, 2020, the Ministry of Internal Affairs issued a circular ordering the use of the code, called a “HES code,” for purchases of all intercity and international travel tickets on public modes of transportation, including air travel.<sup>38</sup> Travelers will not be allowed by operators on public transportation vehicles if their HES codes indicate that they were diagnosed as positive, or they have been in contact with a person diagnosed as such.<sup>39</sup> Moreover, the system will warn passengers who have been in a public transportation vehicle in the last 14 days with a person who was not indicated to be at risk by their HES code at the time of travel but has later been determined to be at risk.<sup>40</sup> Persons who are issued Turkish ID numbers can obtain HES codes via the Life Fits Home mobile application, through Turkey’s general e-

---

<sup>33</sup> Regulation on Personal Health Data, *supra* note 7, art. 6.

<sup>34</sup> Barış Gündoğan, Koronavirüs testi yaptırانlar sonuçlara 'eNabız'dan ulaşabilecek, Anadolu Agency (Mar. 20, 2020), <https://perma.cc/4LD8-WF2K>.

<sup>35</sup> *Pandemi İzolasyon Takip Projesi nedir: Covid-19 salgını kapsamında nasıl kullanılacak?*, BBC News Turkey (Apr. 8, 2020), <https://perma.cc/XDE7-6C6Q>.

<sup>36</sup> *Hayat Eve Sığar uygulaması nasıl indirilir? Hayat Eve Sığar uygulaması nerelerde kullanılacak?*, TRT Haber (May 20, 2020), <https://perma.cc/9LT3-E2MA>.

<sup>37</sup> *Id.*

<sup>38</sup> Muhammed Nuri Erdoğan, 15 ildeki seyahat kısıtlaması bugün gece sona erecek, Anadolu Agency (May 30, 2020), <https://perma.cc/YN72-ZHHV>.

<sup>39</sup> *What Is HES Code?*, Turkish Ministry of Health *Hayat Eve Sığar* Info. Website, <https://perma.cc/EU4U-CGMP> (in English).

<sup>40</sup> *What Is HES Code for?*, Turkish Ministry of Health *Hayat Eve Sığar* Info. Website, <https://perma.cc/BTV8-UU6V> (in English).

government portal *e-Devlet*, or via SMS (short message service).<sup>41</sup> Persons who do not have Turkish ID numbers will not be required to have HES codes to travel until June 5; beginning on June 6, these persons will be able to obtain codes via SMS by using their personal information and passport numbers.<sup>42</sup> HES codes do not appear to include identifiable personal data.<sup>43</sup>

The mobile application also incorporates access to the Ministry's surgical mask distribution scheme, whereby users who are between 20 and 65 years of age can download a data matrix code issued by the Ministry with which to obtain five free surgical masks every 10 days from stocked pharmacies.<sup>44</sup> The free mask distribution scheme complemented the Turkish government's strategy of imposing a stricter curfew on persons who are younger than 20 and older than 65, which aims to enable the low-risk and economically active population to keep participating in production while keeping the high-risk and economically less active population at home.<sup>45</sup>

The Ministry has launched a separate mobile application for the use of contact tracing teams. This application works with the Ministry's "Transmission and Isolation Tracking System" (*Filyasyon ve İzolasyon Takip Sistemi*—FITAS). Through the application, members of contact tracing teams can access the contact information of patients who are assigned to them (persons who have tested positive, or are reported to have had contact with a positive case) to reach these persons to administer tests and inquire about their previous movements and contacts.<sup>46</sup>

Significantly, the privacy policies of both mobile applications state that the Ministry of Health processes the data collected via the applications under the exception for the processing of special categories of personal data provided in article 6(3) of the LPPD, which authorizes the use of health data by authorized institutions without the explicit consent of data subjects for purposes of, among other things, protection of public health, medical diagnosis, treatment, or care services.<sup>47</sup> A press release issued by the Directorate of Communications of the Presidency of Turkey confirmed that the government viewed the data collection and processing for purposes of the

---

<sup>41</sup> *How to Get HES Code?*, Turkish Ministry of Health *Hayat Eve Sığar* Info. Website, <https://perma.cc/UFU4-X3ZT> (in English).

<sup>42</sup> *Id.*

<sup>43</sup> *Is It Safe?*, Turkish Ministry of Health *Hayat Eve Sığar* Info. Website, <https://perma.cc/PP7N-5GLK> (in English).

<sup>44</sup> *Hayat Eve Sığar uygulaması indir: Hayat eve sığar maske kodu nasıl alınır?*, *Hürriyet* (May 4, 2020), <https://perma.cc/ZV6G-FG3E>.

<sup>45</sup> Arwa Damon & Gul Tuysuz, *With Weekend Lockdowns and Age-Specific Restrictions, Turkey Takes a Different Coronavirus Approach*, *CNN* (Apr. 17, 2020), <https://perma.cc/9EUB-VMVT>. This regime was somewhat relaxed by an order of the Ministry of Internal Affairs issued on May 29, 2020, whereby persons between 18 and 20 years of age and persons who were older than 65 but could prove that they were economically active were exempted from the curfews. *81 İl Valiliğine 18 Yaş Altı ile 65 Yaş ve Üzeri Kişilerin Sokağa Çıkma Kısıtlaması Genelgesi*, Turkish Ministry of Health (May 29, 2020), <https://perma.cc/G5F2-UMDU>.

<sup>46</sup> Mehmet Siddik Kaya, *Koronavirüsle mücadelenin sahadaki kahramanları: Filyasyon ekipleri*, *Anadolu Agency* (May 9, 2020), <https://perma.cc/HQ42-6U9B>.

<sup>47</sup> Turkish Ministry of Health, *Hayat Eve Sığar* [Mobile Application Privacy Policy], <https://perma.cc/4KAR-4QXU> (in Turkish); *Filyasyon ve İzolasyon Takip Sistemi* [Mobile Application End User Agreement and Privacy Policy], Turkish Ministry of Health, <https://perma.cc/457Q-C4L2> (in Turkish).

PITP as being in accordance with article 6(3) of the LPPD.<sup>48</sup> Thus, it does not appear that the government is currently making use of the article 28(1)(ç) public safety/order derogation in the LPPD as the basis of its processing of health data in connection with the electronic measures that it employs in the fight against the spread of COVID-19.

---

<sup>48</sup> Press Release, Presidency of Turkey Directorate of Comm., *Kovid-19'a karşı Pandemi İzolasyon Takip Projesi geliştirildi* (Apr. 2020), <https://perma.cc/73FM-4ERC>.

*Middle East and Africa*

# Iran

*Shadi Karimi*  
*Foreign Law Consultant*

**SUMMARY** Given the emergency created by the outbreak of COVID-19 in Iran, the government had several options for managing the crisis, including by utilizing the constitutional powers of the Parliament to interpret and apply articles 68 and 79 of the Constitution to postpone the elections and implement temporary measures to impose social distancing and quarantines. Alternatively, it had available the article 176 constitutional authorities of the Supreme National Security Council to manage the crisis as a national security and defense matter under the leadership of the President, the ministers, and other key governmental and defense figures, within the limits provided by the Supreme Leader and through decisions authorized by him, and this is the management path it chose.

The Supreme National Security Council established the National Headquarters to Combat Corona in February 2020, which is directing the country's efforts against COVID-19 under the direct leadership of the Minister of Health and Medical Education, and has implemented various other measures including applications and websites for voluntary registration, self-assessments, prevention and statistical information, medical assistance, and infection risk notifications. Many of these measures have become contentious due to the arguable infringement of people's rights to privacy and data protection under Iranian law, which is discussed in this report. The information provided is based on Iranian legislation, public measures, news sources, and other publicly available information.

## I. Introduction

As of May 22, 2020, the Iranian government had announced a total of 131,652 confirmed COVID-19 cases and 7,300 deaths; 102,276 recoveries; and 2,659 patients currently in critical condition.<sup>1</sup> The World Health Organization's May 22 report on Iran indicated 129,341 total confirmed cases and 7,249 deaths.<sup>2</sup>

Iranian government officials, including the Ministry of Health and Medical Education, have repeatedly prompted people through text messaging and other methods to participate in providing information by registering with the approved self-assessment applications and websites or to call or respond to calls from dedicated phone numbers. In an attempt to encourage people's trust to engage with providing their information, the Ministry of Health published its privacy policy, indicating that the Ministry is strictly protective of all individuals' privacy and

---

<sup>1</sup> AC19 Official Coronavirus Daily Reports and Registration Page (website as viewed on May 22, 2020), <https://ac19.ir/>; 2,311 New COVID-19 Cases; National Death Toll Reaches 7,300, Ministry of Health and Medical Education (May 22, 2020), <https://perma.cc/8U5N-736Y> (all sources are in Farsi unless otherwise noted) .

<sup>2</sup> *Coronavirus Disease (COVID-19) Situation Report 123*, World Health Organization (May 22, 2020), <https://perma.cc/YN6N-GJ86> (in English).

personal data, in compliance with the 2017 Decree of the Supreme Administrative Council Concerning the Charter on Citizens' Rights in the Administrative Systems.<sup>3</sup>

Iranian government officials have reportedly expressed satisfaction with people's response to the combination of electronic self-assessments, telephone and in-person medical reviews, and the COVID-19 tests. On April 21, 2020, the Deputy Minister of Health and Medical Education indicated that this combination has provided the government with the COVID-19-related information of over 70 million people (the total Iranian population numbers approx. 84 million).<sup>4</sup> On May 3, 2020, the Iranian President made a general statement during an official meeting with the Supreme Leader and the National Headquarters for Combating Corona that roughly 83% of the Iranian population has followed government requests and guidelines for combating the spread of the coronavirus.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

Pursuant to the Iranian Constitution, statutes, and regulations, people's dignity, life, property, rights, domicile, and occupation must not be violated, unless sanctioned by law. Although Iran has not passed comprehensive legislation dedicated entirely to privacy rights and data protection, the right to privacy and data protection has been emphasized in various pieces of legislation and in the Constitution. The law holds as private and protected every individual's private assets, body, character, and places, whether tangible or virtual, where a person can have a reasonable expectation of privacy. This includes personal documents, mail, phones, computers, telephone conversations, and all other data transmitted in a private manner in cyberspace that could be traceable to that individual, such as all personally identifiable information (e.g., an individual's name, home and work addresses, bank accounts) and sensitive personal data (e.g., information concerning family matters, criminal records, tribal or ethnic origins, moral and religious beliefs, ethical characteristics, sexual habits, genetics, health status, and physical or psychological status).<sup>6</sup>

---

<sup>3</sup> *Privacy Policy Statement*, Ministry of Health and Medical Education, <https://perma.cc/F2EJ-P8K4>; Decree of the Supreme Administrative Council Concerning the Charter on Citizens' Rights in the Administrative Systems, Official Gazette of the Islamic Republic of Iran, Apr. 10, 2017, No. 20995, <https://perma.cc/HYL4-ST89>.

<sup>4</sup> Evaluating Latest Corona Situation with Attendance of Government Officials at Health Commission [Meeting], Parliament News Agency (Apr. 21, 2020), <https://perma.cc/ZUM6-DEEL>; Details of Ministry of Health Mandates for Corona, Islamic Republic News Agency (Mar. 3, 2020), <https://perma.cc/HSP6-FSDW>.

<sup>5</sup> *83% of People Have Complied with Health Regulations*, Presidential News Center (May 3, 2020), <https://perma.cc/J7Q2-5QQ8>.

<sup>6</sup> Constitution of the Islamic Republic of Iran 1979, as amended, arts. 22, 25, <https://perma.cc/JN9G-4QUV>, English translation, <https://perma.cc/3CGR-CNRF>; Law on Respect for Legitimate Freedoms and Citizens Rights, May 5, 2004, § 8, <https://perma.cc/HA44-RJSN>; Electronic Commerce Law, Jan. 7, 2004, arts. 1-5, 11, 33-35, 38, 58-60, 71-72, 79, <https://perma.cc/U72P-XFF9> (English translation); Cybercrime Act, Dec. 24, 2009, arts. 1, 2, 5, 25, 32, 34, 38, 39, 48, <https://perma.cc/723P-9WNU>; General Policies for "Security of Production Space and Information Exchange and Communication (Afta)," Feb. 18, 2011, § 1, <https://perma.cc/NF7Z-DLDV>; Law on the Release and Freedom of Information, Aug. 22, 2009, arts. 13-15, <https://perma.cc/M7T4-3PKM>; Criminal Procedure Code of Iran 1392 [2014], arts. 4, 40, 150, <https://perma.cc/D83H-NQZ8>; Law on

Hence, all forms of access and investigation of the aforementioned items or materials, whether for the purpose of searching, collecting, processing, analyzing, using, storing, or sharing it, are generally legally forbidden regardless of whether the intention is good or bad, unless access or inspection is allowed either by informed, express, and written consent of the individual, according to a subject-specific law or regulation, or by a legal order. For example, in *ta'zir* offenses of the fifth to eighth degrees, the court may, with the offender's consent, put the offender under the supervision of an electronic system within a specific area.<sup>7</sup>

Any legal access or investigation based on an individual's informed consent, other laws, or legal orders must be performed within a legally defined scope and is subject to certain requirements. Among others, those requirements include

- consideration for the individual's dignity,
- an adequately secure information system,<sup>8</sup>
- a clear statement of the purpose of access,
- a scope limited to what is necessary for achieving the purported purpose,
- transparency,
- preserving the data's integrity with subsequent updates, and
- anonymization and aggregation to the extent required by law.

Iranian courts generally enforce measures against cyber violations according to the statutorily defined remedies of the applicable laws or regulations, which may include punitive damages and/or imprisonment as defined under the Cyber Crime Act; sanctions on the violators' bank accounts, applications, and websites; and other measures. Generally, crimes committed in cyberspace are within the jurisdiction of the Special Cyber Crime Court and the Iranian Cyber Police (a.k.a. FATA).<sup>9</sup>

---

"Protection of Individuals Who Are Promoting Islamic Ethics," May 23, 2015, art. 5, Official Gazette of the Islamic Republic of Iran, May 23, 2015, No. 20464, <https://perma.cc/4S9R-JB4R>; Charter on Citizens Rights, Nov. 2016, arts. 36–40, <https://perma.cc/VUW7-PD6Z>; Draft of the Bill on the Protection of Data and Privacy in Cyberspace, June 2018, arts. 1–2, 4–8, 12, 14, 19, 26, 27, 67, 68, <https://perma.cc/KA2Z-52AT>.

<sup>7</sup> Islamic Penal Code of Iran 1392 [2013], art. 62, <https://perma.cc/A4PS-C7L4>.

<sup>8</sup> A "secure information system" is defined as an information system that is reasonably protected against misuse or penetration; possesses a reasonable level of proper accessibility and administration; is reasonably designed and organized in accordance with the significance of the task; and is in compliance with secure methods. A "secure method" is a method to authenticate the date, correctness, origin, and destination of data messages, as well as to detect errors and modifications in its communication, content, or storage "from a certain point." A secure message is generated using algorithms or codes, identification words or numbers, encryption, acknowledgement call-back procedures, or similar secure techniques. *Data Protection Laws of the World (Iran)*, DLA Piper (May 23, 2019), <https://perma.cc/CGT8-BQRA> (in English).

<sup>9</sup> Constitution of the Islamic Republic of Iran arts. 22, 25; Law on Respect for Legitimate Freedoms and Citizens Rights § 8; Electronic Commerce Law arts. 1–5, 11, 33–35, 38, 58–60, 71–72, 79; Cybercrime Act arts. 1–2, 5, 25, 32, 34, 38, 39, 48; General Policies for "Security of Production Space, Information Exchange and Communication (Afta)" § 1; Law on Release and Freedom of Information arts. 13–15; Criminal Procedure Code

## B. Data Retention and Location Tracking Legislation

The juxtaposition of the general privacy and data protection framework (as explained in Part II(A), above) and the laws and regulations that reserve the government's right to access private data in situations involving a governmental or public purposes is shown in various statutes and regulations.

Pursuant to article 150 of the Criminal Procedure Code 2015, controlling an individuals' telecommunications is prohibited, except when it is necessary for the national security of the country or in investigation of certain enumerated crimes, and in the case of such exceptions it must be carried out within a specific scope and timeframe. Furthermore, the Supreme National Security Council (SNSC)<sup>10</sup> is the authority that would determine the conditions and requirements for such access or investigation.<sup>11</sup>

Article 15 of the Law on Release and Freedom of Information 2010 is directed at any governmental or nongovernmental entity that might receive a request for release of information that is entrusted with the respective entity, emphasizing that such entities must refrain from providing any data that might reveal private information of a natural person third party, except if the requester is a public entity and that according to the law the requested information is directly relevant to its responsibilities as a public entity, or when the third party has provided express written consent.<sup>12</sup>

---

of Iran arts. 4, 40, 150; Law on "Protection of Individuals Who Are Promoting Islamic Ethics" art. 5; Charter on Citizens Rights arts. 36–40; Draft of the Bill on Protection of Data and Privacy in Cyberspace arts. 1–2, 4–8, 12, 14, 19, 26, 27, 67, 68.

<sup>10</sup> The Supreme National Security Council, led by the Iranian President, is the highest-ranking power after the Supreme Leader in matters of national security against domestic and global threats. The Council's enumerated constitutional authorities for the main purpose of defending national security are explicitly within the limits provided by the Supreme Leader, and its decisions are enforceable as law after his approval. Among the constitutional authorities granted to the Supreme National Security Council is the power to entrust parts of its responsibilities to sub-councils, in which case those sub-councils remain under the control of the President of the country, or the President can delegate the control to another member of the Supreme National Security Council. The National Headquarters for Combating Corona, as a sub-entity of the Supreme National Security Council, could arguably be considered a political entity as well; hence, it is plausible that it could be immune from citizens' lawsuits. Constitution of the Islamic Republic of Iran arts. 173, 176; Law on the Organization and Procedure of the Court of Administrative Justice, Mar. 18, 2017, art. 12, <https://perma.cc/F9VW-CHVV>; *Analysis of the Plausibility of Judicial Oversight on the National Headquarters for Combating Corona*, Allameh Tabataba'i News Agency (Apr. 9, 2020), <https://perma.cc/LBG2-BHDL>. According to Article 176 of the Constitution, the Supreme National Security Council consists of the heads of the three branches of the government (the President as the Chairman of the Council, the Speaker of the Parliament, and the Chief Justice), two representatives appointed by the Supreme Leader, the Chief of the General Staff of the Armed Forces, the Chief of the Army, the Chief of the Islamic Revolutionary Guard, the Minister of Foreign Affairs, the Minister of the Interior, the Minister of Intelligence, the Head of the Management and Planning Organization, and the minister of the ministry that is the subject of the Council's agenda at the time.

<sup>11</sup> Criminal Procedure Code of Iran arts. 4, 40, 150.

<sup>12</sup> Law on Release and Freedom of Information arts. 13–15.

Article 39 of the Charter on Citizens Rights 2017 reiterates that all entities and natural and legal persons must protect the privacy and security of the personal data entrusted to them; however, they must also provide the said data to “judicial institutions and eligible administrative institutions,” upon necessity and request.<sup>13</sup>

Article 4 of the draft Bill on Protection of Data and Privacy in Cyberspace, which has remained in the legislative process since 2018,<sup>14</sup> would require the consent of individuals to access their private data if access was not due to public concerns and circumstances.<sup>15</sup> Article 6 of the same bill would authorize access to individuals’ private data concerning public issues and circumstances, if the individuals directly or indirectly exposed their data or failed to adjust their settings to prevent third-party access.

Article 32 of the Cyber Crime Act 2009 requires providers of electronic, internet, or data services to keep all metadata and tracing data for any information that enters their cyberspace, including the data’s type, origin, direction, destination, duration, date, time, etc. This data must be retained for a minimum of six months from the date of creation of the data. The users’ information, such as IP address, personal identity information, geographic location data, phone numbers, etc., must be retained for a minimum of six months from the date of termination of services.<sup>16</sup>

Generally, in Islamic jurisprudence violating an individual’s private zone, whether that involves a person’s body, private assets, or information, in a manner that is against the individual’s dignity is widely abhorred, and the protection of one’s own and others’ privacy is greatly encouraged; accordingly, a similar approach is visible in Iranian legislations that is substantially motivated by Sharia. However, in both Islamic jurisprudence and Iranian laws and judicial precedent there are principles that grant supreme importance to the benefit of the public and protection of the Islamic system of governance, which, depending on the circumstances, could outweigh the individuals’ privacy and data protection rights if those rights are incompatible with the stated benefits.

A partial oversight measure for this potential incompatibility is that if a governmental entity’s regulations, decisions, or measures or a public nongovernmental entity’s actions infringe a natural or legal person’s privacy and data protection rights, such person has legal standing to hold the governmental or public nongovernmental entities accountable, according to article 12 of the Law on the Organization and Procedure of the Court of Administrative Justice.<sup>17</sup> However, the same statute exempts regulations, decisions, or other measures of a number of indicated entities, which all act in political or judicial capacities, including the Supreme National Security Council. According to some of the available legal interpretations, the reason for this exception is

---

<sup>13</sup> Charter on Citizens Rights of Nov. 2016, arts. 36–40.

<sup>14</sup> *Necessity of Passing Draft Bill on Protection of Data and Privacy in Cyberspace*, Islamic Republic News Agency (Feb. 12, 2020), <https://perma.cc/9A9H-SDEV>.

<sup>15</sup> Draft of the Bill on the Protection of Data and Privacy in Cyberspace arts. 1–2, 4–8, 12, 14, 19, 26, 27, 67, 68.

<sup>16</sup> Cybercrime Act arts. 1, 2, 5, 25, 32, 34, 38, 39, 48, <https://perma.cc/723P-9WNU>.

<sup>17</sup> Enacted pursuant to article 173 of the Constitution, <https://perma.cc/JN9G-4QUV>, <https://perma.cc/3CGR-CNRF> (English translation).

that the regulations, decisions, or measures by the political or judicial entities are not subject to legal action, and the same principle would apply to their sub-entities.<sup>18</sup>

### III. Electronic Measures to Fight COVID-19 Spread

Iran has not adopted any laws, regulations or other public measures<sup>19</sup> that would allow the use of unauthorized or mandatory electronic means to assess general adherence to confinement measures to fight COVID-19 spread. However, it has created a few COVID-19-dedicated applications, websites, and phone services for self-assessments and tracking the spread of the coronavirus. The following apps and websites are operating based on the decisions, support, or authorization of the National Headquarters for Combating Corona;<sup>20</sup> the Ministry of Health and Medical Education, which leads the National Headquarters for Combating Corona; and the Ministry of Information and Communication Technology (ICT).

---

<sup>18</sup> *Analysis of the Plausibility of Judicial Oversight of the National Headquarters for Combating Corona*, supra note 10.

<sup>19</sup> It is notable that pursuant to the Decree of the Supreme Administrative Council Concerning the Charter on Citizens' Rights in the Administrative Systems, the government must be fully transparent regarding decisions and measures that would impact people's rights or benefits; however, again, this law is only applicable to administrative systems and is silent regarding governmental entities such as the Supreme National Security Council and its sub-councils that are acting in a political capacity. Decree of the Supreme Administrative Council Concerning the Charter on Citizens' Rights in the Administrative Systems art. 1, § 4, Official Gazette of the Islamic Republic of Iran, Apr. 10, 2017, No. 20995, <https://perma.cc/HYLA-ST89>.

<sup>20</sup> Reportedly, beginning on February 26, 2020, public sessions of the Parliament were indefinitely terminated (but resumed after 44 days) on the orders of the National Headquarters for Combating Corona, which had been established on February 22, 2020, by an act of the Supreme National Security Council, with the invested authority to create, coordinate, and enforce relevant national guidelines, and utilize national resources to stop the spread of COVID-19. Because the National Headquarters for Combating Corona is a sub-entity of the Supreme National Security Council, its decisions are equivalent to those of its founding Council and, as such, are deemed valid laws. Depending on the circumstances, those decisions can supersede laws passed by the Parliament. The Head of the staff of the National Headquarters is the Minister of Health and Medical Education. Other members are the Deputy Minister of Health and Medical Education; Spokesperson of the Ministry of Health; Minister of the Interior; Minister of Roads and Urban Development; Minister of Education; Minister of Science, Research and Technology; Minister of Cultural Heritage, Tourism and Handicrafts; Minister of Culture and Islamic Guidance; Chief of the General Staff of the Armed Forces; Attorney General; Head of the Management and Planning Organization; Director General of the Islamic Republic of Iran Broadcasting (IRIB); Head of Iran's Hajj and Pilgrimage Organization; government's Spokesperson; and Iran's Chief of Police. *Who Closed Parliament?*, Hamshahri Online (Apr. 8, 2020), <https://perma.cc/77EJ-JYWD>; *Resumption of Parliament's Public Sessions Awaiting Permission from National Headquarters for Combating Corona*, Tabnak World (Apr. 2, 2020), <https://perma.cc/7L9W-3NZR>; *First Open Session of Parliament after Closure*, Tasnim News (Apr. 7, 2020), <https://perma.cc/SYP8-PXDE>; *How Did First Sessions of Parliament Go?*, Islamic Republic News Agency (Apr. 9, 2020), <https://perma.cc/P68E-DULS>; *Decisions of the National Headquarters for Combating Corona Are as Enforceable for All Governmental Agencies as Decisions of the Supreme National Security Council*, Office of the Government Cabinet (Mar. 11, 2020), <https://perma.cc/K5GY-3XG7>; *National Headquarters for Combating Corona Meeting Convened with Supreme Leader in Attendance*, Islamic Republic News Agency (Sept. 3, 2020), <https://perma.cc/WW5K-9EGJ>; Mehdi Moghadasi & Ehsan Akbari, *Legal Importance of the Decisions of the Supreme National Security Council: Abstract*, 47(4) Pub. L. Stud. (Winter 2017), <https://perma.cc/7D8W-AM5L>.

## A. COVID-19 Dedicated Apps and Websites

### 1. The AC19 App

On or around March 3, 2020, the Iranian Ministry of Health and Medical Education reportedly sent a text message to all cell phones across the country, encouraging people to download the AC19\_app (a.k.a. “the Application for Combating Coronavirus” or “the Application Against Coronavirus”). The app allows users to access a COVID-19 self-assessment test, suggesting that it would be a reasonable measure for people with mild symptoms to stay in self-quarantine and to receive an assessment/medical assistance through the application, instead of heading to the hospitals. AC19 is an Android application<sup>21</sup> that is currently available in Café Bazaar, an Iranian website for downloading apps, movies, games, etc., as well as on the AC19 website.<sup>22</sup> The AC19 app was created by the Tehran Headquarters for Combating Corona, the Ministry of Health and Medical Education, and the ICT.<sup>23</sup>

This app reportedly prompts users to provide permission to access their Android devices’ location, and requests personal information such as the users’ phone numbers, names, and addresses. It also asks questions regarding their COVID-19 medical symptoms and those of their family members and social contacts, as well as information concerning age, gender, weight, etc. The AC19 app has caused contention and mistrust for many users and reporters, for several reasons:

- The prompt for accessing the user’s location data is from Android and not the Iranian application developers, hence, it is in English unless the users have changed their Android’s settings to Farsi.
- Users of older Android phones do not receive any prompts at all.
- According to information published by a London-based security researcher, who downloaded the application and evaluated its programming, it is collecting location data—coarse location (WiFi and mobile-based), fine location (GPS-based), latitude, and longitude—with a precision of less than three meters, as well as the live movements of the devices, such as with fitness apps.<sup>24</sup>

---

<sup>21</sup> According to Statcounter Global Status, over 88% of the Iran’s cell phone subscribers are using Android. *Mobile Operating System Market Share (Iran)*, Statcounter Global Status (May 22, 2020), <https://perma.cc/F5NB-GX3W> (in English).

<sup>22</sup> *Application for Combating Corona*, Café Bazaar (May 22, 2020), <https://perma.cc/4GZ3-8VYH>; AC19 Official Coronavirus Daily Reports and Registration Page (website), *supra* note 1.

<sup>23</sup> *Downloading AC19 Application for Corona*, Iranian Labor News Agency (Mar. 16, 2020), <https://perma.cc/6NX8-K46V>; *Application for Combating Corona Released*, Peivast Monthly News (Mar. 4, 2020), <https://perma.cc/2MQU-JPLK>.

<sup>24</sup> David Gilbert, *Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People*, Vice News (Mar. 14, 2020), <https://perma.cc/X7WE-AFAC> (in English); Zak Doffman, *Coronavirus Spy Apps: Israel Joins Iran and China Tracking Citizens’ Smartphones to Fight COVID-19*, Forbes (Mar. 14, 2020), <https://perma.cc/P6L6-LMNZ> (in English); Nariman Gharib, *Ministries of Health and Information Communication Technology Spying on People*, Telegraph (Mar. 6, 2020), <https://perma.cc/4MJB-HQ2Q>.

The Islamic Republic News Agency (IRNA), published a response to the foregoing controversy, stating that AC19 is not a spyware/malware, based on the results of the ZDNet/ESET technical and security evaluations of the application, and indicating that such location data collections are a common practice for many widely used applications.<sup>25</sup>

## 2. *The Salamat Website*

Following the contentious reactions to the AC19 app, the Ministry of Health and Medical Education published a guideline for the general public and developers of COVID-19 apps and websites, indicating that all developers must comply with the guidelines of the National Headquarters for Combating Corona; must register with Ministry of Health and Medical Education prior to operating; and must not obtain any personally identifiable information from the users, such as the National Identification Codes or phone numbers, but must instead, direct the users whose assessments show a higher probability of infection to the Salamat.gov.ir website<sup>26</sup> for a unified medical response and registration.

In the same guideline, the Ministry of Health asked people to register with the Salamat.gov.ir website for self-assessment and medical measures, and stated that a list of authorized COVID-19 apps and websites will be shortly available for the public.<sup>27</sup> In order to do the self-assessment test on the Salamat website the users will have to enter their National Identity Codes and dates of birth, and answer questions regarding their COVID-19 medical symptoms and those of their family members and social contacts. If the assessment shows a high risk of infection, the user will be instructed regarding the closest hospitals and health centers, and a health provider will contact the user through a dedicated (4030) phone number.<sup>28</sup>

## 3. *The Mask App and Website*

Mask is a movement-tracing app that was built for the Ministry of Health and Medical Education by a group of volunteer technical experts from Sharif, Amirkabir, and Shahid Beheshti Universities. It is available on the Mask.ir website<sup>29</sup> and through Café Bazaar. The app's website educates users regarding the developers, goals, and scope of the app's access to user data. It provides an infection-risk map that is based on aggregated data obtained from the Ministry of Health and Medical Education and a live contact/infection-risk notification service. In order to view the map, users do not have to provide personal information. However, to use the self-assessment test, infection-risk notifications, etc., users must register by entering their phone number and authorizing access to their device's location data. The website states that Mask is

---

<sup>25</sup> *Is the Application to Combat Corona Malware?*, Islamic Republic News Agency (Mar. 4, 2020), <https://perma.cc/Y597-S5X9>; Catalin Cimpanu, *Spying Concerns Raised Over Iran's Official COVID-19 Detection App*, ZDNet (Mar. 9, 2020), <https://perma.cc/Z6NV-FCC9> (in English).

<sup>26</sup> <http://www.salamat.gov.ir>.

<sup>27</sup> *Draft Guidelines for Recognition and Introduction of [Legitimate] Websites*, IRIB News (Mar. 10, 2020), <https://perma.cc/XQZ4-KRHM>.

<sup>28</sup> *Necessity of People Joining Salamat Assessment Website to Combat Corona*, Iranian Students News Agency (Apr. 11, 2020), <https://perma.cc/FQ7K-ENJF>.

<sup>29</sup> <https://www.mask.ir/>.

trying to obtain from the Ministry of Health and Medical Education a list of phone numbers of those individuals who have been in close contact with confirmed cases within the last two weeks in order to notify them. It adds that their live contact/infection-risk notification service is merely based on the information that users have provided voluntarily, using anonymization, location tracing, Bluetooth, GPS, QR Code, etc.<sup>30</sup>

#### 4. Website for Coronavirus Self-Assessment, Information, and Registration

The website for coronavirus self-assessment, information, and registration was created with the support of the Deputy of Research and Technology of the Ministry of Health and Medical Education. It contains COVID-19-related educational information, an infection-risk map, and several self-assessment tests, one of which requires the user's phone number.<sup>31</sup>

### B. Oversight Measures

Iran is reportedly in the process of considering reform bills that would implement oversight measures concerning cyberspace violations.<sup>32</sup> Meanwhile, currently,

- if a natural or legal person believes that a government employee has violated his or her privacy or data protection rights, that person has standing to pursue legal action against the government employee, according to the Cyber Crime Act and other subject-matter-specific laws and regulations;<sup>33</sup> and
- if the violator is a governmental entity or a nongovernmental public entity that is acting in an administrative or executive capacity, persons with standing may file legal actions against such entities, according to article 12 of the Law on the Organization and Procedure of the Court of Administrative Justice, which was enacted pursuant to article 173 of the Constitution.<sup>34</sup>

Aside from the aforementioned legal measures, the Maher Center<sup>35</sup> is responsible for receiving cyberspace complaints, confidentially informing the subject persons of their compromised private data, and notifying the highest authority of the violating governmental entity of the

---

<sup>30</sup> *Questions and Answers*, Mask.ir (May 22, 2020), <https://perma.cc/JX36-SB4R>.

<sup>31</sup> Coronavirus Information, Self-Assessment and Registration (website), <https://perma.cc/6S79-E2VJ>.

<sup>32</sup> *Maher's Statement Regarding Unauthorized Disclosure of Some Legal Persons in Cyberspace*, Information Technology Organization (Apr. 26, 2020), <https://ito.gov.ir/fa/news/104852/-بیااینه-مرکز-ماهر-در-رابطه-با-روند-افشاء-داده‌های-سازمان-هاو-کسب‌وکار-ها-در-فضای-مجازی>. For more on the Maher Center, see footnote 35, *infra*.

<sup>33</sup> Cybercrime Act art. 5, <https://perma.cc/723P-9WNU>.

<sup>34</sup> Constitution of the Islamic Republic of Iran art. 173, <https://perma.cc/JN9G-4QUV>, <https://perma.cc/3CGR-CNRF> (English translation); Law on the Organization and Procedure of the Court of Administrative Justice art. 12, <https://perma.cc/F9VW-CHVV>.

<sup>35</sup> The Maher Center is a part of the Information Technology Organization and, as such, a part of the Ministry of Information and Communication Technology. Maher has various subdivisions and governmental and private partners that collectively act as a national information technology Computer Emergency Response Team (CERT). *History of the Organization – Information Technology Organization in One Look*, Information Technology Organization (Sept. 18, 2019), <https://perma.cc/L8TR-ENE5>; *Maher's Statement Regarding Unauthorized Disclosure of Some Legal Persons in Cyberspace*, *supra* note 32.

complaints about that entity.<sup>36</sup> Concurrently, the Afta Strategic Management Center of the Office of the President, acting under the Cyberspace Council of the Supreme National Security Council (an SNSC sub-council), was created to act in conjunction with the Maher Center to coordinate the efforts of the three branches of government, their divisions, and nongovernmental public entities in creating a unified response to cyberspace violations.<sup>37</sup>

---

<sup>36</sup> *The National System for the Prevention and Defense against Cyberspace Incidents Was Approved*, Presidential News Center (Nov. 6, 2017), <https://perma.cc/8HLE-LVN4>; *Maher's Statement Regarding Unauthorized Disclosure of Some Legal Persons in Cyberspace*, Information Technology Organization (Apr. 26, 2020), <https://ito.gov.ir/fa/news/104852/> بیانیه-مرکز-ماهر-در-رابطه-با-روند-افشاء-داده‌های-سازمان-هاو-کسب‌وکار-ها-در-فضای-مجازی. See also *Maher's Statement Regarding Unauthorized Disclosure of Some Legal Persons in Cyberspace*, note 32, *supra*.

<sup>37</sup> *About, Afta* (website), <https://perma.cc/VH4L-Z8MT>.

# Israel

*Ruth Levush*  
*Senior Foreign Law Specialist*

**SUMMARY** The Israeli government has used electronic means to fight the COVID-19 pandemic since March 2020. These include both voluntary and non-voluntary digital tracing to stop the chain of infection.

From March to May 2020 the government utilized the robust surveillance technologies of the Israel Security Agency (ISA) to trace patients and those with whom they came into contact. The ISA authorization has been scrutinized by the Supreme Court, which held that its scope and duration must be regulated by law. Following the Court's ruling the government prepared draft legislation. In response to public criticism and concerns expressed by the ISA Chief, however, the government announced on June 8, 2020, that it would not utilize the ISA abilities to trace COVID-19 patients and would not promote the legislation at this time.

The Ministry of Health offers a voluntary app, HaMagen, which is currently installed on the devices of only a small percentage of the population. The Ministry is working on improving the accuracy of the app and on increasing the number of users.

The use of tracing devices raises challenges to the right to privacy and to patients' rights, which are protected under Israel's basic laws, statutes, and regulations. Although not specifically required by law, the ability to utilize "privacy by design" was held by the Tel Aviv District Court to be a way to limit the harm to privacy associated with digital surveillance.

## I. Introduction

Israel appears to have had relative success in curtailing the spread of the novel coronavirus pandemic. The country has a population of over nine million.<sup>1</sup> As of May 22, 2020, 531,124 tests for COVID-19 had been conducted; 16,690 patients had been diagnosed with COVID-19; 13,915 had recovered; and 279 had died.<sup>2</sup> Due to the low infection rate, the government has been gradually easing social distancing requirements and the economy continues to open under conditions posted on the Ministry of Health (MOH) website.<sup>3</sup>

Cell phones are widely used in Israel. As of 2020, the number of mobile phone internet users in Israel reached about 6.5 million.<sup>4</sup> As discussed below, the number of Israelis uploading a

---

<sup>1</sup> *Population*, Central Bureau of Statistics (last updated Mar. 2020), <https://perma.cc/49AN-MSE7>.

<sup>2</sup> *Coronavirus*, Ministry of Health (May 22, 2020), <https://perma.cc/8W93-VPJX> (in Hebrew).

<sup>3</sup> *Corona Outbreak, Latest Updates*, Davidson Institute, Weizmann Institute of Science (updated May 20, 2020), <https://perma.cc/44HX-JPVU> (in Hebrew).

<sup>4</sup> *Number of mobile phone internet users in Israel from 2015 to 2023*, Statista, <https://perma.cc/PV5G-DFDF>.

voluntary app for COVID-19 tracing reflects the willingness of a significant, though insufficient, portion of the population to share personal data in relation to the pandemic. Improvement of the app's features is expected to increase the number of users.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

#### 1. *Constitutional and Legislative Guarantees*

Basic Law: Human Dignity and Liberty recognizes that “[a]ll persons have the right to privacy and to intimacy . . . [and that] there shall be no violation of the confidentiality of conversation, or of the writings or records of a person.”<sup>6</sup> The constitutional right to privacy, however, is qualified by a “limitation clause” in section 8 of the Basic Law, which requires that any law that limits the rights set out in the Basic Law, including the protected right to privacy, must “[comport with the] values of the State of Israel, [be] enacted for a proper purpose, and to an extent no greater than is required.”<sup>7</sup>

Personal and medical privacy are protected by a number of statutory laws and regulations, including the Privacy Protection Law, 5741-1981 (PPL);<sup>8</sup> the Secret Monitoring Law, 5739-1979 (SML);<sup>9</sup> and the Patient's Rights Law, 5756-1996 (PRL),<sup>10</sup> as well as by court rulings.

#### 2. *Consent for Disclosure*

The PPL prohibits the violation of a person's privacy without his or her consent. The PPL considers the “breach of the duty of confidentiality provided by law regarding a person's private affairs” as a violation of privacy.<sup>11</sup>

---

<sup>5</sup> See “HaMagen Voluntary COVID-19 Tracing App,” Part III(B), below.

<sup>6</sup> Basic Law: Human Dignity and Liberty § 7(d), Sefer Hahukim [SH] No. 1391, 5752 (Mar. 25, 1992), this and all citations below as amended, <https://perma.cc/CTP5-RQMD> (unofficial English translation). Israel does not have a written constitution contained in one document. Based on the 1951 Harari Knesset (Israel's Parliament) Resolution, Israel's Basic Laws were intended to form chapters in its future constitution. *The Constitution*, Knesset, <https://perma.cc/N5X7-KQVY>. Basic Law: Human Dignity and Liberty and Basic Law: Freedom of Occupation, SH No. 1454 p. 90 (Mar. 10, 1994), <https://perma.cc/EVN6-8NRA> (unofficial English translation), however, contain provisions that have been interpreted by the Supreme Court as providing the Court with the authority to repeal statutory legislation that conflicts with the Laws' provisions.

<sup>7</sup> Basic Law: Human Dignity and Liberty § 8.

<sup>8</sup> PPL, SH 5741 No. 1011 p. 128.

<sup>9</sup> SML, SH No. 938 p. 118.

<sup>10</sup> PRL, SH 5756 No. 1591 p. 327.

<sup>11</sup> PPL §§ 1 & 2(7) (all translations by author).

Subject to specified exceptions, a duty of confidentiality is imposed on medical care providers and institutions regarding patients' medical information that has been obtained in the course of treatment.<sup>12</sup>

Disclosure of a patient's private information is authorized under the following conditions:

- (1) The patient consented to the delivery of the medical information;
- (2) The caregiver or the medical institution is required by law to provide the medical information;
- (3) The delivery of medical information is to another caregiver for the purpose of treating the patient;
- (4) Medical information has not been disclosed to the patient under section 18(c) [applicable when the caregiver has determined that the information could cause serious harm to the patient's physical or mental health or endanger patient's life] and the Ethics Committee approved its delivery to another;
- (5) The Ethics Committee, after giving the patient the opportunity to make his or her arguments, determined that the provision of medical information about him or her was essential for the protection of the health of others or the public and that the need for its delivery was superior to the interest in its non-delivery;
- (6) The delivery of medical information is to the treating medical institution or employee of that medical institution for the purpose of processing, filing, or reporting the information [as required] by law;
- (7) The delivery of the medical information is intended for publication in a scientific journal, for research or teaching purposes in accordance with instructions prescribed by the Minister [of Health, provided that no identifying details of the patient were disclosed].<sup>13</sup>

### 3. *Handling of Sensitive Information*

The storage and sharing of sensitive data in databanks, including data on an individual's personality, health, financial status, opinions, or beliefs, is regulated under the PPL and the Privacy Protection (Data Security) (ISA) Regulations, 5777-2017 (PPDS).<sup>14</sup> The PPDS requirements for data protection by databank controllers and processors apply to both the public and private sectors.<sup>15</sup> Sensitive information related to health requires either mid- or high-level security protection when preserved in a databank.<sup>16</sup>

---

<sup>12</sup> PRL § 20(b).

<sup>13</sup> Id. § 20(a)(1), (2) & (5).

<sup>14</sup> PPL ch. B; PPDS, Kovetz Hatakanot [Kt] [Subsidiary Legislation] 5777 No. 7809 p. 1022, <https://perma.cc/6UH6-KD6B>. For a summary of the regulations see Ruth Levush, *Israel: Online Privacy Protection Regulations Adopted*, Global Legal Monitor (June 14, 2017), <https://perma.cc/QCU8-TJS3>.

<sup>15</sup> Omer Tene, *Israel Enacts Landmark Data Security, Notification Regulations*, International Association of Privacy Professionals (IAPP) (Mar. 22, 2017), <https://perma.cc/WX3H-4488>.

<sup>16</sup> See discussion of the PPDS in Part II(B), below.

## B. Data Retention and Location Tracking

### 1. *Data Retention of Health Records*

The PPDS requires mid-level security for databases that are owned by a public body or that are principally intended “to collect data for delivery to another entity,”<sup>17</sup> and that generally includes sensitive information, such as medical, genetic, or biometric information.<sup>18</sup> Databases that would otherwise require mid-level security but include information on more than 100,000 people or are accessible by more than 100 persons, would generally require high-level security.<sup>19</sup>

### 2. *Telecommunications*

Databank owners may not connect databank systems to the internet or to any other public system without installing proper protection against unauthorized penetration of the system or against software capable of causing damage to hardware or other software. Moreover, the transfer of information from a databank on a public system or the internet must utilize common encryption methods. The identity of the user and his or her grant of permission to use the databank will be verified. Access to databanks at mid- and high-levels of security must be provided through a means that is subject to the exclusive control of the access permit holder.<sup>20</sup>

### 3. *Storing and Sharing of Location Data*

A decision rendered by Tel Aviv District Court Judge Agmon-Gonen on July 1, 2019, addressed the danger to privacy that may result from utilizing cross identification enabled by access to big data. The case involved the unauthorized disclosure of personal location data resulting from a requirement that caregivers of Israel Defense Force (IDF) disabled veterans report their work by mobile signature at the beginning and end of their shifts.<sup>21</sup>

Agmon-Gonen determined that the violation of privacy to the caregivers resulting from the requirement did not exceed what was required under the circumstances.<sup>22</sup> It did result, however, in a violation of the right to privacy of the disabled veterans because the care provided might include taking or staying with the disabled veterans outside of their home—for example, when the disabled veteran needed a short psychiatric hospital stay. The use of location data, she held, might “reveal data, such as health information, found in the core of the right to privacy [and]

---

<sup>17</sup> PPDS § 1, KT 5777 No. 7809 p. 1022, <https://perma.cc/6UH6-KD6B>.

<sup>18</sup> *Id.*, App. 1. For specific procedures see Ruth Levush, *Israel*, in *Online Privacy Law (2017 Update)* 17 (Law Library of Congress, Dec. 2017), <https://perma.cc/XN5R-FU2S>.

<sup>19</sup> PPDS, App. 2.

<sup>20</sup> *Id.* § 14.

<sup>21</sup> Adm. TA 28857-06-17 *Disabled Veterans Association v. Ministry of Defense* (decision by Judge Michal Agmon-Gonen), <https://perma.cc/C3RM-DNAA> (in Hebrew).

<sup>22</sup> *Id.* para. 16.6A.

expose location data [which] constituted unlawful harm to the privacy of the disabled [veterans].”<sup>23</sup>

She further concluded that the technology of “privacy by design” could enable caregiver reporting without harming the right to privacy. A tender for selecting a company that would monitor the IDF’s employment of veterans’ caregivers, therefore, should have required that bidding companies would use mobile signature software incorporating principles of “privacy by design” to limit the infringement of the veterans’ right of privacy. For example, a cellular signature could be required at the start and end of the caregiver shift, when the caregiver is with the disabled veterans for the whole shift, without keeping location data.<sup>24</sup> As this has not been done, Judge Agmon-Gonen concluded that

[i]t was impossible to say that the least harmful means was chosen. Therefore, it should be determined, and also anchored in the tender with the monitoring company, that a cellular signature be made so that it does not reveal the location of the disabled, and be designed so that their privacy is not harmed beyond what is required.<sup>25</sup>

### III. Electronic Measures to Fight COVID-19 Spread

In an effort to stop the spread of the virus the MOH has offered a voluntary app called HaMagen to trace COVID-19 patients and those with whom they have been in contact. HaMagen is currently installed on the devices of 1.5 million Israelis, constituting only a small percentage of the population.<sup>26</sup>

In addition, the government has authorized the Israel Security Agency (ISA),<sup>27</sup> which normally handles threats to national security, to conduct surveillance on Israeli citizens and residents in order to stop the spread of the virus. A legislative framework defining the ISA’s surveillance scope and duration is currently being considered by the Knesset (Israel’s parliament) following a decision rendered by the Supreme Court on April 26, 2020, requiring anchoring the ISA authorization in legislation rather than in government decisions.<sup>28</sup>

---

<sup>23</sup> Id. para. 16.6B.

<sup>24</sup> Id. para 16.8.

<sup>25</sup> Id.

<sup>26</sup> Sagi Cohen, *Ministry of Health in Contacts to Connect the HaMagen App to Apple and Google’s Corona Venture*, The Marker (May 4, 2020), <https://perma.cc/F9VF-9WSE> (in Hebrew).

<sup>27</sup> “*The Unseen Shield*”, Israel Security Agency, <https://perma.cc/D8KH-JFZZ>.

<sup>28</sup> HC 2109/20 Ben Meir v. Prime Minister, Israeli Judicial Authority, <https://perma.cc/P999-T2X7>. For analysis of the decision see Ruth Levush, *Israel Security Agency’s Involvement in COVID-19 Tracing Scrutinized*, In Custodia Legis (Law Library of Congress, May 7, 2020), <https://perma.cc/R9QW-W38P>.

## A. Electronic Surveillance by Israel Security Agency

### 1. *Legal Basis*

On March 17, 2020, the Israeli government issued the Emergency Regulations (Authorization of the Israel Security Service to Assist the National Effort to Reduce the Spread of the Novel Coronavirus), 5780-2020.<sup>29</sup> The Emergency Regulations were in effect for a period of 14 days and then replaced by Government Decision No. 4916, on March 24, 2020,<sup>30</sup> and by Government Decision No. 4950, on March 31, 2020, extending surveillance authorities to April 30, 2020.<sup>31</sup> The government expressed interest in further extending the ISA's authorization, especially when social distancing and other restrictions were being lifted.<sup>32</sup>

Government Decision No. 4950 was issued pursuant to section 7(b)(6) of the ISA Law, 5762-2002, which authorizes the ISA to engage in activities other than those enumerated by the Law, as determined by the government, with the approval of the Knesset (Israel's parliament) Committee on the ISA, to be necessary to protect and promote essential national security interests.<sup>33</sup>

### 2. *Scope of Surveillance*

In accordance with Government Decision No. 4950, the ISA was authorized

- (a) . . . to receive, collect and process technological information to assist the Ministry of Health in conducting an examination regarding the period of 14 days prior to a patient's diagnosis, for identifying location data and movement paths of a patient and for identification of persons who came into contact with him, to identify the source of the patient's virus infection and who might be infected by him . . . .
- (b) [and to] . . . transmit necessary information details to the Ministry of Health . . . so that the Ministry of Health can give guidance to patients, people who have come into close contact with them and the general public.<sup>34</sup>

The decision defines "technological information" as

[t]elecommunication data of . . . identification, location and communication, excluding content of conversations within the meaning of the wiretapping law, 5739-1979, as approved by the Knesset Service [ISA] Committee.<sup>35</sup>

---

<sup>29</sup> Emergency Regulations (Authorization of the General Security Service to Assist the National Effort to Reduce the Spread of the Novel Coronavirus), 5780-2020, KT 5780 No. 8393 p. 782, <https://perma.cc/UJ92-HGSK>.

<sup>30</sup> Government Decision No. 4916 (Mar. 24, 2020), <https://perma.cc/BX22-U99R>.

<sup>31</sup> Government Decision No. 4950 (Mar. 31, 2020), <https://perma.cc/U4T2-G8HT>

<sup>32</sup> For government decisions on reopening as of May 14, 2020, see Press Release, Ministry of Health, New Resolutions Regarding Re-Opening (Mar. 14, 2020), <https://perma.cc/5JA2-RLEY>.

<sup>33</sup> ISA Law, 5762-2002, SH 5762 No. 1832 p. 179, as amended, <https://perma.cc/E2TJ-DLEY>.

<sup>34</sup> Decision No. 4950 § 2.

<sup>35</sup> Id. § 3.

It defines “necessary information” details as follows:

- (1) For a patient: Location data and traffic routes in the period of 14 days before the day of diagnosis.
- (2) For persons who have come into contact with a patient: a full name, identity card number, telephone number, date of birth, date, time and location of last exposure to the patient, . . . to the extent possible and necessary.<sup>36</sup>

### 3. *Legitimacy of ISA Authorization to Conduct Surveillance on Patients and Contacts*

The validity of the ISA’s authority to conduct surveillance in the context of the pandemic was reviewed by the Supreme Court. In a unanimous decision rendered on April 26, 2020, the Court held that the ISA authorization could not be based on government decisions. Instead, that authorization had to be anchored in legislation.<sup>37</sup>

On May 5, 2020, the Knesset Intelligence Subcommittee approved a three-week extension of the government’s use of ISA surveillance assistance to fight the COVID-19 pandemic. The extension was granted to enable advancement of the legislative process.<sup>38</sup>

In response to public criticism, on June 8, 2020, the government decided to stop utilizing ISA surveillance for COVID-19 tracing and put on hold legislative efforts for securing its statutory authorization. According to Israeli media, draft legislation providing such authorization in this regard would be authorized by the Ministerial Legislative Committee, but not be submitted for Knesset approval at this time. Expressing his “discomfort” in the ISA usage of its electronic technologies for purposes of monitoring patients, ISA Chief Nadav Argman has reportedly stated that, “if the [pandemic] outbreak was renewed, the law could be quickly enacted, and the ‘ISA would be prepared.’ ” He offered ISA assistance in the improvement of a voluntary app.<sup>39</sup>

## **B. HaMagen Voluntary COVID-19 Tracing App**

As compared with the robust technological surveillance abilities of the ISA, the HaMagen app provides more limited and a less accurate level of monitoring patients and their contacts. The HaMagen may be uploaded on a voluntary basis. It was launched by the MOH in March 2020 with the objective of stopping the chain of COVID-19 infection.<sup>40</sup>

---

<sup>36</sup> Id.

<sup>37</sup> HC 2109/20 Ben Meir v. Prime Minister, <https://perma.cc/P999-T2X7>; Levush, *supra* note 28.

<sup>38</sup> *The Intelligence Subcommittee Has Approved a 3-week Extension to the Use of the ISA’s Tool to Combat Corona – In Order to Facilitate Legislative Process*, Foreign Affairs and Defense Committee (May 5, 2020), <https://perma.cc/KV62-TTAA> (in Hebrew).

<sup>39</sup> T. Tsimuki & I. Ichner, *ISA Tracing Will Be Stopped and the Law Halted, ISA Chief: Develop a Civilian App.*, YNET (June 8, 2020), <https://perma.cc/5RVE-FCY3>.

<sup>40</sup> Cohen, *supra* note 26.

### 1. *HaMagen System Characteristics*

The HaMagen app cross-checks the GPS history of any subscriber against historical geographic data of patients identified by the MOH. The app is available in five languages: Hebrew, Arabic, English, Russian, and Amharic.<sup>41</sup>

The app is free to download from the App Store and Google Play. It notifies subscribers if they “crossed paths with a COVID-19 patient,” provides the exact time and location of the contact, and allows them to “review, and confirm or reject the notification.”<sup>42</sup> Upon confirmation, the user will be asked go into isolation and report to the MOH. If the message in the notification is incorrect, the user “can reject it and carry on as normal.”<sup>43</sup>

Files shared by HaMagen are generated in the MOH’s epidemiological system, and contain

. . . only verified information that was received from laboratories and epidemiological investigations and is monitored by the Ministry of Health. Prior to sending, the file is digitally signed with the Ministry of Health’s digital signature. Upon receiving the file, the digital signature is examined by the application, to verify that the file was received from the Ministry of Health in an orderly manner, in order to prevent the breach of malware into the application.<sup>44</sup>

The MOH website contains a detailed privacy policy for the HaMagen app. With regard to information sharing, the policy states as follows:

- The Ministry of Health puts great emphasis on the information’s confidentiality and privacy. Accordingly, any information shared with the Ministry of Health will go through an encrypted channel and stored in the Ministry’s servers in accordance with all procedures and protocols on information security and protection of privacy applicable to the Israeli healthcare system, and in accordance with the law.
- The Ministry of Health runs routine maintenance checks of the measures ensuring information security and protection of privacy and updates them as needed.<sup>45</sup>

### 2. *Rate of Use and Accuracy*

According to the Ministry of Health, the HaMagen app is currently installed on the devices of 1.5 million Israelis, constituting only a small percentage of the population. Based on GPS location data, the app has been criticized as insufficiently accurate, “certainly not at the required two meters [approx. 6.56 feet]. The app knows if people were around each other, but not beyond that. Nor is it able to identify the location of people within buildings.”<sup>46</sup>

---

<sup>41</sup> *HaMagen*, MOH, <https://perma.cc/7CSC-8TMS>.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Privacy Policy*, para. 6, MOH (last updated May 14, 2020), <https://perma.cc/392C-6HBW>.

<sup>45</sup> *Id.* para. 9.

<sup>46</sup> Cohen, *supra* note 26.

The MOH is reportedly working on adding Bluetooth technology to the app, which will enable identification within buildings and improve accuracy. One commentator opined that

To be effective at curbing the epidemic when removing restrictions, the app needs to be installed with a much larger number of devices - including, as far as possible, in the Arab and ultra-Orthodox sectors. For example, according to a study in Oxford, in order for the Bluetooth-based contact detection app to stop the epidemic, about 60% of the population needs to install the app.

...The need to improve the accuracy of the protective app and dramatically increase its users' reach is important for two reasons: to stop the pandemic's spread in the coming months of the quarantine's opening; and to make the ISA's intrusive and controversial means of surveillance unnecessary.<sup>47</sup>

According to an op-ed by two Israeli experts in game theory and behavioral economics,

the inaccuracy of the HaMagen app alongside the use of mobile tracing tools whose sources of information are unknown to the public has resulted in the sending of numerous false alerts and inconsistent messages between the systems, causing many people to lose confidence in the app as a way to fight the corona epidemic.<sup>48</sup>

They argued that to counter resistance to their use, surveillance apps should incorporate carriers' risk assessment features while preserving the privacy of users. Risk assessment features, they opined, would be welcomed by the public as such features would save users' time and convey the users' commitment to fighting the virus.<sup>49</sup>

---

<sup>47</sup> Id.

<sup>48</sup> Ido Arev & Oren First, *I Am Open, Therefore I Am Safe*, Calcalist (May 20, 2020), <https://perma.cc/NYG7-JQQG> (in Hebrew).

<sup>49</sup> Id.

## South Africa

*Hanibal Goitom*  
*Chief, FCIL I*

**SUMMARY** As part of the effort to combat and mitigate the impact of the COVID-19 pandemic, South Africa established an interim database, the COVID-19 Tracing Database, within the Department of Health. All health care professionals who test a person for COVID-19 must report the person's identification and contact information, including cellphone number, for inclusion in the Database. All accommodation establishments must report similar information relating to anyone who uses their services during the national lockdown. The director-general of the Department is authorized to mandate electronic communications service providers to report to her the location and movements of persons known or suspected of having COVID-19 and anyone who is reasonably suspected to have come into contact with such persons. The director-general is not obligated to inform the persons whose location and movement is being tracked until after the end of the state of national disaster.

The authority of the director-general is subject to some restrictions and oversight. For instance, the director-general's authority to track location and movement of persons is limited to the period from March 5, 2020, through the end of the national state of disaster. Such information may only be obtained, used, or disclosed by authorized persons and only for the purpose of combatting the spread of COVID-19. All information in the Database must be de-identified (anonymized) or destroyed within six-weeks after the expiration of the national state of disaster and this process is subject to judicial and parliamentary oversight. Significantly, the collection or use of tracking information for a purpose other than combatting the spread of COVID-19, unauthorized disclosure of information in the Database, retention of such information beyond the period authorized by law, or failure to de-identify or destroy information as required by law is an offense punishable on conviction by a fine, custodial sentence, or both.

The collection, use, and disclosure of personal information in South Africa is governed under the 1996 Constitution, common law, and a number of statutes. One such law is the 2013 Protection of Personal Information Act. The Act imposes various conditions under which the lawful processing of personal information (including location information) may take place, including accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation, as further defined by statute. Although most parts of the Act have yet to take effect, a guidance note issued by the Information Regulator, an institution established under parts of the Act already in force, requires that processing of personal information done for the purpose of combatting COVID-19 must adhere to the conditions set under the Act.

## I. Introduction

As of May 22, South Africa had conducted 543,032 tests and registered 20,125 confirmed COVID-19 cases.<sup>1</sup> On the same day, South Africa recorded 988 new cases.<sup>2</sup> Of the persons infected, so far 10,104 have recovered and 397 have died.<sup>3</sup>

As part of its effort to combat the spread of COVID-19, South Africa has put in place measures leveraging technology (described in Part III, below), mainly using location and movement data to conduct contact tracing of infected persons and persons who have come into contact with infected persons. The level of permeation of mobile and smartphones in the country, whose population is estimated at about 56.5 million,<sup>4</sup> is important in this regard. As of 2018, mobile cellular subscriptions stood at around 92.5 million, representing about 167 subscriptions per 100 residents in the country.<sup>5</sup> According to the Independent Communications Authority of South Africa (ICASA), the official regulator of the South African communications, broadcasting and postal services sectors, smartphone penetration nearly doubled in a span of two years, from 43.5% in 2016 to 81.7% in 2018.<sup>6</sup> According to the same report, in 2018, South Africa had 65.8 million mobile cellular data subscriptions, a 12.3% increase since 2015, and about 12.6 million LTE device subscriptions.<sup>7</sup>

However, this information must be read in context. According to one source, “[t]he penetration rate likely reflects that many South Africans have more than one smartphone, while a significant portion of citizens are still reliant on basic or feature phones.”<sup>8</sup> According to a Pew Research Centre report, based on a spring 2017 survey, 51% South Africans owned smartphones that could access the internet and apps.<sup>9</sup>

---

<sup>1</sup> Press Release, Department of Health, Republic of South Africa, Update on Covid-19 (May 22, 2020), <https://perma.cc/5U6V-DKQF>.

<sup>2</sup> Id. Press Release, Department of Health, Republic of South Africa, Update on Covid-19 (21st May), <https://perma.cc/VFF5-R57X>.

<sup>3</sup> Press Release (May 22, 2020), *supra* note 1.

<sup>4</sup> *South Africa*, CIA World Factbook (last updated Mar. 16, 2020), <https://perma.cc/23UB-9MP6>.

<sup>5</sup> Id.

<sup>6</sup> Independent Communications Authority of South Africa, *The State of the ICT Sector Report in South Africa* 25-26 (Mar. 19, 2019), <https://perma.cc/2ZLR-N28P>.

<sup>7</sup> Id. at 31. LTE is “the latest generation of mobile technology. A step up from 3G technology, LTE offers faster network download and upload speeds.” *All about LTE: Everything You Need to Know about TE and Wireless Broadband*, Telekom, <https://perma.cc/A2ZK-L69Y>.

<sup>8</sup> Paula Gilbert, *SA Smartphone Penetration Now at over 80%, Says ICASA*, ITWeb (Apr. 3, 2019), <https://perma.cc/CGS8-4HMQ>.

<sup>9</sup> Laura Silver & Courtney Johnson, *Internet Connectivity Seen as Having Positive Impact on Life in Sub-Saharan Africa*, Pew Research Center (Oct. 9, 2018), <https://perma.cc/RFM3-LDJW>.

## II. Legal Framework

### A. Privacy and Data Protection

The collection, use, and disclosure of personal information in South Africa is governed under the 1996 Constitution, common law, and a number of statutes, including the Promotion of Access to Information Act, the Electronic Communications and Transactions Act, and the National Credit Act.<sup>10</sup> In 2013, South Africa enacted the Protection of Personal Information Act, which is considered a codification of privacy protections under the country's common law; however, most parts of the Act have yet to take effect.<sup>11</sup> Nevertheless, the Information Regulator (the Regulator), an entity established under the parts of the Act already in force, recently issued a guidance document requiring responsible parties to follow the requirements under the Act (see Part II(B)(1), below) and the Guidance when processing personal information. Other laws relevant to privacy issues include the Regulation of Interception of Communications and Provision of Communication-Related Information Act and the National Health Act. Relevant parts of these laws are discussed below.

#### 1. *The Constitution*

The right to privacy is guaranteed by the Bill of Rights chapter of the 1996 Constitution, which states that

- [e]veryone has the right to privacy, which includes the right not to have
- a. their person or home searched;
  - b. their property searched;
  - c. their possessions seized; or
  - d. the privacy of their communications infringed.<sup>12</sup>

Limitations may be imposed on the right to privacy, but “only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.”<sup>13</sup> Among the factors that must be considered when imposing a limitation are the importance of the purpose for which the limitation is proposed, the nature and extent of the proposed limitation, the relationship between the proposed limitation and its purpose, and the least restrictive means of achieving the purpose.<sup>14</sup>

---

<sup>10</sup> Adrian Naude, Data Protection in South Africa: The Impact of Protection of Personal Information Act and Recent International Developments (unpublished LLM Thesis, University of Pretoria) (Dec. 2014), <https://perma.cc/S5LP-WEPC>.

<sup>11</sup> *Data Protection Laws of the World: South Africa*, DLA Piper (last modified Jan. 27, 2020), <https://perma.cc/AA99-5Q72>.

<sup>12</sup> South Afr. Const., 1996, § 14, <https://perma.cc/K5MU-5LLH>

<sup>13</sup> *Id.* § 36.

<sup>14</sup> *Id.*

## 2. *Protection of Personal Information Act*

The Protection of Personal Information Act (POPIA) permits the processing of personal information in certain circumstances. It defines “personal information” as “information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including but not limited to . . . any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.”<sup>15</sup> The term “processing” includes “the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use” of personal information.<sup>16</sup>

POPIA puts in place general conditions under which the lawful processing of personal information may take place, including accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation, as further defined by statute.<sup>17</sup> As noted above, the term “personal information” includes location information. The “purpose specification” clause of POPIA requires that the collection of personal information be limited to “a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.”<sup>18</sup> It also requires that further processing of personal information be compatible with the purpose of collection.<sup>19</sup> Significantly, it provides that further processing of personal information is considered compatible with the purpose of collection if “it is necessary to prevent or mitigate a serious and imminent threat to– (i) public health or public safety; or (ii) the life or health of the data subject or another individual.”<sup>20</sup>

POPIA bars the processing of special information<sup>21</sup> except in certain limited instances, including when the data subject consents or it is “necessary for the establishment, exercise or defence of a

---

<sup>15</sup> Protection of Personal Information Act No. 4 of 2003 (POPIA) § 1 (Nov. 19, 2013), <https://perma.cc/ZN2A-PFBN>. Once implemented, POPIA will introduce the same definition of the term “personal information” to the Promotion of Access to Information Act No. 2 of 2000 (PAIA), § 1 (Feb. 2, 2000), <https://perma.cc/56Z5-PWH3>, and the Electronic Communications and Transactions Act No. 25 of 2002 (ECTA), § 1 (July 31, 2002), <https://perma.cc/A5TF-3MU9>. POPIA § 110.

<sup>16</sup> POPIA § 1.

<sup>17</sup> Id. § 4.

<sup>18</sup> Id. § 13.

<sup>19</sup> Id. § 15.

<sup>20</sup> Id. § 15(d).

<sup>21</sup> Id. § 26. This is information relating to

- the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
- the criminal behaviour of a data subject to the extent that such information relates to—
- the alleged commission by a data subject of any offence; or
- any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings. Id.

right or obligation in law.”<sup>22</sup> In this situation, additional conditions relating to the specific information in question apply.<sup>23</sup>

As noted above, POPIA makes putting in place security safeguards one of the conditions for processing personal information. The Act states that “[a] responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent– (a) loss of, damage to or unauthorized destruction of personal information; and (b) unlawful access to or processing of personal information.”<sup>24</sup> In order to effectively meet this requirement, the party must take reasonable steps to

- (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- (b) establish and maintain appropriate safeguards against the risks identified;
- (c) regularly verify that the safeguards are effectively implemented; and
- (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.<sup>25</sup>

POPIA does not apply to instances of processing of personal information by or for a public body involving “national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety.”<sup>26</sup> Nevertheless, as noted above, the Regulator’s recent Guidance (see Part II(B)(1), below) requires that responsible parties, including relevant government entities, adhere to rules under the Act when processing personal information of data subjects as part of the effort to curb COVID-19.

### 3. *Electronic Communications and Transactions Act*

Application of the Electronic Communications and Transactions Act (ECTA) is limited to instances in which personal information is collected through electronic transactions.<sup>27</sup> A data controller “may voluntarily subscribe” to the principles for electronically collecting personal information stipulated in the Act by recording such fact in an agreement with a data subject; however, the data controller must subscribe to all the applicable principles and not just parts thereof.<sup>28</sup> Once POPIA takes effect, it will amend the definition of the term “personal information” under ECTA to include location information.<sup>29</sup> In addition, application of the provisions of ECTA relating to the protection of personal information will be limited to instances

---

<sup>22</sup> Id. § 27(1)(b).

<sup>23</sup> Id. §§ 28 & 33.

<sup>24</sup> Id. § 19(1).

<sup>25</sup> Id. § 19(2).

<sup>26</sup> Id. § 6.

<sup>27</sup> ECTA § 50.

<sup>28</sup> Id.

<sup>29</sup> POPIA § 110.

where they are more extensive than the principles and protections afforded under POPIA.<sup>30</sup> ECTA includes nine principles for electronically collecting personal information:

- (1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.
- (2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
- (3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
- (4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.
- (5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
- (6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.
- (7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
- (8) The data controller must delete or destroy all personal information which has become obsolete.
- (9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.<sup>31</sup>

#### 4. *Promotion of Access to Information Act*

Aimed at implementing the access to information clause of the Constitution, the Promotion of Access to Information Act (PAIA) includes some key data protection provisions. PAIA accords a person the right to access records held by public or private bodies containing his or her personal information.<sup>32</sup> As in the case of ECTA, when POPIA takes effect, the definition of the term “personal information” under PAIA will be amended to include location information.<sup>33</sup> In addition, it bars a public or a private body from disclosing records if doing so “would involve the

---

<sup>30</sup> Id. 3(2)(b).

<sup>31</sup> ECTA § 51.

<sup>32</sup> PAIA §§ 11 & 50.

<sup>33</sup> POPIA § 110.

unreasonable disclosure of personal information about a third party, including a deceased individual.”<sup>34</sup> The Act further requires that public and private bodies take reasonable steps to put in place internal measures for correcting personal information.<sup>35</sup>

5. *Regulation of Interception of Communications and Provision of Communication-Related Information Act*

As a general rule, the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) bars interception of communication, stating that “no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.”<sup>36</sup> However, there are exceptions in which RICA permits the interception and monitoring of direct and indirect communications with an interception direction issued by a designated judge.<sup>37</sup>

**B. Data Retention and Location Tracking**

1. *POPIA*

As noted above, the definition of the term “personal information” under POPIA includes location information. POPIA bars the retention of personal information for a longer period than is necessary to achieve the purpose for which it was collected and processed.<sup>38</sup> However, personal information may be retained beyond that period if the law or a contract between the parties involved authorizes or requires it, “the responsible party reasonably requires the record for lawful purposes related to its functions or activities,” or the data subject consents to it.<sup>39</sup> Further retention is also permitted for “historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.”<sup>40</sup>

After the period for authorized retention of a record of personal information lapses, the responsible party “must destroy or delete a record of personal information or de-identify<sup>[41]</sup> it as

---

<sup>34</sup> PAIA §§ 34 & 63.

<sup>35</sup> Id. § 88.

<sup>36</sup> Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), § 2 (Sept. 2005), <https://perma.cc/K6RN-8AVH>.

<sup>37</sup> Id. § 16.

<sup>38</sup> POPIA § 14.

<sup>39</sup> Id. § 14.

<sup>40</sup> Id.

<sup>41</sup> This means deleting information that: (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject. Id. § 1.

soon as reasonably practicable.”<sup>42</sup> Destruction or deletion of a record of personal information “must be done in a manner that prevents its reconstruction in an intelligible form.”<sup>43</sup>

On April 3, 2020, the Regulator issued a guidance note on processing of personal information. Noting that not all the sections of POPIA have come into effect, the Regulator encouraged responsible parties to proactively comply with its provisions “when processing personal information of data subjects who have tested or are infected with COVID-19, or who have been in contact with such data subjects.”<sup>44</sup> The Guidance states that, when processing personal information, responsible parties must adhere to a number of conditions.<sup>45</sup>

The Guidance requires electronic communications providers to provide the South African government with location-based data of their customers in certain circumstances and authorizes the government to use such information in managing the spread of COVID-19, if

- a) processing complies with an obligation imposed by law on the responsible party; or
- b) processing protects the legitimate interest of a data subject; or
- c) processing is necessary for the proper performance of a public law duty by a public body; or
- d) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

However, the Government must still comply with all the applicable conditions for the lawful processing as set out in this Guidance Note.<sup>46</sup>

The Guidance further notes that communication service providers may provide to the government location-based data for “the purpose of conducting mass surveillance of data subjects if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form.”<sup>47</sup>

---

<sup>42</sup> Id. § 14.

<sup>43</sup> Id.

<sup>44</sup> Information Regulator, Guidance Note on the Processing of Personal Information in the Management of COVID-19 Pandemic in Terms of the Protection of Personal Information Act 4 of 2013 (POPIA), § 2 (Apr. 3, 2020), <https://perma.cc/3TW2-5K24>. Section 3.7 of the Guidance note defines the term “responsible party” as

a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information. The following are examples of responsible parties in the context of the management of COVID-19 and include but not limited to, the NCC, National Department of Health, Provincial Department, Local Government, National Institute of Communicable Disease (NICD), National Health Laboratories Services (NHLS), Independent laboratories, Mobile Network Operators, Voluntary Organizations.

<sup>45</sup> Id. § 4.

<sup>46</sup> Id. § 5.1.

<sup>47</sup> Id. § 5.2.

The Guidance concludes that all regulations issued to combat the spread of COVID-19 “should be implemented in conjunction with the applicable conditions for the lawful processing of personal provided for in POPIA to ensure respect for the right to privacy.”<sup>48</sup>

## 2. RICA

RICA requires that telecommunication service providers “(a) provide a telecommunication service which has the capability to be intercepted;<sup>[49]</sup> and (b) store communication-related information” for three to five years.<sup>50</sup> An interception direction,<sup>51</sup> a direction for gathering real-time communication related information,<sup>52</sup> or a direction for gathering archived communication may be issued for a number of reasons, including if the judge before whom the application for an interception direction is made finds that there are reasonable grounds to believe that “the gathering of information concerning an actual [or potential] threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary.”<sup>53</sup>

RICA expressly bars notification of the subjects of the interception of their communication including after the conclusion of the surveillance.<sup>54</sup>

In September 2019, the Gauteng Division of the High Court of South Africa at Pretoria declared a number of RICA’s provisions unconstitutional. These include the provisions of RICA that bar

---

<sup>48</sup> Id. § 9.

<sup>49</sup> The terms “intercept” and “interception” are defined by section 1 of RICA as

the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the –

- (a) monitoring of any such communication by means of a monitoring device;
- (b) viewing, examination or inspection of the contents of any indirect communication; and
- (c) diversion of any indirect communication from its intended destination to any other destination.

<sup>50</sup> Id. § 30(1). RICA section 1 defines “communication related information” as

any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system.

<sup>51</sup> This is a written or oral direction issued by an authorized judge permitting interception of any communication in the country “in the course of its occurrence or transmission. RICA § 1.

<sup>52</sup> “Real-time communication related information” is “communication-related information which is immediately available to a telecommunication service provider– (a) before, during, or for a period of 90 days after, the transmission of an indirect communication; and (b) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates.” Id.

<sup>53</sup> Id. §§ 16–19.

<sup>54</sup> Id. §§ 16, 17(6), 18(3)(a), 20(6), 21(6) & 22(7).

notification of subjects of interception; the provision that allows for the appointment of a judge responsible for hearing applications for and issuing directions allowing surveillance, to the extent it fails to guarantee the independence of the judge; and the provisions that allow application for and obtaining a surveillance direction to the extent that they fail to “address expressly the circumstances where a subject of surveillance is either a practicing lawyer or a journalist.”<sup>55</sup> However, as required under the South African Constitution, the High Court’s decision will only take effect if it is confirmed by the Constitutional Court.<sup>56</sup>

### 3. ECTA

As noted above, ECTA allows data controllers to voluntarily subscribe to a number of data privacy principles under the umbrella of which they may process data subjects’ personal information, which will include location information once a law amending POPIA takes effect. A data controller that subscribes to these principles may store personal information of the data subject.<sup>57</sup> The applicable principles require that the data controller keep a record of the personal information in question and the record of a third party to whom the record was disclosed, if any, for as long as the personal information is used and for a period of one year afterwards.<sup>58</sup>

### 4. Public Health Act

The Public Health Act permits health workers and health care providers who have access to the health records of a user to disclose the user’s personal information, as defined under POPIA, “to any other person, health care provider or health establishment as is necessary for any legitimate purpose within the ordinary course and scope of his or her duties where such access or disclosure is in the interests of the user.”<sup>59</sup> The Act also requires that a healthcare facility in possession of healthcare records “set up control measures to prevent unauthorised access to those records and to the storage facility in which, or system by which, records are kept.”<sup>60</sup>

## III. Electronic Measures to Fight COVID-19 Spread

On March 15, 2020, South Africa declared a national state of disaster under the 2002 Disaster Management Act due to the coronavirus pandemic.<sup>61</sup> During a state of disaster, the Disaster Management Act allows the government to issue regulations relating to, *inter alia*, “the movement of persons and goods to, from or within the disaster-stricken or threatened area,” “the dissemination of information required for dealing with the disaster,” and “other steps that may

---

<sup>55</sup> Amabhungane Centre for Investigative Journalism NPC and Another v. Minister of Justice and Correctional Services and Others, 2020 (1) SA 90 (GP) 64-68, <https://perma.cc/6QUX-XBJF>.

<sup>56</sup> South Afr. Const. § 167(5).

<sup>57</sup> ECTA § 51.

<sup>58</sup> *Id.*

<sup>59</sup> National Health Act No. 61 of 2003, § 15 (July 18, 2004), <https://perma.cc/HF3A-PCG3>.

<sup>60</sup> *Id.* § 17.

<sup>61</sup> Declaration of a National State of Disaster, Government Notice 313 (Mar. 15, 2020), <https://perma.cc/6HCG-3P7J>.

be necessary to prevent an escalation of the disaster, or to alleviate, contain and minimise the effects of the disaster.”<sup>62</sup> Similarly, the 2004 Disaster Management Regulations (as amended) state that any minister “may issue and vary directions, as required, within his or her mandate, to address, prevent and combat the spread of COVID-19, from time to time, as may be required,” including “steps that may be necessary to prevent an escalation of the national state of disaster, or to alleviate, contain and minimise the effects of the national state of disaster.”<sup>63</sup> Based on these authorities, the Department of Communications and Postal Services and the Department of Cooperative Governance and Traditional Affairs issued directions and regulations relating to location tracking for the purpose of combating the spread of COVID-19.

#### **A. Department of Communications and Postal Services Direction**

On March 26, 2020, the Minister of Communications and Postal Services issued a direction that includes the following “individual track and trace” (contact tracing) clause:

The Electronic Communication Network Service (ENCS) and Electronic Communication Service (ECS) Licensee, internet ad digital sector in general, must provide location-based services in collaboration with the relevant authorities identified to support designated departments to assist and combat the spread of COVID-19.<sup>64</sup>

Responding to concerns of government intrusion into citizens’ lives, the Minister sought to reassure the public in a statement stating that,

[w]hen we say we are going to use cell phone numbers, it doesn’t meant we are going take anybody’s number. Those that test and are found to be positive . . . it is those people that the Department of Health will seek permission from the Electronic Communications Network Service (ECNS) licence[e]s to access their geolocation.<sup>65</sup>

On May 8, 2020, the contact tracing clause was repealed.<sup>66</sup>

The direction also requires the South African Post Office to participate in individual tracking and tracing efforts:

The South African Post Office must make available its national address system and any applicable database to assist the relevant authorities identified to track and trace

---

<sup>62</sup> Disaster Management Act No. 57 of 2002, § 27(2)(f), (k), (n) (Apr. 1, 2004), <https://perma.cc/4LAU-YMJ2>.

<sup>63</sup> Regulations Issued in terms of Section 27(2) of the Disaster Management Act, 2002, § 4(10)(c) (Apr. 29, 2020), <https://perma.cc/9ZP3-AUF8>.

<sup>64</sup> Disaster Management Act (57/2002): Electronic Communications, Postal and Broadcasting Directions Issued Under Regulation 10(8) of the Act, Government Gazette (GG) No. 43164, § 8.1 (Mar. 26, 2020), <https://perma.cc/GCB6-W5VE>.

<sup>65</sup> *Contact Tracing Will Not Be Used to Spy on Citizens*, South Africa Government News Agency (Apr. 2, 2020), <https://perma.cc/RJ9A-M7LA>.

<sup>66</sup> Disaster Management Act (57/2002): Electronic Communications, Postal and Broadcasting Directions Issued Under Regulation 10(8) of the Act, § 8.

individuals that have been infected and such other persons that may have been in direct contact with such infected persons. A database may be correlated with other sources from government and private sector.<sup>67</sup>

This clause appears to be in force to date.

## **B. Department of Cooperative Governance and Traditional Affairs Regulations**

The Regulations issued by the Minister of Cooperative Governance and Traditional Affairs include provisions on leveraging technology for contact tracing.<sup>68</sup> The Regulations mandate the Department of Health to develop a national database (COVID-19 Tracing Database) “to enable the tracing of persons who are known or reasonably suspected to have come into contact with any person known to or reasonably suspected to have contacted COVID-19.”<sup>69</sup> The Database must include various pieces of information, including

- (a) the first name and surname, identity or passport numbers, residential address and other address where such person could be located, and cellular phone numbers of all persons who have been tested for COVID-19;
- (b) the COVID-19 test results of all such persons; and
- (c) the details of the known or suspected contacts of any person who tested positive for COVID-19.<sup>70</sup>

In addition to the restrictions and oversight discussed below, housing the COVID-19 Tracing Database within the Department of Health probably makes it less likely that the information collected for and stored in the Database will be used for purposes other than contact tracing as compared to those countries where national security agencies are involved in contact tracing.<sup>71</sup>

### *1. Testing and Collection of Information*

When a person is tested for COVID-19, the following information is collected for submission to the director-general of the Department of Health and inclusion in the COVID-19 Tracing Database:

---

<sup>67</sup> Id.

<sup>68</sup> Regulations Issued in terms of Section 27(2) of the Disaster Management Act, 2002, § 8.

<sup>69</sup> Id.

<sup>70</sup> Id.

<sup>71</sup> Sara Wild, *Antipoaching Tech Tracks COVID-19 Flare-Ups in South Africa*, Scientific American (May 12, 2020), <https://perma.cc/GK3J-ZP9C>.

- (a) the first name and surname, identity or passport number, residential address, and cellular phone numbers of the person concerned [tested]; and
- (b) a copy or photograph of the passport, driver's licence, identity card or identity book of the person tested.<sup>72</sup>

Any laboratory that tests a sample for COVID-19 is also required to report to the director-general the information of the person whose sample it tested and the test results.<sup>73</sup> Similarly, the National Institute for Communicable Diseases (NICD) must report to the director-general similar information in its possession and any information regarding the persons with whom a COVID-19 patient may have come into contact.<sup>74</sup>

In addition, accommodation establishments are required to report to the director-general, for the purpose of inclusion in the COVID-19 Tracing Database, the contact information, such as phone number, address, and identification information, of every person who stays in the establishment during the lockdown.<sup>75</sup>

## 2. *Location Tracking*

The Regulations authorize the director-general to direct electronic communications service providers to report to him or her the following information:

- (a) the location or movements of any person known or reasonably suspected to have contracted COVID-19; and
- (b) the location or movements of any person known or reasonably suspected to have come into contact, during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated, with a person contemplated in subparagraph (a).<sup>76</sup>

Upon receiving the directive, the electronic communication services provider in question “must promptly comply.”<sup>77</sup> The director-general is not under an obligation to inform the person whose information is being obtained, used, or disclosed during such activities, but must do so within six weeks from the date of expiration of the national disaster declaration.<sup>78</sup> A national state of disaster lapses three months after the date of declaration; however, it may be terminated before that time or extended beyond the three-month window.<sup>79</sup>

---

<sup>72</sup> Regulations Issued in terms of Section 27(2) of the Disaster Management Act § 8(6).

<sup>73</sup> Id. § 8(7).

<sup>74</sup> Id. § 8(8).

<sup>75</sup> Id. The lockdown covers the time period from March 26 through April 30, 2020. Id. § 1.

<sup>76</sup> Id. § 8(10).

<sup>77</sup> Id.

<sup>78</sup> Id. § 8(16).

<sup>79</sup> Disaster Management Act No. 57 of 2002, § 27(5).

### 3. *Restrictions and Oversight*

The information relating to the location and movements of persons described above may only be obtained for the period of March 5 through the expiration of the national state of disaster declaration,<sup>80</sup> and may only be “obtained, used or disclosed” by authorized persons for the limited purpose of “addressing, preventing or combatting the spread of COVID-19 through contact tracing process.”<sup>81</sup> Information relating to the location and movement of such persons must be included in the COVID-19 Tracing Database to the extent it is relevant for the purpose of conducting contact tracing; however, information not included in the Database may only be retained by the director-general for a maximum of six weeks after it was acquired at which time it must be destroyed.<sup>82</sup>

The director-general must provide a weekly report to the COVID-19 designated judge (a Constitutional Court judge designated to perform this oversight role) “the names and details of all persons whose location or movements were obtained.”<sup>83</sup> The designated judge’s oversight authority does not appear to be meaningful while the collection of information and tracking is in progress; however, he or she may make recommendations for changing the applicable regulation or its enforcement to the relevant cabinet members.<sup>84</sup> Once the program for collection of information and tracking of persons concludes, the designated judge’s oversight role with regard to the fate of the information collected for the Database is more significant (see below).

The Regulations require that information in the COVID-19 Tracing Database be de-identified within six-weeks of the expiration of the national state of disaster declaration and that all information not de-identified be destroyed.<sup>85</sup> De-identified information on the Database may be used for research, study, and teaching purposes only.<sup>86</sup>

The de-identification process, destruction process relating to the information on the Database, and notification of data subjects is subject to judicial and legislative oversight. The director-general must file a report on the de-identification and destruction process of the information in the Database, as well as the notification of data subjects, to the designated judge.<sup>87</sup> The designated judge may “give directions as to any further steps to be taken to protect the right to privacy of those persons whose data has been collected, which directions must be complied with.”<sup>88</sup> The director general’s report must also be considered in Parliament.<sup>89</sup>

---

<sup>80</sup> Regulations Issued in terms of Section 27(2) of the Disaster Management Act, 2002, § 8(11).

<sup>81</sup> Id. § 8(11).

<sup>82</sup> Id.

<sup>83</sup> Id. §§ 8(13) & (14).

<sup>84</sup> Id. § 8(15).

<sup>85</sup> Id. § 8(17)(a) & (c).

<sup>86</sup> Id. § 8(17)(b).

<sup>87</sup> Id. § 8(17)(d).

<sup>88</sup> Id. § 8(18).

<sup>89</sup> Id. § 8(19).

#### 4. Penalties

The Regulations bar unauthorized disclosure of information stored in the Database; a violation of this bar is an offense punishable by a fine, custodial sentence not exceeding six-months, or both.<sup>90</sup> The following conduct is also criminalized and subject to the same penalties:

- Failure of accommodation establishments to collect and transmit to the director-general all the required information described above
- Obtaining, using, or disclosing relevant information for a purpose other than addressing, preventing, or combating the spread of COVID-19
- Retention of such information for a period longer than authorized by the Regulations
- Failure to de-identify or destroy information on the Database as required by the Regulations
- Failure of a communications service provider to follow the director-general's direction to collect and make available location and movement information of persons suspected of having contracted COVID-19 and anyone suspected of having come into contact with such persons
- Failure to adhere to directions of the designated judge regarding the steps that must be taken to ensure the privacy of persons whose information has been collected for the Database<sup>91</sup>

---

<sup>90</sup> Id. § 14.

<sup>91</sup> Id.

# United Arab Emirates

*George Sadek  
Foreign Law Specialist*

**SUMMARY** The United Arab Emirate’s (UAE’s) Department of Health, located in the Emirate of Abu Dhabi, has launched a new mobile application, called “TraceCovid.” The purpose of the application is to track infected individuals. The UAE does not have one specific law on privacy and data protection. The country has a number of legal instruments to protect the privacy of individuals. These legal instruments include Federal Law No. 5 of 2012 on Combating Cybercrimes, Federal Law No. 3 of 1987 on the Penal Code, and the 1971 UAE Constitution. Federal Law No. 2 of 2019, known as “the Health Data Law,” is the first and only domestic legislation regulating data retention and protecting the privacy of personal health data.

## I. Overview

As of May 22, 2020, the total number of diagnosed COVID-19 cases in the United Arab Emirates (UAE) was 26, 898 including 12,755 recoveries and 237 fatalities.<sup>1</sup> In response, the UAE’s Department of Health, located in the Emirate of Abu Dhabi, launched a new mobile application, called “TraceCovid.” The purpose of the application is to track infected individuals. The application can be downloaded on both Apple and Android devices. The application uses the Bluetooth function on smartphones and allows users to detect and identify another device with the same application installed.<sup>2</sup>

According to the Department of Health, if two people are near each other, their mobile phones will exchange an encrypted Secure Tracing Identifier (STI) and store the exchanged STI locally on their phones. If one of them is infected with the virus, the relevant authorities will be able to access the user’s data and timestamps. This will allow the medical authorities to track all the other individuals who have come in close contact with the infected person.<sup>3</sup>

Many citizens and expatriates of the UAE have no reservations about sharing their data in general, especially with retailers. According to a report by professional services firm KPMG, 78% of UAE consumers are willing to share their personal data with retailers and other institutions. Only about 22% percent are not in favor of disclosing their personal data with any organization at all, according to the same report.<sup>4</sup> According to the Telecommunications Regulatory Authority

---

<sup>1</sup> UAE Coronavirus (COVID-19) Updates, UAE Sup. Council for Nat’l Security, <https://perma.cc/9QCL-BP4F>.

<sup>2</sup> Varun Godinho, *UAE Launches Covid-19 Tracing App*, Gulf Bus. (Apr. 19, 2020), <https://perma.cc/W4LQ-UTYH>.

<sup>3</sup> Id.

<sup>4</sup> Alkesh Sharma, *UAE Consumers Willing to Share Data with Retailers Despite Cybercrime Threats*, Nat’l (Jan. 9, 2019), <https://perma.cc/EZR4-QZ6Y>.

(TRA), mobile phone penetration in the UAE increased to 228.3 phones per 100 people in the first quarter of 2017, with the total number of subscriptions amounting to 19.8 million.<sup>5</sup>

## II. Legal Framework

### A. Privacy and Data Protection

The UAE does not have one specific law on privacy and data protection. The country has a number of legal instruments protecting the privacy of individuals. These legal instruments include Federal Law No. 5 of 2012 on Combating Cybercrimes, Federal Law No. 3 of 1987 on the Penal Code, and the 1971 UAE Constitution.

#### 1. *Federal Law No. 5 of 2012*

The Law penalizes individuals and entities who disclose any information obtained by electronic means, if such information was obtained in an unauthorized manner.<sup>6</sup> It also criminalizes the act of using, without authorization, any computer network, website or method of information technology to disclose private information.<sup>7</sup>

#### 2. *Federal Law No. 3 of 1987 on the Penal Code*

The penal code of the UAE sanctions any person who violates the private or family life of other individuals by eavesdropping, recording, or transmitting, through a device of any kind, conversations that took place in a private place or by telephone or any other device, or by capturing or transmitting, through any type of device, a picture of a person in a private place.<sup>8</sup>

#### 3. *The 1971 Constitution*

The Constitution states that communications by post, telegraph or other means are confidential.<sup>9</sup>

### B. Data Protection and Retention

Federal Law No. 2 of 2019, known as “the Health Data Law,” is the first and only domestic legislation regulating data retention and protecting the privacy of personal health data.<sup>10</sup> It also

---

<sup>5</sup> UAE’s Mobile Phone Penetration Rises to 228%, Al-Rasub (May 29, 2017), <https://perma.cc/CX9B-DVCR>.

<sup>6</sup> Federal Law No. 5 of 2012, art. 21, al-Jaridah al-Rasmīyah, vol. 540, 13 Aug. 2012, <https://perma.cc/WK27-478N>.

<sup>7</sup> Id. art. 22.

<sup>8</sup> Federal Law No. 3 of 1987, art. 378, 12 Aug. 1978, Abu Dhabi Jud. Dep’t. website, <https://perma.cc/UV8M-GL4F> (in English).

<sup>9</sup> UAE Const. of 1971 arts. 25 (amended 2009), 31, <https://perma.cc/NG8U-MPHV>.

<sup>10</sup> Federal Law No. 2 of 2019, al-Jaridah al-Rasmīyah, vol. 647, 12 Feb. 2014, <https://perma.cc/4UF3-L7DY>.

regulates the use of information technology and communications (ITC) in the healthcare sector.<sup>11</sup> Furthermore, the Law governs the transfer, sharing, and retention of electronic health data, including patient names, consultation, diagnosis and treatment data, alphanumeric patient identifiers, common procedural technology codes, medical scan images and lab results.<sup>12</sup>

Under the title “The Obligation to Use Information Technology and Communications,” the law requires that health care providers use ITC to store and transfer health data to ensure its confidentiality.<sup>13</sup> The law also mandates that health care providers preserve health data against any unauthorized modifications, loss, alteration, deletion or addition.<sup>14</sup>

Health care providers must also create adequate technical procedures to guarantee the security of health data.<sup>15</sup> The Law obligates them to ensure that only authorized personnel have access to patients’ health data to guarantee its confidentiality.<sup>16</sup>

Retention and transfer of the health data of UAE citizens and expatriates outside the UAE are prohibited unless authorized by the Ministry of Health.<sup>17</sup> Violation of this provision by any person or entity is punishable by a fine between 500,000 and 700,000 Emirati Dirham (between US\$125,222 and US\$175,312).<sup>18</sup> Health care providers must retain health data for a period not less than 25 years from the date on which the last procedure took place.<sup>19</sup>

The Law stresses protection of the confidentiality of health data. However, it allows sharing of health data without the permission of the patient under the following circumstances: (1) responding to a request for information issued by insurance companies covering the medical services, (2) for the purpose of adopting public health preventive and treatment measures, (3) to respond to a request for information issued by a judicial authority, and (4) to respond to a request for information about a patient pertaining to the preservation of public health.<sup>20</sup>

The Law imposes disciplinary actions and fines ranging between one thousand and one million Emirati Dirhams (between US\$250 and US\$250,000) on health care providers who violate any of its provisions.<sup>21</sup>

---

<sup>11</sup> Els Janssens & Kellie Blythe, *UAE Issues Law to Protect Health Data and Restrict Its Transfer Outside the Country*, Baker McKenzie (Mar. 20, 2019), <https://perma.cc/AL8D-LXNY>.

<sup>12</sup> PwC, *Health Data Protection in the UAE: A New Federal Law 3 (2019)*, <https://perma.cc/6RFS-YBX8>.

<sup>13</sup> Federal Law No. 2 of 2019, art. 4(1).

<sup>14</sup> *Id.* art. 4(2).

<sup>15</sup> *Id.* art. 6.

<sup>16</sup> *Id.* art. 8.

<sup>17</sup> *Id.* art. 13.

<sup>18</sup> *Id.* art. 24.

<sup>19</sup> *Id.* art. 20.

<sup>20</sup> *Id.* art. 16.

<sup>21</sup> *Id.* art. 25.

### III. Electronic Measures to Fight COVID-19 Spread

On April 19, 2020, the Health Department in Abu Dhabi announced that it had launched a mobile application, called “TraceCovid.” The department has urged all UAE citizens and expatriates to install the application on their mobile devices. The main purpose of the mobile application is to identify any individuals who came close to someone who is a COVID-19 patient.<sup>22</sup>

According to the main web page of “TraceCovid UAE,” the application authorizes users to detect mobile devices that have the same application installed. To illustrate, when a person is located at a supermarket and comes close to another person whose phone also has TraceCovid installed, the application on both mobile devices exchanges an encrypted STI and stores the exchanged STI locally on their devices. The STI consists of anonymized data and a timestamp. In the event that one of those two people gets the virus, the health department will request that the infected person upload the list of STIs stored locally on that person’s mobile phone. Such information will assist the medical authorities in contacting other people who may have come in close contact with the infected person and identify them faster to minimize the spread of the virus.<sup>23</sup>

The Abu Dhabi Health Department has announced that the TraceCovid application does not affect the use and efficiency of Bluetooth on a mobile phone. The application runs in the background to communicate with another person’s mobile device that has the same application. The department also said that the privacy of the personal data of the person installing the application is protected.<sup>24</sup>

The Health Department of Abu Dhabi also launched a second mobile app for individuals who have been identified as COVID-19 patients or who have come in close contact with someone infected with COVID-19. These individuals are ordered to quarantine at home.<sup>25</sup>

According to the health department, these individuals will be asked to download a mobile app from Google Play or the App Store. The app ensures that the quarantined person adheres to mandatory requirements. The main purpose of the app is to send alerts that inform users to stay within the range of movement allowed during the quarantine. The app provides the health authorities with the precise location of these individuals to ensure that they do not violate the quarantine.<sup>26</sup>

We were unable to find any information on tracking individuals who do not possess a mobile device.

---

<sup>22</sup> *Coronavirus: New App to Help Track Covid-19 Cases in UAE*, Nat’l (Apr. 19, 2020), <https://perma.cc/A6R7-JTY5>.

<sup>23</sup> *How TraceCovid Works*, TraceCovid UAE, <https://perma.cc/P6MR-R3HN>.

<sup>24</sup> *Id.*

<sup>25</sup> Ashwani Kumar, *UAE Fights Covid-19: New Self-Quarantine App Launched to Stop Spread*, Khaleej Times (Apr. 3, 2020), <https://perma.cc/C35A-46Q5>.

<sup>26</sup> *Id.*