United Nations A/HRC/52/37

General Assembly

Distr.: General
27 December 2022
English
Original: Spanish

Human Rights Council
Fifty-second session
27 February 2023–31 March 2023
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the COVID-19 pandemic

Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères

Summary

The present report has been prepared pursuant to Human Rights Council resolution 46/16.

In the context of the coronavirus disease (COVID-19) pandemic, data were collected from millions of people in all countries of the world for one sole purpose: to combat the pandemic. Although the principles of purpose and time limitation (which require personal data to be deleted from databases once the purpose has been achieved) are incorporated in national and international regulations on personal data processing, the following questions have nonetheless arisen: What will happen to the personal data collected from these millions of people for the purpose of combating the COVID-19 pandemic? Will they be deleted? Will they be anonymized? Will they be used for purposes other than those for which they were collected?

The Special Rapporteur on the right to privacy, Ana Brian Nougrères, envisages that the review forming the basis of this report might serve as a call on States to ensure timely application of the principles of purpose limitation, deletion of data and demonstrated accountability (also referred to as proactive accountability) in respect of the personal data that were collected from millions of persons in the context of the pandemic.

I. Introduction

1. On 11 March 2020, the World Health Organization (WHO) declared a state of pandemic in view of the rapid spread and severity of the coronavirus disease (COVID-19). The announcement signified that the epidemic had spread to multiple countries and continents throughout the world and was affecting large numbers of people.[1]

2. The declaration of the pandemic prompted States to establish and implement emergency response mechanisms to curb the spread of COVID-19, among other actions.

3. As part of this action, public entities in different countries of the world collected data from millions of people with a view to implementing measures for detecting and combating COVID-19 and tracking its spread, and thus protecting public health and preventing its transmission. In addition to contact and personal identification data, the information collected included health-related data such as details of symptoms, test results and diagnoses, all of which are considered sensitive personal data.

4. Additionally, biosecurity protocols were adopted to mitigate and control the risks associated with the COVID-19 pandemic and ensure an appropriate response in different activities, services, sectors, processes, establishments and locations. The implementation of such measures also entailed the collection and processing of personal data.

5. According to WHO, as at 24 November 2022, 636,089,587 confirmed cases of severe acute respiratory syndrome coronavirus-2 (SARS-CoV-2)[2] had been recorded worldwide. The breakdown of these cases by region is shown in Table 1 below.

Table 1
Number of confirmed cases of COVID-19 in different regions of the world (as at 24 November 2022)

Region	*Confirmed cases*
Europe	263 923 098
Americas	181 395 514
Western Pacific	97 570 958
South-East Asia	60 620 885
Eastern Mediterranean	23 187 814
Africa	9 390 554

Source: WHO (2022).

6. Data processing regulations allow, among other things, for personal information to be collected and used in the event of a medical or health emergency. However, such a situation does not rescind the fundamental right to personal data protection, and compliance with the regulations protecting this right is obligatory for all entities that control and/or process personal data.

7. Data collected for the purpose of combating COVID-19 may be used for this purpose only, and may be stored only for as long as is reasonable and necessary for said purpose. Once the purpose has been achieved, the data must be deleted or anonymized in accordance with the data processing regulations of each country.

8. A set of general principles that provides a basis for the fair and transparent processing of personal data has been established at the international level. These principles consist of a series of rules intended to ensure that the collection and use of personal information does not affect or harm the rights of individuals. By determining whether or not the principles have

[1] Pan American Health Organization, “WHO characterizes COVID-19 as a pandemic”. Available at: https://www.paho.org/en/news/11-3-2020-who-characterizes-covid-19-pandemic.

[2] See https://covid19.who.int/ (accessed 25 November 2022).

been respected, it is possible to verify whether, in any given case, the data processing is being carried out fairly and lawfully.

9. The following sections examine three of the principles relevant to the processing of data in the context of the fight against COVID-19, namely, purpose limitation, deletion of data and demonstrated or proactive accountability.

II. Principle of purpose limitation for the processing of data collected to combat the COVID-19 pandemic

10. A number of texts drawn up by organizations in different parts of the world[3] provide that personal data may be collected for specific, clear and lawful purposes. The principle of purpose limitation:

(a) Limits the purposes for which the personal data may be used;

(b) Prevents personal information from being used arbitrarily by persons or entities holding the personal data of third parties;

(c) Requires that data be used only for purposes permitted by law or for which the data subjects have given their consent;

(d) Allows data to be used for purposes compatible with those permitted by law or for which the data subjects have given their consent. The subsequent processing of personal data for scientific and historical research purposes or for statistical ends, all in the public interest, is not usually considered incompatible with initial purposes, provided that States establish appropriate safeguards.

III. Principle of deletion of data collected in the context of the COVID-19 pandemic

11. Not only must data be processed for a specific, clear and lawful purpose; it must also be processed for a period no longer than is necessary to achieve the intended purpose. In other words, as a general rule, the processing of data should be subject to a time limit and should not be permitted to continue indefinitely or ad infinitum.

12. Once the time limit has expired, the data must be either definitively deleted or else anonymized in such a way that, beyond the period of time necessary to achieve the purposes for which the data were collected, it is impossible to identify the data subject.

13. At the international level, this principle generally means that:

[3] Organisation for Economic Co-operation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980 and July 2013 update; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108 of 28 January 1981; United Nations, Guidelines for the regulation of computerized personal data files, 14 December 1990; Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, 8 November 2001; Asia-Pacific Economic Cooperation Forum, Asia-Pacific Economic Cooperation Privacy Framework, 2004; Spanish Data Protection Agency, Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data, Madrid, 5 November 2009; European Parliament and Council of the European Union, 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); Ibero-American Data Protection Network, Guidelines for Harmonization of Data Protection in the Ibero-American Community, 2017; Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, October 2018; and Organization of American States, Inter-American Juridical Committee, Updated Principles on Privacy and Personal Data Protection, 2021.

(a) Data cannot be retained indefinitely or in a form that allows for individual data subjects to be identified;

(b) Personal data may be retained no longer than is necessary to achieve the intended purpose;

(c) Provided the regulations establish appropriate safeguards, personal data may be retained for a longer period for historical, statistical or scientific purposes;

(d) Data must be either deleted or, where appropriate, converted into an anonymous form that can continue to be processed without the data subjects being identified.

IV. Principle of demonstrated or proactive accountability in the processing of data collected to combat the COVID-19 pandemic

14. The term "accountability" comes from the Anglo-Saxon world[4] and, despite the varying interpretations that may be attributed to it, as far as data protection is concerned, the term is understood to refer to the action that entities should take to comply with the relevant regulations in practice and what they should do to demonstrate that the action taken is appropriate, relevant and effective.

15. Ensuring that data protection regulations are effectively applied in practice is an ongoing challenge for any entity. Although it is important to adopt regulations, adoption alone is insufficient since regulations are not automatically effective; measures to give them effect are also necessary. Efforts should therefore be focused on ensuring that data processing regulations set specific, tangible goals rather than purely theoretical ones, and are thus of genuine benefit.

16. The principle of accountability is of paramount importance to achieving this end. This principle requires those who control and/or process data to implement appropriate, effective and verifiable measures through which to demonstrate that they have duly complied with personal data processing regulations. Such measures should be subject to ongoing review and evaluation in order to gauge how effective they are in terms of ensuring compliance and protecting the rights of data subjects.

17. The principle of accountability calls for less rhetoric and more action in fulfilling the obligations established under personal data processing regulations. It requires entities to take specific action to ensure that personal data are processed fairly and lawfully.

18. The challenges that entities face in ensuring respect for the principle of accountability extend beyond the simple issuance of documents since, in the exercise of their duties, they are required to demonstrate genuine and effective compliance in practice. The purpose of the principle of accountability is to ensure that constitutional and legal obligations related to personal data processing are verifiably upheld and genuinely serve to protect the rights of individuals.

19. From the various international documents consulted,[5] it can be concluded that demonstrated responsibility, which is also referred to as proactive accountability:

[4] European Commission, Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, paras. 21–23. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

[5] A detailed study of the principle of demonstrated accountability in the field of international regulation and of the various guides published on the subject can be found in: Nelson Remolina, Manuel Tenorio and Gustavo Quintero, *De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil: hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información* (Bogotá, Temis, 2018). Available at: https://habeasdatacolombia.uniandes.edu.co/?p=2836.

(a) Requires entities to implement appropriate, relevant, timely and effective measures and procedures to demonstrate compliance with personal data processing regulations;

(b) Entails implementing and supervising verification procedures to ensure that the measures adopted not only exist on paper but are implemented and work in practice (internal or external audits, etc.).[6]

V. Findings

20. The following paragraphs describe the methodology used to establish whether the principles of purpose limitation, deletion of data and demonstrated accountability are being respected in practice.

21. Firstly, questionnaires were sent to 186 countries asking, among other questions,[7] when personal data collected for the purpose of combating COVID-19 would be deleted and whether States had incorporated the concept of "post-pandemic" in their regulations for purposes of the deletion of this information.

22. The following 18 countries are thanked for their responses: Albania, Algeria, Austria, Bermuda, Chile, Costa Rica, Croatia, Cyprus, Czechia, Honduras, Ireland, Mauritius, Morocco, Poland, Qatar, Romania, Saudi Arabia and Uruguay.

23. Although not all countries responded to all the questions, it can be concluded from the responses received that there is no specific guidance for the retention of COVID-19-related data in the countries in question and that the general principles and regulations for the protection of personal data therefore apply – specifically, the principle of purpose limitation, which means that data may be kept until the lawful purpose for which they were collected has been achieved, taking into consideration health sector-specific standards. Information may also be kept for scientific or statistical purposes, provided it is in a form in which the data subjects can no longer be identified.

24. Secondly, checks were carried out to corroborate information about the applications and web pages created by the public authorities of a representative sample of 20 countries – selected from Africa, the Americas, Asia, Europe and Oceania – for the purpose of collecting and processing personal data for use in detecting and/or combating COVID-19 and tracking its spread with a view to protecting public health and preventing the transmission of the virus.

25. To establish whether these applications and web pages took account of the principles of purpose limitation, deletion of data and demonstrated responsibility, the following questions were asked:

- Question 1 (purpose limitation): Are users informed of the purpose for which their personal data are being collected and processed?
- Question 2 (deletion or anonymization): Are users expressly informed that their data will be deleted or anonymized as soon as the purpose for which they were collected is achieved?
- Question 3 (accountability in general): Are any measures for ensuring demonstrated or proactive accountability in respect of the processing of personal data mentioned?
- Question 4 (accountability and deletion): Have you committed to implementing demonstrated or proactive accountability measures to comply with the principle of deletion of data?

[6] European Commission, Article 29 Data Protection Working Party, Opinion 3/2010 on the principle accountability, paras. 21–23. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

[7] Question 7 of the questionnaire asks: "When will the personal data concerning COVID-19 be deleted from the databases?" Question 8 asks: "Has your country regulated the post-pandemic concept from the point of view of the removal of personal data from databases?"

- Question 5 (verification): Is there any mention of a verification procedure for demonstrating or proving that personal data have been deleted or anonymized?
- Question 6 (audit): Is the use of an external auditor to certify that personal data have been effectively deleted or anonymized envisaged?

The results are shown in Table 2 below.

Table 2
Comparison of application of the principles of purpose limitation, deletion of data and demonstrated accountability in data processing in the applications and/or websites used to combat COVID-19 in 20 countries

Country	*Question 1 (purpose limitation)*	*Question 2 (deletion or anonymization)*	*Question 3 (accountability in general)*	*Question 4 (accountability and deletion)*	*Question 5 (verification)*	*Question 6 (audit)*
Argentina	Yes	Yes (deletion)	No	No	No	No
Australia	Yes	Yes (deletion)	No	No	Yes	No
Belgium	Yes	Yes (deletion)	Yes	No	No	No
Brazil	Yes	No	No	Yes	No	No
Colombia	Yes	Yes (deletion)	Yes	Yes	No	No
France	Yes	Yes (deletion)	Yes	No	No	No
Germany	Yes	Yes (deletion)	No	No	No	No
India	Yes	No	No	No	No	No
Ireland	Yes	Yes (deletion and anonymization)	Yes	No	No	No
Italy	Yes	Yes (deletion)	No	No	No	No
Japan	Yes	No	No	No	No	No
Latvia	Yes	Yes (deletion)	No	No	No	No
Mauritius	Yes	Yes (deletion)	No	No	No	No
Mexico	Yes	No	No	No	No	No
Netherlands	Yes	Yes (deletion)	Yes	No	No	No
New Zealand	Yes	Yes (deletion)	Yes	No	No	No
Singapore	Yes	Yes (deletion)	No	No	No	No
South Africa	Yes	Yes (deletion)	Yes	No	No	No
Spain	Yes	Yes (deletion)	Yes	No	No	No
United Kingdom	Yes	Yes (deletion and anonymization)	Yes	Yes	No	No

Sources: See annex II.

VI. Conclusions

26. **After verification of the information provided about the policies adopted by the public authorities in 20 countries[8] in Africa, the Americas, Asia, Europe and Oceania and the terms and conditions of the applications and/or web pages created by the entities responsible for collecting and processing personal data with a view to detecting and/or combating COVID-19, tracking its spread and thus protecting public health and preventing transmission, the following conclusions were drawn:**

- **All of the public entities applied the principle of purpose limitation in the processing of personal data. Accordingly, all of the policies and/or terms and conditions for the applications and/or web pages contained information about the purpose for which the personal data were being collected and processed.**
- **Not all the public entities provided information about the deletion or anonymization of data once they ceased to be useful for the purposes for which they were collected. Specifically, 20 per cent did not expressly state that the data would be deleted or anonymized as soon as the purpose had been achieved, 70 per cent stated that the information would be deleted and 10 per cent indicated that it would be either deleted or anonymized as soon as the purpose for which it was collected had been achieved.**
- **As regards application of the principle of demonstrated or proactive accountability, the survey revealed that 55 per cent of entities envisaged in their policies the adoption of general demonstrated or proactive accountability measures for processing the data collected, while the remaining 45 per cent made no mention of this aspect.**
- **Only 15 per cent of the entities had committed to implementing demonstrated or proactive accountability measures to comply with the principle of deletion of data.**
- **Notwithstanding the foregoing, very few, if any, entities had established transparent mechanisms for verifying whether personal data had been deleted or anonymized. In fact, only one public authority (equivalent to 5 per cent of the total number of entities surveyed) had established a verification procedure for demonstrating or proving that personal data had been deleted or anonymized, and none of them envisaged using an external auditor to certify that personal data had effectively been deleted or anonymized.**

VII. Recommendations

27. **The Special Rapporteur urges States to ensure that they are genuinely and effectively complying with the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in respect of the data of millions of people that were collected for the purpose of detecting and/or combating COVID-19 and tracking its spread with a view to protecting public health and preventing its transmission.**

28. **The Special Rapporteur calls on States to reinforce the application of the principle of demonstrated or proactive responsibility in all programmes and policies involving the processing of personal data. This requires them, among other things, to adopt relevant, appropriate, timely and effective measures to comply with the legal obligations established in personal data processing regulations. Such measures should be subject to ongoing review and evaluation in order to gauge how effective they are in terms of ensuring compliance and the protection of personal data.**

[8] Argentina, Australia, Belgium, Brazil, Colombia, France, Germany, India, Ireland, Italy, Japan, Latvia, Mauritius, Mexico, the Netherlands, New Zealand, Singapore, South Africa, Spain and the United Kingdom.

29. **States should implement processes and use tools that demonstrate and provide evidence of due compliance with their obligations. Such processes and tools should be transparent and easily verifiable by the competent public authorities and the public in general.**

30. **It is suggested that, before commencing the design and development of applications and software that involve processing personal data for the purpose of carrying out State functions, States should take proactive, preventive measures with a view to establishing a risk monitoring and management system that will ensure that data are processed fairly and lawfully.**

31. **States should also work to cement a public culture that fosters transparent and ethical processing of personal data, with all due safeguards, so as to ensure that transparency becomes an essential component in the design and implementation of all public programmes and policies that involve the processing of personal data.**

32. **The Special Rapporteur urges States to build and consolidate levels of public confidence in the programmes of public entities that involve the processing of personal data by implementing transparent, publicly accessible mechanisms that allow citizens to verify, through a simple process and at any time, that public entities comply in practice with the procedures and commitments set forth in their policy notices and/or terms and conditions for activities that involve the collection, use and exchange of personal data or any other activity in which personal data are processed.**

Annex I

Highlights of the Special Rapporteur's activities in 2022

25 January

Day of Data Protection and Privacy a virtual round table discussion "Management Systems for the Protection of Personal Data: security measures and documents"

15 February

Virtual workshop BTECH Gaps and ways forward in applying the UNGPs for regulating business conduct in the technology sector

23 February

Young Reporters and privacy at the UN, Palais des Nations, Geneva

10–14 March

Presentation of thematic report (A/HRC/49/55) to Human Rights Council in Geneva, and panellist at the Annual Interactive Debate on the Rights of Persons with Disabilities Report on Data Protection

5–7 April

Privacy Symposium conference in Venice organised by University of Geneva

27–29 April

Fifth meeting of the Intergovernmental Group of Experts on E-commerce and the Digital Economy on "Recovering from COVID-19 in an increasingly digital economy: Implications for sustainable development", UNCTAD

2–5 May

World Press Freedom Day 2022 Global Conference, Punta del Este, Uruguay

23–25 May

Panel on the "Regulation of global data flows: a story of the impossible?" at the Computers, Privacy and Data Protection (CPDP2022) in Brussels

6–10 June

Special Rapporteur Annual Meeting in Geneva

11–13 July

CPDP LatAm 2022 dedicated to "Artificial Intelligence and Data Protection in Latin America"

30 August

EU programme "Promoting data protection and cross-border flows" conference on the draft bill to reform Law 25.326 on Data Protection in Argentina

19 September

Virtual side event on Human rights as a guidepost on the pathway of new and emerging digital technologies on Promoting and Protecting Human Rights in the Digital Era, Human Rights Council, Geneva

4 October

Virtual participation in the Expert Roundtable on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy

4–7 October

ICEGOV 2022 roundtable on artificial intelligence and privacy, Guimarães, Portugal

18 October

Presentation of thematic report (A/77/196) at the Third Committee, General Assembly, NY

24 October

Keynote speaker to open the Artificial Intelligence and Data Transfers in Latin America, CPDP LatAm a virtual side event of the Global Privacy Assembly (GPA)

25–28 October

"A Matter of Balance: Privacy in the Era of Rapid Technological Advancement" and a side event *"The Latin American approach to Model Contractual Clauses: a recipe for free and secure data flows"* Global Privacy Assembly, Istanbul, Türkiye

7–8 November

Data Privacy Global Conference (DPGC) Sao Paulo, Brazil

11 November

Conference "From broadband to a future of 'extended reality'" A panel discussion on "Public policy challenges for privacy in the next decade in Latin America" organised by The Centre for the Study of Technology and Society (CETyS) in Buenos Aires

29–30 November

70th Meeting of the "Berlin Group" – International Working Group on Data Protection in Technology in London, UK

12–16 December

Official county visit to Lithuania

Annex II

The specific sources used to corroborate the information contained in Table 2 are listed below. Countries are listed in alphabetical order.

Argentina

Name of the application or web page	*CUIDAR mobile application and website*
Website	https://play.google.com/store/apps/details?id=ar.gob.coronavirus&hl=en_CO&gl=US https://www.argentina.gob.ar/aplicaciones/coronavirus
Information processing policy of the application and/or website	https://www.argentina.gob.ar/terminos-y-condiciones (Accessed 9 September 2022)
Entity responsible for processing	Office of the Undersecretary for e-Government
Basis for reply to question 1	Unnumbered section of the privacy policy entitled “Finalidad de los datos recolectados”
Basis for reply to question 2	Section of the privacy policy entitled “Información al Usuario titular de los datos personales”, specifically the paragraphs referring to the principle of deletion
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Australia

Name of the application or web page	*COVIDSafe app*
Website	https://www.health.gov.au/resources/apps-and-tools/ covidsafe-app The application has been decommissioned and is no longer in use
Information processing policy of the application and/or website	https://covidsafe.gov.au/privacy-policy-previous.html (Accessed on 4 October 2022)
Entity responsible for processing	Department of Health
Basis for reply to question 1	At https://covidsafe.gov.au/privacy-policy-previous.html, see: “What personal information will be collected, and why is it being collected?”
Basis for reply to question 2	At https://covidsafe.gov.au/privacy-policy-previous.html, see: “How will personal information be stored?”

Name of the application or web page	*COVIDSafe app*
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	In the section of the privacy policy article in Spanish (https://covidsafe.gov.au/decom-translated-privacy-policy/privacy-policy-spanish.html) “¿Qué pasará con mi información?
Basis for reply to question 6	N/A

Belgium

Name of the application or web page	*Coronalert mobile application*
Website	https://coronalert.be/en/
Information processing policy of the application and/or website	https://coronalert.be/en/privacy-and-data/ (Accessed 10 September 2022)
Entity responsible for processing	Sciensano
Basis for reply to question 1	At https://coronalert.be/en/privacy-statement/index.html, see section 3: “What is the purpose of the contact tracing app and how does it work?”
Basis for reply to question 2	At https://coronalert.be/en/privacy-statement/index.html, see section 8: “How long are the personal data kept?”
Basis for reply to question 3	At https://coronalert.be/en/privacy-and-data/index.html#privacy-3, see the sections entitled “Privacy-by-design” and “Transparency-statement” At https://coronalert.be/en/privacy-statement/index.html, see section 8: “How long are the personal data kept?”
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Brazil

Name of the application or web page	*Coronavirus-SUS*
Website	https://play.google.com/store/apps/details?id=br.gov.datasus.coronavirus&hl=en_CO&gl=US
Information processing policy of the application and/or website	https://apps-politica-privacidade.saude.gov.br/ (Accessed 7 September 2022)

Name of the application or web page	*Coronavirus-SUS*
Entity responsible for processing	Ministry of Health
Basis for reply to question 1	At https://apps-politica-privacidade.saude.gov.br/, see: “Para que fim utilizamos seus dados?”
Basis for reply to question 2	N/A
Basis for reply to question 3	N/A
Basis for reply to question 4	The Privacy Policy (https://apps-politica-privacidade.saude.gov.br/) states that: “O site se compromete a cumprir as normas previstas na Lei Geral de Proteção de Dados (…), e respeitar os princípios dispostos no Art. 6º: (…) X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.” (The site undertakes to comply with the rules set forth in the General Data Protection Law (...), and to respect the principles set forth in article 6: (...) X - Responsibility and accountability: demonstration, by the entity, of the adoption of effective measures for verifying that the regulations governing personal data protection have been respected, and of the effectiveness of such measures.)
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Colombia

Name of the application or web page	*CORONAPP mobile application and website*
Website	https://coronaviruscolombia.gov.co/Covid19/aislamiento-saludable/coronapp.html
Information processing policy of the application and/or website	https://coronaviruscolombia.gov.co/Covid19/politica-de-privacidad.html
Entity responsible for processing	Administrative Department of the Office of the President of the Republic
Basis for reply to question 1	Section of the information processing policy entitled “Finalidad del tratamiento al cual serán sometidos los datos personales”
Basis for reply to question 2	Section of the information processing policy entitled “Principios relacionados con el uso de datos personales”
Basis for reply to question 3	Section of the information processing policy entitled “Responsabilidad demostrada (accountability) frente al tratamiento de datos personales”
Basis for reply to question 4	Section of the information processing policy entitled “Responsabilidad demostrada (accountability) frente al tratamiento de datos personales”

Name of the application or web page	*CORONAPP mobile application and website*
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

France

Name of the application or web page	*TousAntiCovid mobile application*
Website	https://www.economie.gouv.fr/tousanticovid#
Information processing policy of the application and/or website	https://bonjour.tousanticovid.gouv.fr/en/privacy/anonimity https://bonjour.tousanticovid.gouv.fr/privacy.html https://tousanticovid.stonly.com/kb/fr/donnees-personnelles-26615 (Accessed 11 September 2022)
Entity responsible for processing	Directorate General of the Ministry of Health and Prevention
Basis for reply to question 1	At https://tousanticovid.stonly.com/kb/guide/fr/mentions-legales-wvfIhEROYq/Steps/129521, see “Finalités et responsable de traitement”. At https://tousanticovid.stonly.com/kb/guide/fr/mentions-legales-wvfIhEROYq/Steps/129514,129518, see “Données personnelles traitées dans l’application TousAntiCovid”
Basis for reply to question 2	At https://tousanticovid.stonly.com/kb/guide/fr/mentions-legales-wvfIhEROYq/Steps/129514,129516 see “Durée de conservation”
Basis for reply to question 3	At https://tousanticovid.stonly.com/kb/guide/fr/protection-des-donnees-w7ZfB4pPai/Steps/129765, see: “Protection des données”, especially the reference to the principle of minimization
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Germany

Name of the application or web page	*CORONA-WARN APP*
Website	https://www.coronawarn.app/en/
Information processing policy of the application and/or website	https://www.coronawarn.app/en/privacy/ https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf (Accessed 6 September 2022)

Name of the application or web page	*CORONA-WARN APP*
Entity responsible for processing	Robert Koch Institute and Federal Government of Germany
Basis for reply to question 1	Paragraph 5: “What data is processed? Paragraph 6: “Why is your data processed?”
Basis for reply to question 2	Paragraph 9: “When will your data be deleted?”
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

India

Name of the application or web page	*AAROGYASETU*
Website	https://aarogyasetu.gov.in/
Information processing policy of the application and/or website	https://www.aarogyasetu.gov.in/privacy-policy/ (Accessed 7 September 2022)
Entity responsible for processing	Designed by the National Informatics Centre (Ministry of Electronics and Information Technology) for the Ministry of Health and Family Welfare
Basis for reply to question 1	See “Consent based registration”
Basis for reply to question 2	N/A
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Ireland

Name of the application or web page	*COVID Tracker App*
Website	https://www.hse.ie/eng/about/who/primarycare/socialinclusion/travellers-and-roma/irish-travellers/covid19-tracker-app.html https://www.covidtracker.ie/

Name of the application or web page	*COVID Tracker App*
	https://play.google.com/store/apps/details?id=com.covidtracker.hse&hl=en_419&gl=US
Information processing policy of the application and/or website	Information processing policy of the application and/or website
Entity responsible for and processing	Health Service Executive and Department of Health
Basis for reply to question 1	At https://www.hse.ie/eng/gdpr/covid-tracker-app/dpin.html, see section 4: “What the app does”
Basis for reply to question 2	At https://www.hse.ie/eng/gdpr/covid-tracker-app/dpin.html, see section 11, entitled “How long your personal data is held for”, section 12, entitled “Data Subject rights” and section 9.2., entitled “Other recipients” See also Department of Health, Data Protection Impact Assessment for the COVID Tracker App, appendix H on Data Retention, 2020. Available at https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%2026.06.2020.pdf
Basis for reply to question 3	At https://www.hse.ie/eng/gdpr/covid-tracker-app/dpin.html, section 14, entitled “Further information”, mentions that an impact assessment has been carried out. This assessment (https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%2026.06.2020.pdf) describes how the minimization principle was implemented in Appendix G, on Data Minimisation. Appendix H, on Data Retention, describes the reasons for the retention of each item of personal data and the measures necessary to ensure compliance with the retention policy described.
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Italy

Name of the application or web page	*immuni mobile application*
Website	https://www.immuni.italia.it/
Information processing policy of the application and/or website	https://www.immuni.italia.it/pn.html (Accessed 10 September 2022)
Entity responsible for processing	Office of the President of the Council of Ministers, Department for Digital Transformation
Basis for reply to question 1	In the privacy policy notice (Informativa privacy) for the application, see the section entitled “Come vengono trattati i

Name of the application or web page	*immuni mobile application*
	tuoi dati personali - periodo di conservazione - base giuridica". In the section on frequently asked questions, see the question: "Come viene tutelata la mia privacy?
Basis for reply to question 2	In the section on frequently asked questions, see the question: "Come viene tutelata la mia privacy?"
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Japan

Name of the application or web page	*COCOA application*
Website	https://play.google.com/store/apps/details?id=jp.go.mhlw.covid19radar&hl=en&gl=US&pli=1
Information processing policy of the application and/or website	https://www.mhlw.go.jp/stf/seisakunitsuite/english_rk_00031.html (Accessed 7 September 2022)
Entity responsible for processing	Ministry of Health, Labour and Welfare
Basis for reply to question 1	At https://www.mhlw.go.jp/stf/seisakunitsuite/english_rk_00031.html, see article 2, "Definitions", para. 10
Basis for reply to question 2	N/A
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Latvia

Name of the application or web page	*Apturi Covid*
Website	https://www.apturicovid.lv/#en
Information processing policy of the application and/or website	https://www.apturicovid.lv/privatuma-politika (Accessed 9 September 2022)

Name of the application or web page	*Apturi Covid*
Entity responsible for processing	Centre for Disease Prevention and Control The Centre for Disease Prevention and Control and the data processing institutions of the European Union member State that use the European Federation Gateway Servce (EFGS) (the common server that allows for data to be exchanged between the different COVID-19-related applications) act as joint controller of data processing in the EFGS
Basis for reply to question 1	In the privacy policy, at https://www.apturicovid.lv/privatuma-politika, see chapter 2, “Purposes of processing data”
Basis for reply to question 2	In the privacy policy, at https://www.apturicovid.lv/privatuma-politika, see chapter 7, “Storage and deletion of data”, and chapter 8, “Receivers of data”
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Mauritius

Name of the application or web page	*beSafeMoris*
Website	https://www.myt.mu/mobile/besafemoris https://play.google.com/store/apps/datasafety?id=mu.mt.healthapp&hl=en&gl=US
Information processing policy of the application and/or website	https://besafemoris.mu/privacy-policy/ (Accessed 9 September 2022)
Entity responsible for processing	It is unclear whether Mauritius Telecom Ltd. (the national telecommunications company) or the Ministry of Health and Wellness is in charge
Basis for reply to question 1	At https://besafemoris.mu/privacy-policy/, see sections entitled “What is the purpose of the App?, “What information does the Application gather and how is it used?” and “Android App Permissions”
Basis for reply to question 2	The State indicates that the data will be deleted, but does not say exactly when At https://besafemoris.mu/privacy-policy/, see the paragraph entitled “Data Retention Policy”
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A

Name of the application or web page	*beSafeMoris*
Basis for reply to question 6	N/A

Mexico

Name of the application or web page	*COVID-19MX mobile application*
Website	https://play.google.com/store/apps/details?id=mx.gob.www&hl=es_CO&gl=US
Information processing policy of the application and/or website	Comprehensive privacy notice for the *COVID19MX* mobile application available at: https://framework-gb.cdn.gob.mx/applications/covid/avisoprivacy.pdf (Accessed 6 September 2022)
Entity responsible for processing	Ministry of Health, through the Office of the Undersecretary for Prevention and Health Promotion
Basis for reply to question 1	Comprehensive privacy notice for the *COVID19MX* mobile application: “Las finalidades del tratamiento de los datos personales recabados son: • Brindar orientación médica a las personas que proporcionaron sus datos para ser contactadas y en su caso atender la situación de emergencia que potencialmente pueda ocasionarse. • [Proporcionar los datos] [e]stadísticos necesarios para que las autoridades sanitarias y epidemiológicas dirijan acciones pertinentes a la enfermedad COVID-19.” (The purposes for which the data collected are processed are: • Providing medical guidance to persons who provided their contact information and, if necessary, responding to any emergency situation that might potentially arise • [Providing the] statistical data necessary for the health and epidemiological authorities to take relevant action in response to the COVID-19 disease)
Basis for reply to question 2	N/A
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Netherlands

Name of the application or web page	*Corona Melder (application switched off temporarily on 22 April 2022)*
Website	https://coronamelder.nl/en/
Information processing policy of the application and/or website	See Privacy Policy, "*CoronaMelder Privacy Statement*", https://coronamelder.nl/en/privacy. (Accessed 9 September 2022)
Entity responsible for processing	The Ministry of Health, Welfare and Sport, in respect of personal data processed in the design and management of CoronaMelder and in the context of European coordination with other notification applications. Together with the designated authorities of other participating countries, the Ministry of Health, Welfare and Sport is the controller of the European Federation Gateway Service (the common server that allows for data to be exchanged between the various COVID-19-related applications) The Municipal Health Service, in respect of personal data gathered through the application in the context of contact tracing
Basis for reply to question 1	At https://coronamelder.nl/en/privacy, see section 2: "For what purpose are personal data processed?"
Basis for reply to question 2	At https://coronamelder.nl/en/privacy, see section 7: "Retention of personal data"
Basis for reply to question 3	At https://coronamelder.nl/en/privacy, see section 2: "Your rights with regard to your personal data", in which it is stated that the application was designed in accordance with the principles of minimization and privacy by design
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

New Zealand

Name of the application or web page	*NZ COVID Tracer*
Website	https://www.health.govt.nz/covid-19-novel-coronavirus/ covid-19-resources-and-tools/nz-covid-tracer-app
Information processing policy of the application and/or website	https://www.health.govt.nz/covid-19-novel-coronavirus/ covid-19-resources-and-tools/nz-covid-tracer-app (Accessed on 4 October 2022)
Entity responsible for processing	Ministry of Health
Basis for reply to question 1	At https://covid19.govt.nz/about-this-site/privacy/, see "Information stays on your phone unless you share it" and Privacy Impact Assessment, para. 25 (https://covid19.govt.nz/assets/reports/COVID-19-contact_tracing_app_privacy-impact-assessment.pdf).

Name of the application or web page	*NZ COVID Tracer*
Basis for reply to question 2	At https://covid19.govt.nz/about-this-site/privacy/, see "Information stays on your phone unless you share it"
Basis for reply to question 3	Privacy Impact Assessment
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Singapore

Name of the application or web page	*Trace Together*
Website	https://www.tracetogether.gov.sg/
Information processing policy of the application and/or website	https://www.tracetogether.gov.sg/common/privacystatement/index.html (Accessed 8 September 2022)
Entity responsible for processing	Ministry of Health
Basis for reply to question 1	At https://www.tracetogether.gov.sg/common/privacystatement/index.html, see "We store limited data"
Basis for reply to question 2	At https://www.tracetogether.gov.sg/common/privacystatement/index.html, see "Data about devices near you is stored on your device"
Basis for reply to question 3	N/A
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

South Africa

Name of the application or web page	*COVID Alert SA mobile application*
Website	https://sacoronavirus.co.za/covidalert/
Information processing policy of the application and/or website	https://sacoronavirus.co.za/covidalert/privacy-policy/ (Accessed 10 September 2022)
Entity responsible for processing	Ministry of Health

Name of the application or web page	*COVID Alert SA mobile application*
Basis for reply to question 1	At https://sacoronavirus.co.za/covidalert/privacy-policy/, see section 3: “Collection and processing of personal data”
Basis for reply to question 2	At https://sacoronavirus.co.za/covidalert/privacy-policy/, see section 6: “How long will data be retained and when will it be destroyed?”
Basis for reply to question 3	At https://sacoronavirus.co.za/covidalert/privacy-policy/, see section 6: “Rights of all app users”, specifically the reference to the “privacy by design” principle
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

Spain

Name of the application or web page	*RADAR COVID mobile application*
Website	https://radarcovid.gob.es/
Information processing policy of the application and/or website	https://radarcovid.gob.es/politica-de-privacidad (Accessed 9 September 2022)
Entity responsible for processing	The Ministry of Health and the Autonomous Communities are responsible for data processing on this application. The General Secretariat for e-administration also processes data on the application.
Basis for reply to question 1	Section 4 the COVID Radar application’s privacy policy entitled “¿Qué datos tratamos sobre ti?”. Section 6 entitled “¿Para qué y por qué utilizamos tus datos?
Basis for reply to question 2	Section 7 of the COVID Radar application’s privacy policy entitled “¿Durante cuánto tiempo conservamos tus datos?”
Basis for reply to question 3	At https://radarcovid.gob.es/preguntas-frecuentes, see sections entitled “Datos personales y privacidad” and “Cómo se protege mi privacidad?
Basis for reply to question 4	N/A
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A

United Kingdom

Name of the application or web page	*NHS COVID-19 app*
Website	https://www.gov.uk/government/collections/nhs-covid-19-app

Name of the application or web page	*NHS COVID-19 app*
Information processing policy of the application and/or website	https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice (Accessed 8 September 2022)
Entity responsible for processing	Department of Health and Social Affairs
Basis for reply to question 1	At https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice, see "Compliance with the Privacy and Electronic Communication Regulations (PECR)"
Basis for reply to question 2	At https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice, see "Retention of data" and "Data the app uses" At https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-our-processing-of-special-categories-of-personal-data, see "Retention and erasure policies" under "Guidance NHS COVID-19 app: our processing of special categories of personal data" At https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028998/NHS_COVID_19_App_DPIA.pdf, see "Retention of data from the app" (Department of Health and Social Care, The NHS COVID-19 app (Early October 2021 release): data protection impact assessment, p. 62)
Basis for reply to question 3	At https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-our-processing-of-special-categories-of-personal-data, see "How we ensure we comply with the Data Protection principles (Procedures for ensuring compliance with the principles)" under "Guidance NHS COVID-19 app: our processing of special categories of personal data" Department of Health and Social Care, "The NHS COVID-19 app (Early October 2021 release): data protection impact assessment". Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028998/NHS_COVID_19_App_DPIA.pdf.
Basis for reply to question 4	At https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-our-processing-of-special-categories-of-personal-data, see "How we ensure we comply with the Data Protection principles (Procedures for ensuring compliance with the principles)" of "Guidance NHS COVID-19 app: our processing of special categories of personal data"
Basis for reply to question 5	N/A
Basis for reply to question 6	N/A