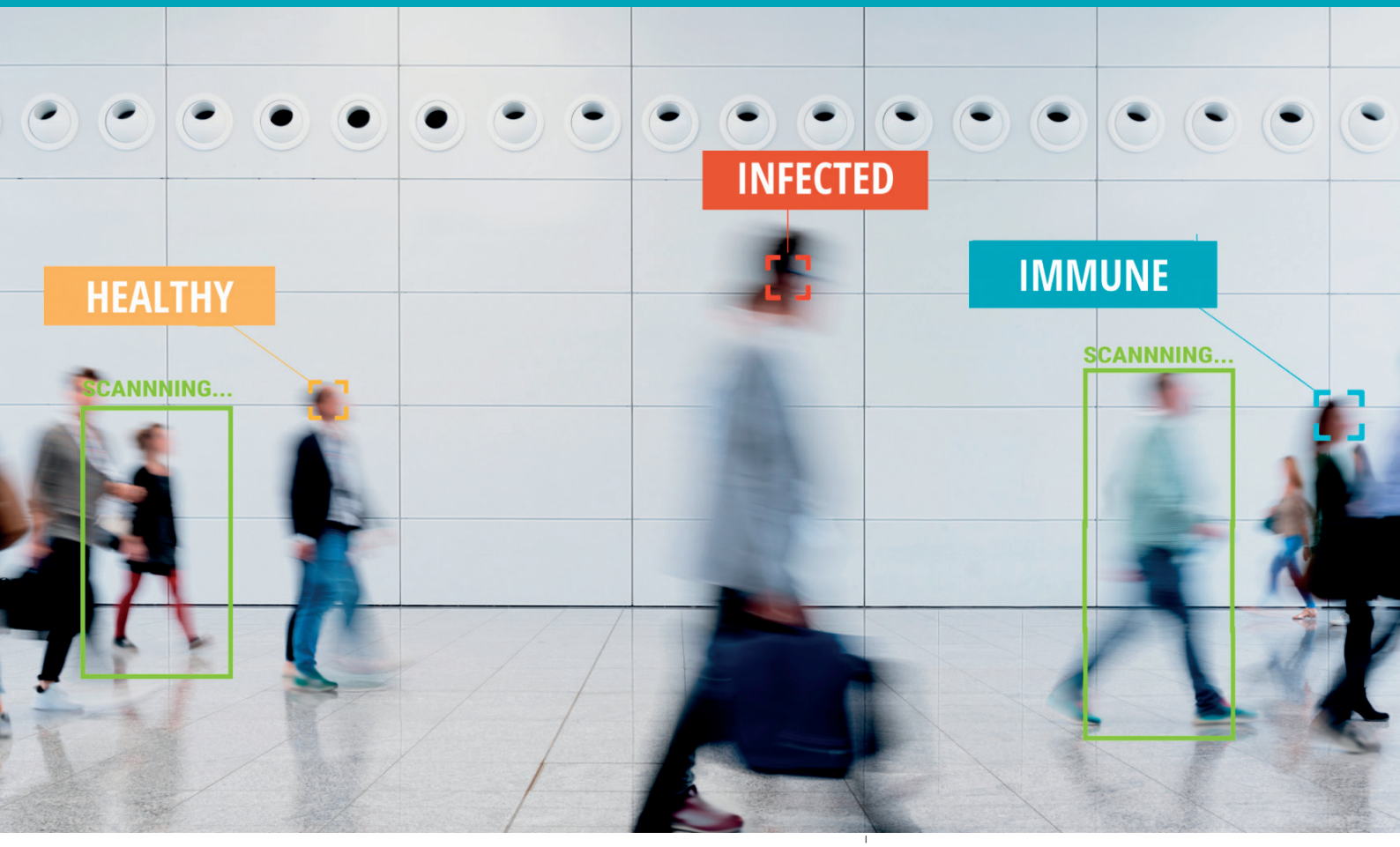
DIGITAL SOLUTIONS TO FIGHT COVID-19



2020 DATA PROTECTION REPORT

October 2020

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DIGITAL SOLUTIONS TO FIGHT COVID-19

2020 Data Protection Report

October 2020

Council of Europe

Cover and layout:
Documents and Publications Production Department (SPDP), Council of Europe

Photo: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Printed at the Council of Europe

Acknowledgments

This report has been prepared by the Data Protection Unit of the Council of Europe on the basis of the extensive work carried out by Anne-Christine Lacoste and Sjoera Nas, data protection consultants.

Table of Contents

Executive summary

2020 marks a turning point.

Challenges faced worldwide by our societies, governments and health care systems have provided a unique opportunity to reaffirm our founding values of democracy, rule of law and human rights.

Confronted with the Covid-19 health crisis, governments have been seeking to protect their populations and responding effectively to urgent and vital needs. Emergency measures have been adopted that have affected the enjoyment of the rights to privacy and data protection. To avoid undermining the bedrock of our societies, such necessary exceptional measures have to respect the general principles of law, remain proportional to the threat they address and be limited in time.

The pandemic has required swift and effective measures, leading to an increased use by governments of digital technologies to fight the spread of the virus, such as mobile applications installed on smartphones (apps), used for various purposes. This increased interest in new technologies has often been accompanied by a shift towards digital solutions offered by the private sector, public authorities working in cooperation with companies of the digital market.

The use of emerging technologies providing distance communication *in lieu* of human contacts, and algorithms replacing human intervention has simply exploded. Digital technologies used in public places to monitor population, at home, while teleworking or self-diagnosing, or when learning remotely became the new 'normal'.

This quantum-leap in the digitalisation of our lives requires that measures adopted by governments during the health crisis uphold the protection of individuals with regard to the processing of personal data. Privacy and data protection have a pivotal role, essential in building and sustaining trust in digital solutions. Those rights are not an obstacle to the protective responses adopted by governments, they are the guarantee that such responses will be taken in full consideration of human dignity and integrity.

Exceptional measures taken by governments must be provided for by law, respect the essence of fundamental rights and freedoms and be necessary and proportionate in a democratic society.

Countries should pay particular attention to the following aspects when using technological tools which process personal data to combat the pandemic:

- the need for a **time limit** (applied to the retention period of all collected personal data) and legal sunset clauses;
- a legally guaranteed **purpose limitation** (the purpose of any processing must be precisely defined, and based on a specific legal basis, with the exclusion of further processing for any other purpose);
- **proportionality** of the measures taken and ongoing assessment of the proportionality considering the effective results of the measures (with the possibility to withdraw the measure where there is no concrete evidence of its benefits);
- cooperation with the **national data protection authority**, at early stages of the design of the processing, as well as at later stages (for example to process the feedback on a data protection impact assessment or an enforcement action);

- **transparency and explainability** of the data processing operations, especially for automated tracing tools (this notably includes the publication of the source code of the software, of impact assessments and security audits);
- **accountability** of data controllers, integration of **privacy by design**, realisation of **data protection impact assessments** of the processing and relevant security measures.

Greater awareness and compliance with those requirements contribute to increase the trust that individuals place in their governments and acceptance of the measures adopted in the general interest.

The role of international fora such as the Council of Europe is essential in recalling the path to take, issuing recommendations and guidance, enabling exchange of information and best practices. Such is the objective of the present report, to provide insights on what a significant number of countries have done to fight the pandemic, and how this complies with the applicable standards.

The manner in which the health crisis has been addressed prompts a reaffirmation of the resilience of the data protection principles as a key component of the effective functioning of our democracies. The future lies in our capacity to react promptly to new challenges without undermining our core values and putting our societies at greater risk on the longer term than do the present threats we have to address.

Introduction

2020 brought immense challenges to our societies. Governments had rapidly and effectively to respond to the exceptional and evolving situation linked to the Covid-19 pandemic.

The impact on human rights and fundamental freedoms of measures taken to curb the spread of the virus represents both a challenge to the resilience of data protection principles and an opportunity to test such resilience.

In respect of data protection, the digitisation of our societies has also been considerably accelerated by the crisis and the isolation imposed, which required many of us to work, to learn and to socialise at a distance.

This report gives an overview of the data protection landscape in that specific context of 2020, in the countries parties to the Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (hereafter "Convention 108").

55 states[1] are parties to Convention 108, which has recently been modernised in order to adapt this landmark instrument to the new realities of an increasingly connected world, and to strengthen the effective implementation of the Convention. The Protocol[2] amending Convention 108 was opened for signature on 10 October 2018 in Strasbourg (CETS No. 223) and has since been signed and ratified by numerous countries to bring this modernised instrument, "Convention 108+", rapidly into force.

2020 brought another important change to the enforcement of the right to data protection in the field of transatlantic international data transfers, with the invalidation of the "Privacy shield" agreement concluded between the European Union (EU) and the United States of America (USA). The decision of the Court of Justice of the EU will affect international data flows and negotiations beyond the sole EU-USA scope and once again highlights the importance of Convention 108+ at a global level[3].

This report[4] contains two parts. The first part provides an overall analysis of legislative and key developments and their impact on the fundamental rights to privacy and data protection. The second part provides an in depth and technical review of the use of digital contact tracing applications and monitoring tools. The report contains an assessment of the main findings, with recommendations on how to ensure efficiency and resilience of the data protection framework.

The changes to the legal framework, governmental decisions, reactions of the private sector and the civil society are assessed against the principles of Convention 108. When the new principles of Convention 108+ are taken as a reference, such as the principles of accountability, privacy by design and by default, this is specifically mentioned in the report. Indeed, while Convention 108+ has not yet entered into force, its new principles represent a relevant reference for all current parties to Convention 108 (including parties that are members of the EU and already bound by equivalent provisions in accordance with the data protection legal framework of the EU).

1. List of countries available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
2. Text of Convention 108+ available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
3. Also see the Joint Statement of 7 September by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe on " Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services" at https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb
4. The present report takes into account positions and statements of the main oversight bodies and institutions at regional and international level, including the Council of Europe, the Fundamental Rights Agency of the EU and the European Data Protection Board, the Global Privacy Assembly, the World Health Organisation and the OECD, as well as reliable sources of information including academic work on constitutional matters, civil society publications and recent jurisprudence. It also relies on the replies to a questionnaire sent to parties to Convention 108 on data protection and the use of digital tools in the context of Covid-19.

I. Legal analysis of the legislative developments

Governments have been facing difficult challenges in seeking to protect their populations from the threat of Covid-19. This could alter the regular functioning of democratic societies and lead to measures which could infringe upon on rights and freedoms.

Convention 108+ allows the lawful use by governments of exceptions without necessarily having to adopt emergency measures (which include exceptional derogations). However, such exceptions must be provided for by law, respect the essence of fundamental rights and freedoms and be necessary and proportionate in a democratic society.

> "Data protection can in no manner be an obstacle to saving lives and [..] the applicable principles always allow for a balancing of the interests at stake."
>
> "Data protection standards are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health, it is crucial to ensure that the necessary data protection safeguards are implemented when adopting extraordinary measures to protect public health." [5]

If it is necessary to go beyond those rules, a special law or decree in compliance with constitutional principles is required. However, the sole requirement of legal certainty does not guarantee that such derogations to individual rights are necessary and proportionate. Indeed, emergency measures have to comply with other specific requirements. In particular, any measure must be necessary and meet an important objective of public interest, and the essence of individual fundamental rights must be preserved, especially the rights of access, opposition and deletion of data[6].

A. Emergency measures

Due to the pandemic, most countries parties to Convention 108 have adopted emergency measures which restrict fundamental rights, based on the possibilities afforded by their own legal system.

Three main approaches can be identified:

- adoption of general emergency measures giving the government special powers (notably based on laws or decrees, in application of constitutional law);
- adoption of emergency measures in specific sectors, often based on public health or pandemic regulations;
- adoption of emergency measures without a specific legislative basis.

These different approaches have led to a patchwork of provisions in the 55 countries parties to Convention 108. Most provisions give extensive power to the governments, though usually only for a limited period of time.

Nine parties to the European Convention on Human Rights (ECHR) made use of Article 15 of the ECHR on derogation in time of emergency: Albania, Armenia, Estonia, Georgia, Latvia, North Macedonia, Romania, San Marino, and Serbia[7]. Such derogations must have a clear basis in domestic law in order to protect against arbitrariness and must be strictly necessary to the public emergency, in this case, fighting against the pandemic.

5. Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter
6. The guidance provided by the EDPB with regard to the GDPR is equally relevant and valid in the context of Convention 108 : EDPB statement on the restrictions to data subjects rights in connection to the state of emergency in Member States, 2 June 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/autre/statement-restrictions-data-subject-rights-connection-state_en.
7. Reservations and Declarations for Treaty No.005 - Convention for the Protection of Human Rights and Fundamental Freedoms, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/declarations

Measures range between national ones based on emergency processes clearly defined (where there is more transparency and legal certainty) and local or regional measures taken by local authorities. Whichever approach applies, the degree of intrusiveness of the measures adopted and their impact on individuals has in any case to be assessed.

The principles governing a state of emergency have been identified by the Venice Commission[8] and clarified in the toolkit published by the Secretary General of the Council of Europe[9], as follows:

- overarching principle of the Rule of Law
- necessity
- proportionality
- temporariness
- effective (parliamentary and judicial) scrutiny
- predictability of emergency legislation
- loyal co-operation among state institutions

Measures such as mandatory quarantines and lockdowns limiting the freedom of movement may be necessary to combat the Covid-19. However, it seems from available reports and in particular the report of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe and the Bulletins of the Fundamental Rights Agency of the EU[10] that some of those measures do not always comply with these principles.

Even though such measures can be highly invasive and constitute important limitations to fundamental rights (privacy, data protection but also freedom of movement and assembly, and in some cases freedom of speech), the necessary oversight by supervisory authorities, parliaments and courts has sometimes been missing. Some constitutional courts have already issued rulings on some measures[11]. Other courts were prevented from fulfilling their role[12].

How emergency measures have impacted more specifically the rights to data protection and privacy, and especially the principles of Convention 108 and Convention 108+, depends on the nature of the measures adopted (secondary laws, decrees, decisions), their implementation and on the effectivity of oversight, including the judiciary and the supervisory authorities.

B. Analysis of the impact on specific provisions of Convention 108 and Convention 108+

1. Legal basis

Article 5 of Convention 108+ provides that the processing of data can be carried out on the basis of the "free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law", which, according to the explanatory report to the Convention[13], includes processing « necessary for the protection of the vital interests of the data subject or of another person, (…) for compliance with a legal obligation to which the controller is subject, and data processing carried out on the basis of grounds of public interest or for overriding legitimate interests of the controller or of a third party. »

As clearly recalled by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe in their joint statement of 30 March 2020[14], the catalogue of legal bases is broad

8. Reflexions on Respect for Democracy, Human Rights and the Rule of Law during States of Emergency, Venice Commission, available at https://rm.coe.int/respect-for-democracy-hu-man-rights-and-rule-of-law-during-states-of-e/16809e82c0
9. Council of Europe toolkit on respecting the rule of law in state of emergency, available at https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40
10. The impact of the Covid-19 pandemic on human rights and the rule of law, Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, available at https://pace.coe.int/en/files/28679
11. In the **Czech Republic**, although the Constitutional Court invoked a lack of competence to review the declaration of a state of emergency, it did annul some specific measures of the Ministry for Health. In **Romania**, the Constitutional Court annulled the quarantine rules adopted by the government as according to the Court, this limitation of the freedom of movement should have been based on a law adopted by the Parliament.
12. In **Hungary** for instance, ordinary courts were closed thus preventing the Constitutional Court review of the proportionality of measures introduced under emergency conditions as this procedure could solely be initiated by ordinary courts.
13. Explanatory Report, paragraph 46.
14. Joint Statement of 30 March on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter

enough to cover various data processing activities developed in the context of the Covid-19 crisis. Besides consent and necessity to process data based on the public interest, the vital interest of the data subject and of others can in particular cases be invoked to justify data processing for the purpose of monitoring of a life-threatening epidemic.

While the processing of data in the context of the fight against the pandemic can find its legitimacy in the Convention, the exceptional circumstances related to the vital threat and the public interest call at national level for additional and more specific regulation to ensure compliance with the principle of legal certainty. Such regulations should define the scope and purpose of the intended data processing.

Legal basis: legal obligation and public interest

Processing of personal data without a specific and appropriate legal basis has been denounced in particular by academia and civil society concerning a number of emergency responses adopted in some countries.

In **Greece** and in **France**, the use of drones triggered such concerns and legal action. In Greece, an NGO highlighted that the deployment of drones was based on a law which did not include any specific data protection guarantees and did not explicitly refer to the data protection legislation[15]. In France, two NGOs brought an action before the Conseil d'État. They flagged the absence of an explicit legal framework for the use of drones over Paris to monitor people's movement during and after the lock-down period. The Conseil d'État ordered the government to immediately cease the surveillance[16].

Though most countries parties to Convention 108 have made the use of Covid-19 mobile phone applications (apps) voluntary, this is not the case for isolation containment apps. In **Russia**[17] and **Turkey**[18], use of isolation containment apps is mandatory. **Slovenia**[19] appears to be the only country party to Convention 108 that has made the use of a proximity and contact tracing app mandatory by law, while subsequently announcing that its use would be on a voluntary basis.

Countries may invoke the legal basis of public interest with reference to health law provisions to contain a pandemic, or general provisions allowing regional authorities to maintain order. This ground has been invoked by countries that have introduced mandatory temperature scans at borders, airports, and public places or mandatory registration of contact data for visits to cafés and restaurants for the purpose of contact tracing. However, in order to successfully invoke this legal basis, there must be a very close link between the law and the public interest purpose, and the country must ensure that the processing is strictly necessary for this purpose.

A specific legal basis is essential to enable a public authority to process personal data for a determined purpose. Additional benefits of separate legislation, aside from due parliamentary process and legal certainty, are the possibility to introduce a sunset clause, as well as a legal requirement to obtain advice from the data protection authority, a legal obligation to conduct a data protection impact assessment and a requirement to implement appropriate data protection safeguards.

Use of telecommunications data requires specific attention. Telecommunications data are not only protected by general data protection law but also by specific regulations guaranteeing confidentiality of communications (constitutional protections of telecommunication secrecy). Even the mandatory processing of aggregated – and thus anonymous – data requires detailed legislation, since the creation of such statistics first requires an intervention from the telecom operators to process individual location data, for a purpose which is not part of their initial competence. In view of the data protection risks for individuals, countries cannot merely rely on the ground of public interest without specific legislation. This explains why a number of parties to Convention 108 adopted or amended existing telecommunication regulations, in order to allow for a wider processing of telecommunication data to create statistics.

15. Coronavirus pandemic in the EU – Fundamental Rights Implications – Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
16. Conseil d'État, Order of 18 May 2020, n° 440442, 440445, available at https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones
17. https://www.mos.ru/news/item/73074073/ See also Human Rights Watch, Russia: Intrusive Tracking App Wrongly Fines Muscovites, available at https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites
18. In Turkey, the app is mandatory for those diagnosed with Covid-19. Virus case tracking app launched in Turkey, Daly News, 19 April 2020, available at https://www.hurriyetdailynews.com/virus-case-tracking-app-launched-in-turkey-154005
19. Slovenian PM calls for mandatory coronavirus app against Commission advice Samuel Stolton, Euractiv, 8 July 2020, available at https://www.euractiv.com/section/digital/news/slovenian-pm-calls-for-mandatory-coronavirus-app-against-commission-advice/

Legal basis: consent

While consent is one of the possible lawful basis to process personal data, the requirements for consent to be valid are hard to meet, especially in view of the sensitivity of health and location data and in the Covid-19 circumstances, the pressure to accept processing due to the exceptional pandemic context. In the employment and educational context, consent is not considered as an optimal legal basis as, due to the imbalance of power, it is difficult to assess if it is freely given. In such circumstances, the legal obligations of the employer or the public interest obligations of educational institutions would be a more suitable ground, as suggested by the European Data Protection Board (EDPB) in its statement[20] on the pandemic. The inadequate use of consent was also pointed out by the data protection authority of **Slovenia** in the context of a legislative proposal concerning the processing of telecommunication data. This led to the withdrawal of the proposal before the law was adopted[21].

2. Purpose limitation, storage and sharing of data

Article 5.4.b) of Convention 108+ provides that personal data should be "collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes". Further use is not forbidden *per se*, and its compatibility with the original purpose depends on the details of the processing and the context. Further use of health data for scientific research, often based on coded or anonymised data, will not trigger the same limitations as their use in order to control individuals' movements or impose sanctions.

Compliance with this principle appears to be one of the major challenges in the context of the Covid-19 crisis. Confronted with an unknown and constantly evolving situation, some governments have adopted broad regulations giving them an extensive margin of manoeuvre.

It follows from reports[22] and replies to the questionnaire developed in part II, that boundaries between health care and police enforcement purposes have been sometimes blurred. In **Slovenia**, **Greece** and **Hungary**, health authorities share patients' lists with the police and other enforcement authorities. In **Austria**, mayors have access to some patients' data as they are in charge of providing food and services to those in quarantine. In the **Netherlands**, the municipal healthcare service has to report infection cases to the mayor of the municipality in which the patient resides as well as to the regional safety authority, with a view to allow the adoption of measures such as mandatory quarantine for those infected[23].

In **Hungary**, the Minister for Innovation and Technology as well as an operational body consisting of representatives of the Ministry of Interior, the police, and health authorities, are entitled by decree[24] to acquire and process any kind of personal data from private or public entities, including traffic and location data from telecommunication providers, with a very broad definition of the purpose for which data can be used. The decree also requires medical and health care universities and high schools to transfer students' data to the police, to fulfil the urgent need for extra public health staff. In **Denmark**, an executive order[25] first foresaw broad access by the police and the Danish Patient Safety Authority to personal data including bank transfers and communication data, before its scope was narrowed.

Some countries have published data on patients or deceased persons. Even if such data were presented as anonymised, published details such as age, gender, combined with location in regions with a low population density, enabled reidentification and further use. In **Montenegro**[26], directly identifiable data were published,

20. Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/ edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf
21. Statement of the Slovenian data protection authority of 20 March 2020, available at https://www.ip-rs.si/novice/epidemija-ne-sme-biti-razlog-za-ukinitev-ustavnih-pravic-1178/
22. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1 , Country reports - Coronavirus COVID-19 outbreak in the EU - Fundamental Rights Implications - April 2020 - Country research, available at https://fra.europa.eu/en/country-data/2020/coronavirus-covid-19-outbreak-eu-fundamental-rights-implications-april-2020
Recommendations on privacy and data protection in the fight against Covid-129, Access Now, March 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf
23. See details at the Dutch National Institute for Public Health and the Environment, available at https://www.rivm.nl/
24. Governmental Decree no. 46/2020 on prevention, avoidance of the mass human disease threatening the safety of human health and property, and on the measures taken in the state of danger in order to protect the health of the Hungarian citizens (III.) (*46/2020. (III. 16.)*, 16 March 2020, Article 13, available at http://njt.hu/cgi_bin/njt_doc.cgi?docid=218547.380736.
25. Bekendtgørelse om oplysningsforpligtelser samt behandling af personoplysninger med henblik pa˚ hindre udbredelse og smitte i forbindelse med håndtering af Coronavirussygdom 2019 (COVID-19), 30 May 2020 available at https://www.retsinformation.dk/eli/lta/2020/746 .
26. Montenegro publishes personal data of persons in isolation, 27 March 2020, available at https://privacyinternational.org/examples/3576/montenegro-publishes-personal-data-persons-isolation

with the full name of the infected persons. The same issue was raised in the **Czech Republic**[27], **Slovakia**[28], **Portugal**[29], **Romania**[30], and **Hungary**[31].

The duration of the storage of data is often unclear, especially when data are made public or are shared with several health or police entities. This issue was raised in **Greece**, on data related to quarantined persons. Even if few coercive measures were taken in this country, civil society expressed concern that the retention periods and further processing of personal data were not sufficiently clarified[32]. In the **United Kingdom**, the Coronavirus Act[33] foresees that the Secretary of State may make regulations to extend the time that biometric samples such as DNA and fingerprints may be retained for national security.

Data collected by tracing apps benefit, in the vast majority of parties to Convention 108, of a limited duration of storage: in the countries that use decentralised contact and proximity tracing apps, data are generally deleted after two weeks.

3. Proportionality

The intrusive character of measures adopted during the pandemic is at the core of reactions by many actors including data protection authorities, parliaments, courts and the civil society. The "fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake" foreseen in Article 5 of Convention 108+ has been assessed in different contexts.

Measures that cannot achieve their intended purpose can never be considered proportionate. However, the real effectivity of many measures has yet to be tested and examined, and debates regarding the proportionality of the interference with the right to data protection, in light of the evidenced and actual efficiency of the measure adopted are still underway.

In **Norway**, the data protection authority required suspension of the contact-tracing app because of the low number of downloads. This low number had an essential impact on the effectiveness of the tool, and the authority decided in an order of 12 June 2020 that the balance between privacy and necessity of the measures did not justify the processing of data, which had to be deleted[34]. In the **United Kingdom**, the government initially suspended the further development of its own proximity tracing app, after an extensive test on the Isle of Wight showed that only one person was notified through the app out of the 55 000 people that had installed it. It also revealed that the app could only correctly identify contacts on Android phones 75% of the time, and 4% of the time on iPhones. On 24 September 2020, the government launched a revamped version of the proximity tracing app, based on the Google Apple Exposure Notification System.[35]

Measures can also be disproportionate if their impact on the private life of individuals is too high. In **France**, the scope of the envisaged measures led to a reaction of the Senate: the emergency law project proposed an amendment[36] to permit, for a period of six months, "any measure" to allow the collection and processing of health and location data to deal with the COVID-19 epidemic. The degree of intrusion of the measure in the fundamental right to privacy was the reason for its rejection[37]. The State Data Protection Inspectorate of the Republic of **Lithuania** imposed a temporary limitation on the processing of personal data in the "quarantine" mobile app. for the possible breaches of Articles 5 (2) of the General Data Protection Regulation (GDPR)

27. *Prima*, Jonah experienced hatred on the Internet because he is infected with coronavirus, 25 March 2020, available at https://prima.iprima.cz/koronavirus-sars-cov-2/jonas-zazil-nenavist-na-internetu-protoze-je-nakazeny-koronavirem
28. Coronavirus COVID-19 outbreak in the EU, Fundamental Rights Implications, Country report, Slovakia, 4 May 2020, available at https://fra.europa.eu/sites/default/files/fra_uploads/sk_report_on_coronavirus_pandemic-_may_2020.pdf
29. Coronavirus COVID-19 outbreak in the EU, Fundamental Rights Implications, Country report, Portugal, 23 March 2020, available at https://fra.europa.eu/sites/default/files/fra_uploads/portugal-report-covid-19-april-2020_en.pdf
30. Coronavirus COVID-19 outbreak in the EU, Fundamental Rights Implications, Country report, Romania, 23 March 2020, available at https://fra.europa.eu/sites/default/files/fra_uploads/romania-report-covid-19-april-2020_en.pdf
31. Jogsértő Listát Közölt az Állam A Koronavírus Áldozatairól, 31 March 2020, available at https://tasz.hu/cikkek/jogserto-listat-kozolt-az-allam-a-koronavirus-aldozatairol
32. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
33. Coronavirus Act 2020, available at https://www.legislation.gov.uk/ukpga/2020/7/section/24/enacted
34. Order of the Norwegian data protection body of 12 June 2020, available at https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/midlertidig-stans-av-appen-smittestopp/
35. Digital Health, NHS Covid-19 contact-tracing app to be launched in England and Wales, 11 September 2020, https://www.digitalhealth.net/2020/09/nhs-covid-19-contact-tracing-launch-england-wales/
36. Amendement au Projet de loi, *Faire face à l'épidémie de Covid-19 - PJL*, available at: http://www.senat.fr/amendements/commissions/2019-2020/376/Amdt_COM-57.html
37. http://www.senat.fr/amendements/commissions/2019-2020/376/Amdt_COM-57.html and OECD Policy Responses to Coronavirus (COVID-19) - Ensuring data privacy as we battle COVID-19, available at http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/

of the EU[38]. In **France** again, the Conseil d'État acknowledged the claim of the French Human Rights league and ordered the suppression of thermal cameras in a school, as their use was considered disproportionate in respect of the right to privacy right of children[39].

In many parties to Convention 108, the measures taken in order to allow a wider processing of telecommunication data triggered specific reactions. According to Article 8 of the ECHR, they benefit from a specific protection under the principle of secrecy of correspondence and communications. The role of parliaments, and especially opposition groups, is visible in several instances. Some proposed measures were either stopped before adoption of the law or contested, in a few cases, before the constitutional courts.

In **Slovakia**, some members of the parliament filed a constitutional complaint against the telecommunications law allowing for access to telecommunications data for Covid-19 purposes, arguing that the scheme disproportionately infringed the rights of data subjects, and did not provide a robust control mechanism against possible misuse of the data. This has led the Constitutional Court to suspend[40] part of the measure before adopting its final decision[41]. A similar action was launched by members of parliament before the Constitutional Court of **Bulgaria** against rules allowing health and police authorities to use location data to track individuals, for violation of the right to privacy and the confidentiality of correspondence[42].

In **Croatia**, amendments foreseen in the Electronic Media Act[43] to track cell phones with a view to protect national and public security were blocked in the legislative process by amendments of the opposition[44].

In **Germany**[45] and **Slovenia**[46], a strong reaction from the data protection authorities led to a withdrawal of measures foreseeing wide processing of telecommunications data (and especially location data) to trace persons at risk, while in **Denmark**, human rights and tech associations raised strong concerns about the intrusiveness of the tracking of individuals with location data[47].

4. Security measures

Protecting data against unlawful access is all the more important considering the sensitive character of most of the data collected in response to the health crisis. Both data protection authorities and civil society have played a crucial role in verifying and reinforcing the security of the proposed digital solutions.

The Information Commissioner of **Slovenia** for instance identified, further to numerous complaints, security weaknesses on the website processing self-reported health data, and especially a lack of proper encryption. The website operators had to suspend the online activities of the site until the necessary improvements were brought to the system, including a privacy impact assessment[48].

In **Austria**, the source code of the contact-tracing app was reviewed by independent research organisations.[49] They identified weaknesses and inspired the developer to adapt the application.

38. Decision of the Lithuanian Data Protection Inspectorate of 25 June 2020, available at https://vdai.lrv.lt/lt/naujienos/nurodyta-laikinai-sustabdyti-programele-karantinas-del-galimai-netinkamo-asmens-duomenu-tvarkymo
39. Caméras thermiques à Lisses : le juge des référés ordonne de mettre fin à leur usage dans les écoles, available at https://www.conseil-etat.fr/actualites/actualites/cameras-thermiques-a-lisses-le-juge-des-referes-ordonne-de-mettre-fin-a-leur-usage-dans-les-ecoles
40. Decision of the Constitutional Court of Slovakia of 13 May 2020, PL. ÚS 13/2020-103, available at https://www.ustavnysud.sk/documents/10182/1270838/PL_+US+13_2020+-+Rozhodnutie+-+Uznesenie+z+predbezneho+prerokovania.pdf/464a47b6-66b4-4545-9a9f-eb0f10b4bd80
41. Slovakia: Change of Government under COVID-19 Emergency, Slavomíra Henčeková, Šimon Drugda, 22 May 2020, available at https://verfassungsblog.de/slovakia-change-of-government-under-covid-19-emergency/
42. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
43. Amendments to the Electronic Media Act, available at https://vlada.gov.hr/UserDocsImages/2016/Sjednice/2020/O%C5%BEujak/216 sjednica VRH/216 - 3.docx
44. Croatia's Response to COVID-19: On Legal Form and Constitutional Safeguards in Times of Pandemic, Nika Bačić Selanec, 9 May 2020, available at https://verfassungsblog.de/croatias-response-to-covid-19-on-legal-form-and-constitutional-safeguards-in-times-of-pandemic/
45. Statement of the Federal German data protection authority of 23 March 2020, available at https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_Novelle-InfektionsschutzG-Bundestag.html?nn=5217016
46. Statement of the Slovenian data protection authority of 30 March 2020, available at https://www.ip-rs.si/novice/epidemija-ne-sme-biti-razlog-za-ukinitev-ustavnih-pravic-1178/
47. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
48. Decision of the Slovene data protection authority of 3 April 2020, available at https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1503
49. Report on the findings of the organisations available at https://noyb.eu/en/report-red-cross-corona-app-reviewed-noyb

5. Transparency

Data controllers have the obligation under Article 8 of Convention 108+ to inform data subjects about several aspects of the processing, including their identity, the legal basis and purpose of the processing, the categories of data processed, recipients and the means for data subjects to exercise their rights.

In several parties to the Convention, data protection authorities insisted on the need to clearly inform individuals about the collection and processing of their data. This was the case in **France**, where the CNIL called for clear information about the functioning of the Covid tracing app and the conditions of deletion of data[50]. The lack of adequate information of data subjects was also flagged in **Hungary**, on how and for what purposes traffic and location data are processed, and in **Romania**, about the geo-tracking of people in quarantine[51].

As shown in more detail in the second part of this report, 20 countries actively published the source code of their apps. This transparency represents a significant and highly welcome change compared to the existing practice of software development.

6. Rights of the data subjects

Data protection authorities and regional bodies such as the EDPB and the Chair of the Committee of Convention 108[52] have urged to respect the rights of individuals in a context where many intrusive measures were being considered or adopted. In practice however, the exercise of rights such as the right of access or opposition as foreseen under Article 9 of Convention 108+ can be difficult for the data subjects. In some instances, these rights have even been formally restrained.

In **Ireland**[53] and in the **United Kingdom**[54], the data protection authorities formally expressed understanding for the position of data controllers who face time constraints due to the crisis and may be unable to reply to access requests within legal deadlines. While recalling that those deadlines are set by law, the authorities announced that, when examining claims of individuals, they would take into account extenuating circumstances or compelling public interests to the benefit of data controllers. The **British** Information Commissioner added however, that it would take a strong regulatory approach against organisations taking advantage of the health crisis to breach data protection laws.

Hungary on the other hand has formally limited individuals' fundamental rights by the decree 179/2020 of 4 May 2020. The government has adopted derogations to the GDPR, allowing data controllers involved in Covid-19 related data processing to suspend the fulfilment of data subjects' requests under Articles 15-22 of the GDPR, such as the right of access or erasure, until the state of emergency is revoked[55]. This has triggered several concerned reactions, including by the EDPB[56].

7. Automated decision making and use of AI

Article 9 of Convention 108+ protects individuals against automated decision making. It provides for the right "not to be subject to a decision significantly affecting (them) based solely on an automated processing of data without having (their) views taken into consideration". Data subjects also have the right to obtain knowledge of the reasoning underlying data processing applied to them.

In the context of the pandemic, this provision protects individuals against automated decisions affecting them directly, which would be based on personal data gathered by apps and other e-devices. The principle would apply, for instance, to immunity passports projected or developed in some countries such as **Argentina**,

50. Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », available at https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid
51. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
52. Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter
53. Covid 19 and Subject Access Requests, 25th March 2020, available at https://www.dataprotection.ie/en/covid-19-and-subject-access-requests
54. The ICO's regulatory approach during the coronavirus public health emergency, 13 July 2020, available at https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf
55. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
56. EDPB response to NGOs on Hungarian decrees and statement on Article 23 GDPR, 3 June 2020, available at https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en

Germany and **Italy**[57], as long as they use health data of users to automatically decide on their freedom of movement. The purpose of such "immunity passports" or "risk-free certificates" would be to enable individuals to travel or to return to work assuming that they are protected against re-infection, based on the detection of antibodies. The World Health Organisation (WHO) has however warned that "there is currently no evidence that people who have recovered from COVID-19 and have antibodies are protected from a second infection"[58] which raises doubts regarding the reasoning underlying the decision-making process and the validity of automated decisions taken by an app or a passport on such basis.

The same issues arise when AI is used in digital contact tracing apps, notably to help to calibrate the assessment of the risk of contamination, which may be questionable as without clear understanding of the contamination patterns, the construction of relevant mathematical models cannot be guaranteed.

In response to the questionnaire, **Croatia**, **Portugal**, **Morocco**, **Tunisia** and the **Slovak Republic** have indicated the use of AI in such apps.

8. Accountability, privacy impact assessment, privacy by design and by default

Convention 108+ includes new accountability obligations for data controllers in its Article 10. Among those is the obligation to make a specific assessment of the impact of a data processing activity on the fundamental rights of the data subjects. Including privacy by design and privacy by default in digital solutions developed to fight the pandemic is another essential element of the data protection framework.

The development of specific applications will be examined in more detail in the second part of this report, but some positive examples are worth mentioning here. Some governments have involved independent actors with an oversight role at an early stage of their actions and have shared the required impact assessments.

In **Finland** for instance, a parliamentary working group on information policy[59] was involved in the identification of data protection and privacy requirements before the contact tracing app was developed. Further to heavy criticism by the **Slovenian** data protection authority, a web-based project relying on self-reporting that enabled individuals to report symptoms, recovery and other Covid-19 related information, was suspended and put offline as long as the data protection impact assessment was not completed further to the authority's instructions[60].

In **France**, **Belgium**, **the Netherlands**[61] and **Italy** notably, data protection authorities were consulted prior to the development of a contact-tracing app[62], which sometimes led to substantial changes to the design of the application.

Privacy by design is also a key asset used by governments in their reflexions on whether to set up centralised or decentralised tracing apps. In their second joint statement[63] on digital contact tracing, the Chair of the Committee of Convention 108 and the Council of Europe Data Protection Commissioner considered that "digital contact tracing systems should be based on an architecture which relies as much as possible on the processing and storing of data on devices of the individual users". While no system can protect completely against security vulnerabilities and risks of re-identification, centralised storage presents more risks of further misuse of data than a decentralised system. Of the 55 countries parties to Convention 108, 14 have chosen such a centralised approach for proximity and contact tracing apps, while 26 countries have chosen a decentralised approach. In addition, 5 countries do not plan to use apps at all. Part II of the report describes in more detail the choices made by parties to Convention 108.

57. Covid-tech, the sinister consequences of immunity passports, Ella Jakubowska, EDRI, 10 June 2020, available at covid-tech-the-sinister-consequences-of-immunity-passports
58. Immunity passports in the context of Covid-19, scientific brief, WHO, 24 April 2020, available at immunity-passports-in-the-context-of-covid-19
59. The webpage of the parliamentary working group is available at https://tietopolitiikka.fi/en/members/
60. Decision of the Slovene data protection authority of 3 April 2020, available at https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1503
61. Dutch DPA, Privacy corona-apps not demonstrated (in Dutch only), available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-corona-apps-niet-aangetoond
62. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 47, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
63. Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 28 April 2020, available at https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7

9. Transborder data flows

The importance of reliable data analytics and benefits of sharing of data in the common efforts of both governments and private sector actors worldwide to combat the pandemic is striking. In that context, the application of transborder data flows regimes implies that personal data transferred from the jurisdiction of a party to Convention 108 continues to be appropriately protected wherever it flows.

Derogations exist, which require a case-by-case approach for each specific transfer that would be made outside the jurisdiction of parties to the Convention.

International transfers could for instance rely on the explicit, specific and free consent of the data subject who has been informed of risks arising in the absence of appropriate safeguards or on the basis of prevailing legitimate interests, in particular important public interests such as public health imperatives, where this is provided for by law and constitutes a necessary and proportionate measure.

Convention 108+ in its Article 14 and with the other principles it lays down protects the individuals while providing a framework for international data flow, which is even more acute and relevant in the context of Covid-19.

10. Enforcement and sanctions

Convention 108+ foresees in its Article 15 supervisory powers for data protection authorities, including the right to impose administrative sanctions and to engage in legal proceedings "or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention".

While supervisory authorities have been very active in issuing statements and recommendations, and also in accompanying governmental decisions in several instances, few coercive decisions have been taken[64]. This may be explained by the exceptional context and the option taken by most authorities to avoid antagonising the right to data protection and public health interests which may have led, in a crisis and emergency context, to disproportionate responses.

Civil society and NGOs[65] have been very active in triggering enforcement actions before courts.

C. Specific legislation and processing of personal data

Governments have adopted secondary legislation or amended existing laws in order to facilitate the management of the health crisis, touching upon the health sector but also the telecommunications sector.

The following practices have been permitted by legislative measures:

- use of mobile phone applications, for different purposes;
- use of traffic and location data from mobile phones and apps;
- use of other technical tools (eBracelets, smart cameras allowing for facial recognition, thermal scans, remote control by drones and robots, mandatory testing).

Few of these measures were adopted after completion of the appropriate legislative procedure, including parliamentary scrutiny. In many other cases no specific legal basis was considered necessary.

1. Mobile applications

The use of mobile apps has been one of the main technologies used by governments and companies to contain the pandemic and serving many different purposes. Although most countries developed apps to aid proximity and contact tracing, some other countries invested efforts in apps aimed at fulfilling other purposes.

64. See as one of the few examples, the order of the Norwegian supervisory authority to suspend the Covid tracing app: Order of the Norwegian data protection body of 12 June 2020, available at https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/midlertidig-stans-av-appen-smittestopp/
65. Such as the French action brought by « La Quadrature du Net » against drones, with the Conseil d'État, Order of 18 May 2020, n° 440442, 440445, available at https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones , and the Human Rights League's action against thermal scans in schools, with the decision available at https://www.conseil-etat.fr/actualites/actualites/cameras-thermiques-a-lisses-le-juge-des-referes-ordonne-de-mettre-fin-a-leur-usage-dans-les-ecoles

Examples of such other purposes are:

- information to population (news, general alerts, general instructions to avoid infections, maps to avoid hotspots);
- medical support (self-diagnosis, reporting, information to access to health services);
- crowd control (mandatory and non-mandatory applications - quarantine enforcement, forms for movement during lockdown, map travel patterns, record physical passage, contact and proximity tracing, report of violation of rules).

Some countries have used non-specific Covid-19 applications to map hotspots (**Czech Republic**) or send alert to populations (AlertSwiss in **Switzerland**).

The development and use of those digital solutions triggered opinions and statements from national and regional data protection bodies[66]. These opinions insist on the need for specific legislation to determine the purposes of data processing by the Covid-19 apps and to prohibit the processing of data collected for further purposes.

However, only a few countries prepared specific legislation - this was the case in **Norway**, **Italy, Belgium, France and Finland**[67] - and took the required preliminary steps to limit the impact of the tool on fundamental rights. In its answer to the questionnaire, Norway explained: "The legal foundation for the app is a dedicated regulation. The Parliament recently supported the use of a twofold purpose, with separate consents for each: 1) Contact tracing and 2) (aggregate) analysis of infection patterns and infection control impact. The app provides links to services for self-reporting of symptoms, but is not part of the (legal) purpose of the app." More detailed observations about the different types of apps and their purposes are provided in the second part of this report.

2. Use of traffic and location data from mobile phones and apps

The Joint European Roadmap prepared by the EU to support lifting the containment measures[68] encourages governments to process aggregate and anonymised data from social media and mobile network operators, to reveal patterns and trends in social mobility and help predict the spread of the virus. Such use of aggregated data[69] has actually been put in place in most parties to Convention 108, with the notable exception of the United Kingdom, Poland and the Netherlands[70].

The Joint Research Centre currently receives data from 14 mobile network operators in 19 EU member states (**Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden**) and **Norway**.

In **Germany** and **Denmark**, concerns were expressed regarding the irreversibility of anonymisation and potential third-party access to the data[71]. Similarly, in the **Netherlands**, the data protection authority issued an initial negative advice about a legislative proposal aimed at obliging telecom operators to systematically provide anonymised data to the national statistics agency (CBS).

Some countries process directly identifiable location data to help contain the spread of the virus. The **Polish** Covid Act[72] for instance, imposes an obligation on the telecommunication operators to provide location

66. EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf and Joint Statement on the right to data protection in the context of the COVID-19 pandemic, Alessandra Pierucci, Chair of the Committee of Convention 108, and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 14/05/2020, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter
67. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 52, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
68. Joint European Roadmap towards lifting COVID-19 containment measures, 15 April 2020, p. 7, available at https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/european-roadmap-lifting-coronavirus-containment-measures_en
69. Information gathered from multiple sources and expressed in a summary form for purposes such as statistical analysis, to notably examine trends, make comparisons, or reveal information and insights that would not be observable when data elements are viewed in isolation.
70. The Joint Research Center has published a first set of three technical reports based on the data. See: https://ec.europa.eu/digital-single-market/en/news/coronavirus-mobility-data-provides-insights-virus-spread-and-containment-help-inform-future and https://ec.europa.eu/jrc/en/news/coronavirus-mobility-data-provides-insights-virus-spread-and-containment-help-inform-future.
71. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
72. Special Covid-19 Act of 2 March 2020 and subsequent Act of 31 March 2020, Act on special support instruments in relation to the spread of virus SARS-CoV-2 of 16 April 2020, available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000567

data of phones belonging to persons subjected to quarantine upon request of the Ministry of Digitalisation. The government also launched the mobile app "Home Quarantine" which allows police to monitor individuals' compliance with quarantine, including facial recognition technology and providing for fines in case of non-compliance[73].

In **Slovakia**, a new provision of the Electronic Communications Act[74] enables the public health authority to access phone-location data normally subject to telecommunication secrecy. Some data are processed in anonymised form, for statistical purposes of identifying, preventing and modelling threats to life and public health, but also to identify individuals who should be notified of special measures taken to protect their life and health.

Similar measures were adopted in **Bulgaria**. An amendment to the Law on Electronic Communication, implemented through the Law on Emergency, allows the police to request from telecommunication companies 'immediate access' to traffic data of users to control quarantine compliance, with *a posteriori* judicial oversight[75].

For the same purpose of quarantine control, telephone companies in **Mexico** are obliged to provide access to cell phone antennas to the Digital Agency for Public Innovation[76]. The province of **Santa Fe** in Mexico is allegedly requiring those who have violated quarantine to download an app that specifically tracks their movements[77]. In **Argentina**, the Ministry for Health developed an app that every visitor entering the country is legally required to install and use for 14 days. The app gives the ministry access to real-time location data.[78]. Similarly, in **Turkey**, it is mandatory for people infected with Covid-19 to download an app called "Life fits inside the house" (HES) as part of the "Pandemic Isolation Tracking Project." The app follows the movement of people instructed to self-isolate, and if they leave their homes, they receive a warning via SMS and are contacted instantly through automatic call technology and told to return to isolation. Use of the app is also mandatory for people wishing to travel by train or plane between cities in Turkey. Only if the app confirms that they have not been infected with the virus, will they be allowed to travel.[79]

In **Austria**, the law allows for the processing of identification and movement data by telecommunication providers in order for them to be able to send SMS warnings to end users[80]. Similarly, in **Lithuania**, following the adoption of a resolution declaring a state-level emergency, mobile operators are required to send text messages to customers requiring them to self-isolate when they return from foreign countries affected by the virus[81]. It is not clear if the mobile operators provide personal data to the relevant ministries.

3. Other digital solutions

Examples of other digital solutions and tools that have been put in place, often without a specific law, to help monitoring the spread of the virus, are:

- websites with health questionnaires;
- use of eBracelets;
- use of smart cameras allowing for facial recognition;
- thermal scans;

73. Details on the website of the Polish Government, at https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa-ruszyl-proces-jej-udostepniania
74. Slovakia: Change of Government under COVID-19 Emergency, available at https://verfassungsblog.de/slovakia-change-of-government-under-covid-19-emergency/
75. European Union Fundamental Rights Agency, Coronavirus pandemic in the EU – Fundamental Rights Implications, national report for Bulgaria, available at https://fra.europa.eu/sites/default/files/fra_uploads/bg_report_on_coronavirus_pandemic_-_may_2020.pdf
76. Statements on the web portal of the city of Mexico, available at https://cdmx.gob.mx/portal/articulo/cierre-de-centros-comerciales-por-emergencia-sanitaria
77. Controlarán a quienes incumplieron elaislamiento con una App en sus celulares, 23 March 2020, available at https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html
78. Disposición 1771/2020 on the Covid-19 application, adopted 25 March, available at https://www.boletinoficial.gob.ar/detalleAviso/primera/227170/20200326
79. Human Rights Watch, https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa See also: duvaR.english, Health Ministry's mobile app for travel may breach privacy law, experts warn https://www.duvarenglish.com/health-2/coronavirus/2020/05/25/health-ministrys-mobile-app-for-travel-may-breach-privacy-law-experts-warn/_ ore information about the Pandemic Isolation Tracking Project is available on the official site of the Directorate of Communications : https://www.iletisim.gov.tr/english/haberler/detay/director-of-communications-altun-shares-a-post-on-pandemic-isolation-tracking-project
80. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
81. This use of the telecommunications data was approved by the Lithuanian State Data Protection Inspectorate, Text Messages on the Coronavirus Pandemic to Persons Returning from Abroad are Sent Legally in Lithuania, available at https://vdai.lrv.lt/en/news/text-messages-on-the-coronavirus-pandemic-to-persons-returning-from-abroad-are-sent-legally-in-lithuania

- remote control by drones and robots;
- mandatory virus testing.

The processing of health data through websites and apps that encourage self-reporting of health-related data to health authorities while at the same time providing advice to individuals, is generally based on the (explicit) consent of individuals, while other digital solutions require a specific legal basis.

In nine countries (**Denmark, Finland, Ireland, Italy, Mauritius, Norway, Spain, Ukraine, and Uruguay**) websites are available with health questionnaires where people can report symptoms. A **Dutch** website from the RIVM (National Institute for Public Health and the Environment) was taken offline twice, due to structural information security problems.[82] It is important to note that the input to these health questionnaires can be used to publish maps indicating virus hotspots.

eBracelets are currently used in **Liechtenstein** and **Cyprus** and tested in **France**. **Liechtenstein** is testing an existing electronic bracelet that measures skin temperature, pulse, respiration and blood flow.[83] The Liechtenstein government funds the test on 2 200 of the 38 000 inhabitants of the principality, in the hope it can also detect Covid-19 infection in early stage.[84]

According to the answers to the questionnaire, wearable technology is also used in **Cyprus**, but no public information could be found. Bluetooth-enabled wristbands can also be used to enforce physical distancing, and collect information about compliance with this rule. The port of Antwerp[85] in **Belgium**, for instance started to use Bluetooth-enabled wristbands to enforce social distancing rules on the workplace. The wearables give off warning signals when workers come too close to each other.

Although the location data are only exchanged locally, proximity details are stored on a central server.[86] On its website, the Belgian data protection authority confirms that completely anonymous proximity tracing bracelets may be used on the workplace[87] and explicitly warns that such bracelets may not be used if (location) data of identifiable persons are used and stored. Such processing is only permitted based on the (explicit) consent of the employee, which is of concern in view of the imbalance of power between employees and employers.[88]

While none of the parties to Convention 108 currently have plans to make the use of wearables mandatory, it is interesting to mention developments in **Singapore**, as many countries were previously inspired by Singapore to develop contact tracing apps to contain the virus. Singapore is currently planning to equip all 5,7 million inhabitants with a wearable contact tracing device.[89] The Ministry for Health has not ruled out that use will be made mandatory. An online petition against use of the dongle has been initiated[90] and privacy advocates have warned on the risks of placing Bluetooth sensors in public places, *de facto* turning the dongles into potential population location trackers.[91]

Drones and robot surveillance are used to monitor compliance with physical distancing measures in public spaces, notably in **Greece**, **Belgium** and **Hungary**[92]. Robots with thermal imaging cameras have been

82. *MBS News*, RIVM website infection radar temporarily offline after data breach, 7 June 2020, available at https://www.mbs.news/en/2020/06/rivm-website-infection-radar-temporarily-offline-after-data-breach-inland.html.
83. ICO Liechtenstein, What a COVID-19 Bracelet Says about Liechtenstein, 7 August 2020, available at https://www.ico.li/what-a-covid-19-bracelet-says-about-liechtenstein/
84. *Basler Zeitung*, Liechtenstein als Corona-Labor, Fruchtbarkeits-Armbänder gegen das Virus, 18 April 2020, available at https://www.bazonline.ch/das-liechtenstein-experiment-867253873911 See also the manufacturer information, available at https://www.avawomen.com/ava-bracelet-for-covid-19/.
85. The company that produces the bracelets writes: "*When an employee is infected, the company physician can consult the wearable register to retrieve the identities of the colleagues that have been too close to the employee during the previous two weeks.*"
86. Bracelets, Beacons, Barcodes: Wearables in the Global Response to COVID-19, available at https://www.globaldiasporanews.com/bracelets-beacons-barcodes-wearables-in-the-global-response-to-covid-19/ See also : https://rombit.be/covid-solutions/
87. Belgian data protection authority, Covid-19 on the work floor (in Dutch only), https://gegevensbeschermingsautoriteit.be/burger/thema-s/covid-19/covid-19-op-de-werkvloer
88. Ibidem.
89 Reuters, Singapore plans wearable virus-tracing device for all, 5 June 2020, available at https://www.reuters.com/article/us-health-coronavirus-singapore-tech-idUSKBN23C0FO.
90. *Change.org*, Singapore says 'No' to wearable devices for Covid-19 contact tracing, available at https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-covid-19-contact-tracing
91. *BBC*, Coronavirus: Why Singapore turned to wearable contact-tracing tech, 5 July 2020, available at https://www.bbc.com/news/technology-53146360
92. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, op. cit., p. 56.

used for the same purpose in **Tunisia**[93]. Drones have also been used to record people's temperature in **Croatia**[94] and equipped with cameras for crowd control in **Cyprus**[95].

Smart cameras can be used in various ways, from facial recognition used to control quarantine compliance, as is the case in **Moldova**[96] and **Russia**[97], to automated recognition of masks in public transports, as developed in a **French** project[98].

Thermal scans are also being widely used to monitor access to public and private premises, increasingly in airports. In **Argentina**, **Cyprus**, **Estonia**, **Mauritius**, **Spain**, and **Ukraine**, thermal cameras are used for fever detection, including mounted on drones.[99] The use of infrared thermometers triggered reactions from several data protection authorities. The **Dutch**[100], **Lithuanian**[101] and **Portuguese**[102] authorities stated that the use of thermal scans by employers is illegal, while others like the **Belgian** authority questioned the legal basis for their use in airports[103]. The **Spanish**[104], **French**[105] and **Cypriot** data protection authorities[106] issued general reminders about the strict application of the data protection framework to thermal scans.

The most recent development concerns plan of mandatory testing of visitors, as well as inhabitants. In **France**[107] and **Germany**[108], visitors from certain countries could be subjected to mandatory testing of the presence of the virus.

Both in **Monaco** and **Andorra**, announcements refer to the testing of the entire population to examine the presence of the virus[109].

Regardless of the type of test used (viral or antibody) mandatory testing is a highly invasive measure as it involves the use of biometric samples to detect the health status of individuals. Its deployment will have to be weighed in light of the effectivity of the system in limiting the spread of the virus, knowing that the virus may go undetected, while it may take 1 to 3 weeks for antibodies to be present after an infection and that there is still a lack of scientific evidence on immunity and contagion aspects.

4. Increase of teleworking and distance learning

Many countries have adopted lockdown measures, which led to a rapid uptake of teleworking and distance learning, and heavy reliance on new digital solutions. Such digital solutions have the potential to lead to additional intrusions in the private life of individuals as they imply significant processing of personal data of a sensitivity as it belongs to the most intimate sphere of the individuals.

93. Coronavirus: Tunisia deploys police robot on lockdown patrol, Rana Jawad, 3 April 2020, available at https://www.bbc.com/news/world-africa-52148639
94. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
95. Answer to the questionnaire but no public information sources provided.
96. Moldova: Transnistria uses facial recognition to identify quarantine violators, 23 March 2020, available at https://privacyinternational.org/examples/3629/moldova-transnistria-uses-facial-recognition-identify-quarantine-violators
97. 100 000 cameras: Moscow uses facial recognition to enforce quarantine, 24 April 2020, Sam Ball, available at https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine
98. La détection automatique des masques dans le métro parisien remise en cause, Armelle Exposito, 13 May 2020, available at https://ateliers.cfjlab.fr/2020/05/13/la-detection-automatique-des-masques-dans-le-metro-parisien-remise-en-cause/
99. Answers to questionnaire CoE, no public information sources provided.
100. Statement of the Dutch supervisory authoirity on thermal scans, 24 April 2020, available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-temperatuur-meten-mag-niet-zomaar
101. Statement of the Lithuanian DPA on Personal Data Protection and Coronavirus COVID-19, 16 March 2020, available at: https://vdai.lrv.lt/en/news/personal-data-protection-and-coronavirus-covid-19
102. Statement of the Portuguese supervisory authority on the unlawfulness of the use of thermal scans by employers, 23 April 2020, available at https://www.cnpd.pt/home/orientacoes/Orientacoes_recolha_dados_saude_trabalhadores.pdf
103. Statement of the Belgian supervisory authority on the legal basis for thermal scans in Brussels airport, 17 June 2020, available at https://www.autoriteprotectiondonnees.be/citoyen/controles-de-temperature-lapd-prend-contact-avec-brussels-airport
104. Statement of the Spanish DPA regarding the taking of temperature by shops, work centers, and other establishments, 30 April 2020, available at https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos
105. Statement of CNIL on the use of thermal scans and smart cameras in relation to the pandemic, 17 June 2020, available at https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras?
106. Statement of the Cypriot DPA on the use of thermal scans, 24 April 2020, available at http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/798C8B6809EBDC87C2258554004137CB?OpenDocument.
107. *Forbes*, 16 High-Risk Countries Face Mandatory Covid Tests In France, 24 July 2020, available at https://www.forbes.com/sites/tamarathiessen/2020/07/24/us-16-countries-mandatory-covid-tests-france/
108. Reuters, Germany fights virus uptick with mandatory testing for travellers, 6 August 2020, available at https://www.reuters.com/article/us-health-coronavirus-germany-cases-idUSKCN252074T.
109. https://all-andorra.com/13-latest-covid-19-updates-and-events-across-the-country-as-of-wednesday-25th-march-2020-20h/. See also : *ARD*, Tageschau, Andorra testet alle, 2 April 2020, available at https://www.tagesschau.de/ausland/andorra-coronavirus-101.html

In the majority of cases, the use of these digital solutions was not decreed or organised via legislation. Instead, employers, doctors, schools and universities simply began to use freely available tools, sometimes without the necessary anticipation and consideration of the potential data protection impact.

Data protection authorities have expressed concerns about the following issues notably:

- legal basis for the processing of employees and students' data;
- risks of constant on-line monitoring;
- disproportionate access to the terminal and private home of the individual (screenshots);
- risk of function creep;
- data security.

In **Italy** for instance, the supervisory authority recalled that data processed for teaching purposes may not be used for other purposes. It also raised cybersecurity concerns, as did the authorities of the **Netherlands** and **Sweden**. The data protection authorities also addressed the difficulty of obtaining a valid consent as the legal basis for the data processing. In view of the imbalance of power between employers and employees at work, or between students and their teachers, it is very difficult to meet the threshold of *freely given* consent.

In a **Dutch** court case, students from the university of Amsterdam tried to obtain prohibition of the mandatory use of online proctoring software to take tests during the pandemic. In summary proceedings, the judge explained that the measure was necessary to execute the public task of the university, and proportionate, as long as there were no alternative means of taking exams in a physical classroom[110].

Guidance on distance learning was published in **Greece**, the **Netherlands**, **Portugal**, **Sweden**, **Italy** and **Lithuania**[111]. The Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe also provided recommendations in that respect[112]. They stress the need for data protection oriented standard configurations, with a view to limit the data collection to what is strictly necessary, recall the need of full transparency about the processing of data, the choice of a proper legal basis and the approval of parents in this respect.

With regard to teleworking, and the processing of health data of employees, many data protection authorities have emphasised the need to apply the same requirements of privacy by design and by default. While details of the guidance may differ due to specific national health and labour law, the supervisory authorities have generally insisted on the need for a proper legal basis and minimisation of the collection of data. The data protection authorities share a preference for a collection of data limited to general risks exposure, rather than explicit health data including medical diagnosis. In **Luxembourg**, **France** and **Belgium**, for instance, employers' questionnaires including such health data have been forbidden due to the sensitivity and specific protection of that data. Proportionality of the measures, balanced with the existence of a specific risk, is a widely shared requirement[113].

110. District Court Amsterdam, 11 June 2020, ECLI:NL:RBAMS:2020:2917, available at http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2020:2917 Student Proctoring Software Gets First Test Under EU Privacy Law, 29 July 2020, available at https://news.bloomberglaw.com/tech-and-telecom-law/student-proctoring-software-gets-first-test-under-eu-privacy-law.
111. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
112. Joint Statement on the right to data protection in the context of the COVID-19 pandemic, Alessandra Pierucci, Chair of the Committee of Convention 108, and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 14 May 2020, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.
113. EU Member State Data Protection Authorities Deal with COVID-19: An Overview, p. 4 and s., Christina Etteldorf, EDPL, 2/2020, available at https://www.lexxion.eu/wp-content/uploads/2020/03/COVID-19-Special-Data-Protection-Authorities-Deal-with-COVID-19.pdf

II. A case-study: the use of digital solutions

When the impact of the Covid-19 pandemic became clearer, many parties to Convention 108 started to develop digital solutions and technical tools to control the dissemination of the virus. Most countries focussed on the use of apps. Though most countries developed apps to aid contact tracing, some countries also invested efforts in apps to help people with self-diagnosis of symptoms, or to enforce containment measures.

The Council of Europe sent a questionnaire on 27 May 2020 to the 55 parties to Convention 108.

The questionnaire consisted of 5 questions with multiple choice answers and limited free space for additional information:

1. Do public authorities in your country plan to use or already use Covid-19 apps? If so, for what of the mentioned purposes?
2. What guarantees will, or do, the Covid-19 apps offer to ensure the right to respect for private life and the protection of the personal data of those concerned?
3. To your knowledge, do these apps use artificial intelligence (machine learning) and if so, for what purpose?
4. Do public authorities in your country plan to use, or already use, other information technologies to monitor and/or control the spread of Covid-19?
5. Is the data protection authority (in the countries where it exists) involved in the development, deployment, control of any app or other technology listed above?

47 recipients answered the questionnaire, out of which 6 are African and Latin American parties to Convention 108[114] and the analysis that follows is based on the replies made. In order to get a more complete overview of digital solutions implemented in the countries parties to Convention 108, external news and aggregation sources were also used, as referenced in footnotes[115]. The situation rapidly evolving, changes may have occurred in some countries after the publication of this report and readers are invited to consult the latest national references for a fully up-to-date information.

Governments and stakeholders involved in the fight against the pandemic have been relying on data analytics and digital solutions to fight the spread of the virus, by notably using mobile location data to evaluate movements of population or to enforce confinement measures, using devices as digital proof of immunity, symptoms' detection, self-testing, or digitally tracing the contacts of an infected person. This first digital solution, which was the most broadly considered worldwide is the first to be examined.

114. No answers were received from Azerbaijan, Greece, Malta, Montenegro, Poland, the Republic of Moldova, the Russian Federation and Turkey. In view of the low spread of the virus in the Principality and the uncertainty as regard its population's acceptance, the authorities of Monaco decided that such a system was not necessary. Of the non-respondent countries, only Greece and Montenegro do not seem to have any digital contact tracing app.
115. Relevant sources that were checked for information about (new) contact tracing apps, are: XDA developers list of countries with apps, available at https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/, MIT Technology Review Covid Tracing Tracker, available at https://public.flourish.studio/visualisation/2241702/ , European Commission, Open Source Solutions helping to tackle COVID-19, available at https://joinup.ec.europa.eu/collection/digital-response-covid-19/open-source-solutions#Tracking , European Mhealth solutions for managing the covid-19 outbreak, available at https://mhealth-hub.org/mhealth-solutions-against-covid-19, Github European contact tracing apps for Android, available at https://github.com/ct-report/summary and List of Covid-19 Apps at https://docs.google.com/spreadsheets/d/1qfbhFZbWCXd4GspSD6LL8CNmgzKEYtL-gQQk1gEKqrk/edit#gid=0

A. Digital contact tracing apps

Looking manually at contact tracing (and alerting) has always been used in epidemic monitoring to reduce the spread of infections and consists in identifying the persons who may have come into contact with an infected person to alert them, where necessary, and allow them to get the necessary care and self-isolate to avoid further spread of the disease.

With this health crisis, mobile apps have been seen by many as a complementary response to the need to rapidly perform such contact monitoring, with sometimes limited consideration of the absence of evidence of their efficacy, and thus of the proportionality of the measures adopted.

Mobile apps are a computer program (or software application) designed to run on a mobile device (a smartphone or tablet computer) rather than on desktop or laptop computers.

In order for the mobile devices to communicate possibly with other devices, a protocol establishes the set of rules determining how the data will be transmitted.

Regarding digital contact and proximity tracing, various protocols have been developed since the beginning of the health crisis, providing different functionalities.

The table below provides an overview of the existing protocols used in digital contact and proximity tracing.

Table 1 – Existing protocols

Name	Origin	Centralisation	Link
Exposure Notification	Apple and Google	Decentralised	https://www.apple.com/covid19/contacttracing
Blue Trace/ Open Trace	Singapore Government Digital Services	Semi-centralised	https://github.com/opentrace-community
DP-3T (Decentralized Privacy-Preserving Proximity Tracing)	EPFL, ETHZ, KU Leuven, TU Delft, University College London – UCL, CISPA, Oxford, University, Torino University, ISI Foundation	Decentralised	https://github.com/DP-3T
OpenCovidTrace	1Checkin, Evocativideas, MLM Holdings, Nebula Ventures, open source community, Quantstellation	Decentralised	https://opencovidtrace.org https://github.com/OpenCovidTrace
PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing)	Fraunhofer Institute for Telecommunications, R. Koch Institute, Technical University of Berlin, TU Dresden, Erfurt University, Vodafone Germany	Semi-centralised	https://github.com/pepp-pt/pepp-pt-documentation
PACT: Private Automated Contact Tracing	MIT Computer Science and Artificial Intelligence Laboratory, Massachusetts General Hospital, MIT Lincoln Laboratory, MIT Media Lab, Boston University, Weizmann Institute of Science, Brown University		https://pact.mit.edu
Privacy-Sensitive Protocols And Mechanismsfor Mobile Contact Tracing (PACT)/ CovidSafe	Microsoft volunteers, University of Washington		https://arxiv.org/abs/2004.03544 https://github.com/covidsafe
RecoVer	Softmining, Nexus TLC, Minervas (Trucky), Pushapp		https://www.smcovid19.org/recover/

Name	Origin	Centralisation	Link
ROBERT (ROBust and privacy-presERving proximity Tracing protocol)	Inria	Semi-centralised	https://github.com/ROBERT-proximity-tracing
TCN Protocol (Temporary Contact Number)	CovidWatch, CoEpi, ITO, Commons Project, Zcash Foundation, Openmined	Decentralised	https://github.com/TCNCoalition/TCN
Tensho	CryptIQ		https://github.com/cryptiqdev/tensho
Whisper Tracing Protocol	Nodle, Coalition Network		https://github.com/NodleCode/coalition-android https://www.coalitionnetwork.org/

A key difference in approach, embedded in the protocol, is the choice between centralised data collection by the national (possibly health) authorities versus decentralised data processing.

The main difference with the centralised contact tracing apps is that all proximity data, including the Bluetooth strength, are exclusively calculated on, and processed in, the app.

If users are diagnosed with the virus, they can choose to upload the data they have collected from other nearby Bluetooth devices to an application server from a designated health authority. Every app periodically downloads the temporary exposure keys shared voluntarily by other infected users, and compares these keys with the random codes registered in the previous days as a result of contacts with other users with the app. If a match is found, the application runs an algorithm on the device which, depending on the estimated duration and distance of the contact, and in accordance with the criteria established by the health authorities, decides whether to display a notification on the user's device exposed to the risk of contagion. The notification warns the user of the match, its date, invites him to self-confirm, and contact the health authorities. This technical design of the app prevents users from involuntarily sharing personal data with other users, or with the health authorities.

To prevent false positives, the protocol foresees the use of unique codes generated by the health authorities. Users first have to upload such a unique code in the app after they have tested positive, before their app sends its logfiles to the server.

Table 2 below shows whether countries have chosen a central approach for their proximity and contact tracing apps, or a decentralised approach. For countries without an app, the URL of official information is shown, usually from the Ministry for Health in that country.

Of the 55 countries parties to Convention 108, 14 have chosen a centralised approach for proximity and contact tracing apps (some solutions are actually semi-centralised, such as the app used in **France** or apps using the PEPP-PT protocol). In **Norway**, the use of the centralised tracking app is suspended due to data protection concerns.

In total, 25 jurisdictions have chosen a decentralised approach (**Austria, Azerbaijan, Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, the British Overseas Territory of Gibraltar (hereafter Gibraltar), Ireland, Italy, Latvia, Malta, Morocco, Netherlands, Poland, Portugal, Slovak Republic, Slovenia, Spain, Switzerland, Tunisia, United Kingdom** and **Uruguay**). Apps using the DP-3T protocol or the Google Apple Exposure Notification System (GAEN) follow a decentralised approach.

In addition, 6 countries do not plan to use a contact tracing app at all (**Bosnia and Herzegovina, Greece, Liechtenstein, Luxembourg, Mauritius** and **Sweden**). In **Lithuania** , a private sector initiative for a contact tracing app was abandoned.

In 10 countries, the technical approach retained is unclear, with the probable use of an app from a neighbouring country (**Andorra**, **San Marino**), or because the app is still in development, or there are no plans to use an app for contact and proximity tracing (**Albania, Cabo Verde, Georgia, Montenegro, Moldova, Senegal, Serbia** and **Ukraine)**.

Table 2 – Digital contact tracing apps: central or decentral approach

Jurisdiction	Name of application	Government information about the app or official information on the app	Central	Decentral
Albania	Unknown.	https://www.kryeministria.al/en/?s=corona&post_type=newsroom		
Andorra	(for self diagnosis)	https://visitandorra.com/en/covid-19-in-andorra/		
Argentina	CuidAR	https://www.argentina.gob.ar/jefatura/innovacion-publica/acciones-coronavirus/aplicacion-y-tableros-de-gestion	√	
Armenia	COVID-19 Armenia	https://play.google.com/store/apps/details?id=am.gov.covid19	√	
Austria	Stopp Corona	https://at.roteskreuz.stopcorona		√
Azerbaijan	Watch COVID (COVİD izlə)	https://apps.apple.com/az/app/covid-izle/id1511326016		√
Belgium	In development[116]	https://www.info-coronavirus.be/en/		√
Bosnia and Herzegovina	No plans to introduce app.	https://covid-19.ba/		
Bulgaria	Virusafe – not BLE but GPS	https://virusafe.info/	√	
Cabo Verde	unknown	https://covid19.cv/		
Croatia	Stop COVID-19	https://www.total-croatia-news.com/news/45331-croatia-presents-its-stop-covid-19-app		√
	Digital Assistant Andrija	https://andrija.ai/		
Cyprus	COVTRACER	https://covid-19.rise.org.cy/en/ https://www.pio.gov.cy/coronavirus/en/index.html	√	
Czech Republic	eRouška ("eFace-Mask")	https://koronavirus.mzcr.cz/en/		√[117]
	Mapy.cz	https://en.mapy.cz/		
Denmark	Smittestop	https://com.netcompany.smittestop_exposure_notification		√[118]
Estonia	Covid app – in development	https://e-estonia.com/trace-covid-19-while-respecting-privacy/		√[119]
	Immuunsuspass – In development[120]			
Finland	Ketju - In development[121]	https://thl.fi/en/web/thlfi-en/-/corona-application-trial-starts-on-tuesday		√[122]
	Selfdiagnosis	https://www.omaolo.fi/		
France	STOPCOVID	https://www.economie.gouv.fr/appli-stop-covid-disponible	√	
Georgia	Stop Covid	https://stopcov.ge/		
Germany	Corona-Warn-App	https://www.coronawarn.app/de/		√
Greece	No app			
Gibraltar	Beat Covid Gibraltar	https://www.gibraltar.gov.gi/beatcovidapp/privacy		√

116. https://www.computable.be/artikel/columns/overheid/6963986/5658341/blyaert-betwist-geen-corona-app-voor-eind-september.html
117. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19, Progress reporting June 2020, available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf page 4.
118. Ibid and https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/
119. Ibid.
120. https://medicalxpress.com/news/2020-06-estonia-virus-immunity-passport-app.html
121. https://github.com/ct-report/summary
122. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020, page 4.

Hungary	VirusRadar	https://virusradar.hu/	√	
	HKR	https://hazikaranten.hu/	√	
Iceland	Rakning C-19 App	https://www.covid.is/app/is	√	
Ireland	Covid Tracker	https://www.hse.ie/eng/services/news/newsfeatures/covid19-updates/covid-tracker-app/		√
Italy	Immuni	https://www.immuni.italia.it		√
Latvia	APTURI COVID	https://www.apturicovid.lv/#en		√
Liechtenstein	No app	https://www.liechtenstein.li/land-und-leute/gesellschaft/gesundheitswesen/corona-virus/		
Lithuania	App suspended by DPA	https://koronastop.lrv.lt/en/news/useful-and-meaningful-self-isolation-with-a-mobile-app-quarantine		
Luxembourg	No app	https://coronavirus.gouvernement/en.lu.html		
Malta	In development	https://deputyprimeminister.gov.mt/en/health-promotion/covid-19/Pages/landing-page.aspx		√[123]
	Covid-19 Check	https://covid19check.gov.mt/		
Mauritius	No app	http://www.covid19.mu		
Mexico	COVID-19 MX (self-diagnosis & info)[124]	https://play.google.com/store/apps/details?id=mx.gob.cdmx.adip.covid19cdmx&hl=en_US		
Monaco	Uses French app	https://en.gouv.mc/Portail-du-Gouvernement/Policy-Practice/Coronavirus-Covid-2019	√	
Montenegro	No app	http://www.gov.me/en/homepage/measures_and_recommendations/		
Morocco	Wiqaytna	www.wiqaytna.ma/		√
Netherlands	Coronamelder in development	https://coronamelder.nl/corona		√
	OLVG corona app – self diagnosis	https://www.olvg.nl/de-corona-check		
North Macedonia	Stop Korona!	https://stop.koronavirus.gov.mk/en	√[125]	
Norway	Smittestopp – suspended by DPA 6/16[126]	https://www.fhi.no/en/id/infectious-diseases /coronavirus/use-of-smittestopp-privacy-policy/ & https://helsenorge.no/coronavirus/smittestopp	√	
Poland	ProteGO Safe	https://www.gov.pl/web/koronawirus/protegosafe		√[127]
	Kwarantanna domowa	https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa--ruszyl-proces-jej-udostepniania		
Portugal	STAYAWAY COVID In development	https://covid19estamoson.gov.pt/app-estamoson-covid19/		√
Republic of Moldava	Unknown	https://ansp.md/index.php/category/actualizarea-situatiei-privind-coronavirus/		
Romania	Unknown			
Russian federation	Social Monitoring	https://www.mos.ru/news/item/73074073/	√	
San Marino	Unknown, can probably use Italian app	http://www.iss.sm/on-line/home/artCataggiornamenti-coronavirus.49004093.1.20.1.html		

123. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020, page 4.
124. The Ministry for Health (Federal Public Administration Agency) of the Mexican government developed and launched the application COVID-19 MX to help self-diagnosis, find nearby hospitals and provide statistics.
125. https://stop.koronavirus.gov.mk/en
126. https://github.com/ct-report/summary
127. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19, Progress reporting June 2020, page 4.

Senegal	Unknown. Appears to be Daancovid19	https://daancovid19.sn		
Serbia	Unknown	https://covid19.rs/eng-instituteforpublichealth-updates/		
Slovak Republic	COVID19 Zostan Zdravy	https://www.dhis2.org/covid-19	√	
Slovenia	Ostani Zdrav In development	https://www.gov.si/en/news/2020-07-30-application-for-protecting-public-health-and-lives-is-anticipated-to-be-available-in-mid-august/		√
Spain	Radar COVID. In development[128]	https://www.mineco.gob.es/portal/site/mineco/menuitem.2efe1f7b4e40d4856c8a0f35026041a0/?vgnextoid=de1969e8c9b11710VgnVCM1000001d04140aRCRD + regional apps, such as https://play.google.com/store/apps/details?id=org.madrid.CoronaMadrid		√[129]
Sweden	No plans to introduce app	https://www.government.se/government-policy/the-governments-work-in-response-to-the-virus-responsible-for-covid-19/		
Switzerland	SwissCovid	https://www.bag.admin.ch/bag/de/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html#-728718249		√[130]
Tunisia	E7mi (contact tracing)	https://e7mi.tn/faq_ar.html		√[131]
	Stop Corona (self-diagnosis)	https://www.stopcorona.gov.tn/		
Turkey	HES (Life fits inside the house)	https://play.google.com/store/apps/details?id=tr.gov.saglik.hayatevesigar&hl=en_US	√	
Ukraine	Name unknown	https://covid19.gov.ua/ & https://www.kmu.gov.ua/news/projdi-observaciyu-vdoma & https://moz.gov.ua/koronavirus-2019-ncov		
United Kingdom	New NHS Covid-19 launched 24 Sept. 2020	https://covid19.nhs.uk/		√
Uruguay	CoronavirusUY (self- diagnosis)	https://www.gub.uy/ministerio-salud-publica/coronavirus		√[132]

1. Centralised tracing apps

Inspired by the Singapore Trace Together app and the South Korean Corona 100 app, for example the **United Kingdom**, **Germany**, **Hungary**, **Slovenia**, **Malta** and **France** started to develop centralised contact tracing apps. In total, 14 countries have apps with a centralised data collection. Some countries were inspired by the Pan-European Privacy-Preserving Proximity Tracing protocol (PEPP-PT). This first generation of apps raised many privacy alerts, as these apps sent contact logs with pseudonymised personal data to a central (government) back-end server after a user reported to be infected with the virus. This centralised approach allowed the recipient authority to calculate the proximity, and individually notify other users of the app of potential contact with an infected person. On 19 April 2020, the approach chosen by PEPP-PT was strongly criticised by over 300 security and privacy academics from 26 countries. Though many countries have since moved to a decentralised model of contact tracing, and the centralised apps deployed in the **United Kingdom**

128. https://english.elpais.com/society/2020-06-29/spain-launches-first-phase-of-coronavirus-tracking-app.html
129. *El Pais*, Spain launches first phase of coronavirus-tracking app, 29 June 2020, available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf
130. https://www.bag.admin.ch/bag/de/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html#-728718249
131. https://e7mi.tn/faq_fr.html and https://e7mi.tn/presentation.pdf, only available in Arabic.
132. https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

and **Norway** were suspended for lack of effectivity, **France** continued with a semi-centralised approach, launching StopCovid.[133]

In **Bulgaria**, the government developed a contact tracing app based on GPS location data, instead of Bluetooth data. The app *Virusafe* aims at assisting the competent authorities in organising and controlling the anti-epidemic measures imposed in the country. The controller of the personal data processed through the app is the Ministry for Health. Use of the app is voluntary and all data processing, including data about health and geolocation data, is based exclusively on consent.

In **Cyprus**, in addition to the use of ebracelets, a proximity tracing app is deviced. The purpose is to check the users' location trails and identify the places a carrier has visited and in turn, locate other contacts who have been in close proximity with the diagnosed carrier.

In **Hungary** and **North Macedonia**, a contact tracing app (named *Virusradar* in Hungary and *StopKorona!* in North Macedonia) requires users to provide a mobile phone number. The user receives a code via SMS that is necessary to register with the app, which entails the possibility to establish a connection between the phone number and the app's unique ID. Like other contact tracing apps, *Virusradar* uses Bluetooth to communicate with other users and exchanges encrypted, anonymous data about the distance of surrounding devices if they have been at a dangerous distance for the past 14 days. Users can choose to share their data with epidemiologists, but they can also be asked by professionals to share their data, thereby notifying people who have been in close contact with an infected person. Hungary and North Macedonia have chosen slightly longer time and distance limits than most other countries: 20 minutes within 2 metres distance, instead of 15 minutes within 1.5 metres distance.[134]

2. Decentralised tracing apps

25 respondents have indicated that the decentralised approach has been retained in the development of their apps.

Numerous parties to Convention 108 already use, or plan to shortly use , the DP-3T protocol or the Google Apple Exposure Notification System (GAEN). These are: **Austria, Belgium, Croatia, Denmark, Estonia, Finland, Germany, Ireland, Italy, Latvia, Malta, Poland, Portugal, Slovenia, Spain, Switzerland, the Netherlands** and the **United Kingdom**.

The privacy policy of the **Spanish** RadarCovid app provides an interesting level of detail[135].

In **Austria**, the Red Cross Stop Corona app was reverse engineered by security firm SBA Research. In a joint analysis with NOYB-founder Max Schrems, they concluded the app complied with data protection laws, even though the app transmits a mobile number to the Red Cross servers.

Belgium initially did not plan to launch a proximity tracking app. In **Luxembourg**, members of parliament urged the government in May 2020 not to introduce a digital tracing app. They insisted on four necessary conditions should the government decide to develop an app: "the app should protect privacy, disclose the source code, communicate with other European apps and not allow data identifying individuals to be collected centrally."[74] In Belgium, the government finally decided to launch after the summer its Coronalert app.

The **Danish** *Smittestop* app was based on the Norwegian example with the same name, with the difference that the Danish app is based on the GAEN system and does not collect additional location data on top of the bluetooth exchanges. The reason the Norwegian app developers initially choose to collect other location data was due to the fact that more than half of Norwegians use iPhones and prior to the launch of the GAEN system, iPhones were not recording the data when users were not actively using the app.[136]

Italy explains that it uses data from the app to monitor the evolution of the epidemic and to enhance the accuracy of the model through which the app establishes whether the contact is sufficiently at risk as to trigger a notification. It is not clear how Italy obtains data from the app, which allegedly operates in a decentralised way.

133. *RFI*, France's Covid-19 tracking app has only identified 14 people at risk, 24 June 2020, https://www.rfi.fr/en/science-and-technology/20200624-france-s-covid-19-tracking-app-has-only-identified-14-people-at-risk
134. *Hungary today*, Coronavirus: New App to Track Nearby Positive Cases Available to Download, 14 May 2020, available at https://hungarytoday.hu/coronavirus-hungary-app-virusradar/ North Macedonia, StopKorona!?, available at https://stop.koronavirus.gov.mk/en
135. RadarCovid privacy policy (in Spanish), available at https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html
136. *DR*, Danish corona app 'according to Norwegian model': This is what you can expect, (in Danish only), 8 April 2020, available at https://www.dr.dk/nyheder/penge/dansk-corona-app-efter-norsk-model-det-kan-du-forvente

Latvia underlined the decentralised nature of the app, based on a voluntary use, with all data remaining on the device. It is only when a user chooses to provide contact information that a notification is sent from the device to the health authority with the contact phone number, date and duration of the contact with the infected person. The logs on the app are automatically deleted after 14 days. With regard to the purpose of contact tracing, the use of the app is presented as making it possible to achieve the goal of detecting new cases of the disease more efficiently and in a more precise way.[137]

B. Other purposes

Although most countries deviced apps for the purposes of proximity and contact tracing, some countries invested efforts in apps aimed at achieving other purposes. Some of these purposes operate at a general level to bring assistance and guidance to users, while others imply more intrusive and coercive features with a view to control the spread of the pandemic.

Examples of such other purposes are:

- provide general news and information about the pandemic;
- help people with self-diagnosis of symptoms;
- provide instructions to avoid infection;
- provide information about access to health services;
- create maps to help people avoid virus hotspots;
- enforce containment measures;
- fill in a form about reasons for movement during lockdown;
- map travel patterns from inhabitants;
- create daily statistics of recorded cases;
- record physical passage of visitors at entry and control points;
- allow users to submit online reports about the violation of rules by other people;
- provide crowd control.

Table 3 below shows the different purposes for which countries use such apps, based on the answers to the questionnaire, as completed with publicly available information sources.

Table 3 – Different purposes of the apps

Jurisdiction	Name of application	Purpose(s)						
		Contact tracing/ Proximity Alert	Self-diagnostic	Containment check	Crowd control	Map travel patterns	Immunity pass-port	Other
Andorra	In development		√					
Argentina	CuidAR		√	√	√	√	√	
Armenia	COVID-19 Armenia	√	√					√
Austria	Stopp Corona	√		√	√			
Azerbaijan	Watch COVID (COVİD izlə)	√						√
Belgium	Coronalert	√						
Bulgaria	Virusafe – not BLE but GPS	√	√					
Croatia	Andrija		√					
Cyprus	COVTRACER	√						
Czech Republic	eRouška	√				√		
Denmark	Smittestop	√						
Estonia	In development	√						

137. Latvian Data Protection Inspectorate, in Latvian only, Stop Covid does not track people, available at https://www.dvi.gov.lv/lv/zinas/mobila-lietotne-apturi-covid-neizseko-personas/

Finland	Ketju In development[138]	√	√					√
France	STOPCOVID	√						
Georgia	Stop Covid	√				√		
Germany	Corona-Warn-App	√						
Gibraltar	Beat Covid Gibraltar	√						
Hungary	VirusRadar	√		√				
Iceland	Rakning C-19 App	√						
Ireland	Covid Tracker	√	√					√
Italy	Immuni	√						√
Latvia	APTURI COVID	√	√					
Liechtenstein	No app but wearable	√						
Lithuania	Coronavirus – No longer available	√	√					
	Quarantine app suspended			√				
Luxembourg	No app							
Malta	Covid- 19 Check		√ [139]					
Mexico	Self diagnostic		√					
Monaco	French app	√						
Morocco	Wiqaytna	√	√					
Netherlands	Coronamelder In development	√						
	OLVG Corona app		√					
North Macedonia	Stop Korona!	√						
Norway	Smittestopp – suspended 6/16[140]	√				√		
Poland	ProteGO Safe	√						
	Kwarantanna Domowa		√	√				
Portugal	STAYAWAY COVID In development	√						
Russian federation	Social Monitoring			√				
San Marino	Unknown			√				
Senegal	Daancovid19	√	√	√		√		
Serbia	Unknown							
Slovak Republic	COVID19 ZostanZdravy	√		√				
Slovenia	Ostani Zdrav In development	√						
Spain	Radar COVID		√					
Switzerland	SwissCovid	√				√		
Tunisia	Stop Corona	√						
	E7mi		√					
Turkey	HES	√	√	√		√	√	
Ukraine	Name unknown		√	√		√		
United Kingdom	NHS Covid-19 contact-tracing app	√						
Uruguay	CoronavirusUY	√	√					

In **Finland, Lithuania, Malta, Mexico,** the **Netherlands, Poland** and **Slovenia** apps and websites are developed for self-diagnosis. In Finland, a web-based symptom checker has been implemented. The symptom checker enables anyone to analyse his/her symptoms, get reliable guidance/information and contact health care for further guidance and testing. A similar website with a health questionnaire from the Dutch National

138. Source: https://github.com/ct-report/summary
139. *Malta Independent*, Coronavirus: Take the test – web app launched, 30 April 2020, available at https://www.independent.com.mt/articles/2020-04-30/local-news/Coronavirus-Take-the-test-web-app-launched-6736222624\
140. Source: https://github.com/ct-report/summary

Institute for Public Health and the Environment was taken offline twice due to structural information security problems. The website should have shown an anonymised map of the Netherlands showing zones with high grades of infection.[141] As described in the first part of this report, the Slovenian website was suspended pending completion of a Data Protection Impact Assessment.

The **Lithuanian** app enables daily coronavirus symptom tracking, and the receiving of health advice and information. The **Mexican** app gives direct access to the epidemiological health care telephone number and provides a map that identifies the closest health units to the user's location. The app also provides information about the virus, tips to prevent infection and official government news about the pandemic. In **Uruguay**, the CoronavirusUY app is aimed at people that suspect they are infected with the virus. In a second phase, all people that have been diagnosed with the virus will be invited to download the app. The Uruguayan Ministry for Health has assured that the app does not collect geolocation data of the app users, and that the data are not used for any other purpose.[142]

In **Armenia**, the Covid-19 app is presented as producing daily statistics of recorded cases, (legal) decisions, a list of medical institutions, instructions to avoid infection, as well as tools for public control, including an opportunity to submit an online report on violations of the rules by other people or to fill in a mandatory electronic movement form.

In **Azerbaijan**[143] and **Ireland**, the app provides news and information sources about the pandemic. The app in Azerbaijan enables direct contact to the Anti-Coronavirus Hotline in one touch.

Only two countries that answered the questionnaire (**Argentina** and **Austria**) plan to use the app for crowd control, while seven countries plan to use data from the app to map (aggregated) travel patterns (**Argentina, Czech Republic, Georgia, Norway, Senegal, Switzerland and Ukraine**). In addition, **Turkey** uses its HES app to map intercity travels by train and by plane.

According to the answers to the questionnaire, eight countries plan to use the app to enforce quarantine measures. These countries are **Argentina, Austria, Hungary, Lithuania, Senegal, Slovak Republic** and **Ukraine**. It seems from public sources that **Poland**, **San Marino**, **Turkey** and **Russia** also use(d) an app for this purpose.

Initially, **Poland** only developed an app to enforce quarantine measures. Use of this Home Quarantine app would be mandatory for everybody that notified officials they had contracted the virus, or because they returned to Poland from abroad. The app collected detailed location data and required people to upload selfies when prompted so that officials could pinpoint their exact location.[144] The use of this app is not mandatory. Later, Poland also decided to develop a proximity tracing app based on the decentralised proximity tracking technology of GAEN.[145]

Hungary has also developed an app to enforce quarantine measures, The *Házi Karantén Rendszer* app (The Home Quarantine System, HKR). People who have been officially quarantined for Covid-19 infection have to be registered, and their location data are monitored. At randomly generated times, the HKR system sends remote control requests via SMS, and a health assessment questionnaire once a day. Users have to start the app within 15 minutes of receiving the request. The app automatically takes several pictures of the user, to provide proof of their identity and location. These data are then compared with the address of the home quarantine provided during registration.[146] The data are sent to the GP from the patient, and are used in an aggregated, anonymised form to predict health needs.

Since April, based on a decree of the mayor of **Moscow**, infected patients must install the Social Monitoring app if they wish to do the quarantine at home. Prior to installation of the app, "the nurse takes a picture of the patient and records the data in an identity document. This information is transferred to a single data center

141. MBS News, RIVM website Infection radar temporarily offline after data breach, 7 June 2020, available at https://www.mbs.news/en/2020/06/rivm-website-infection-radar-temporarily-offline-after-data-breach-inland.html.
142. Uruguay Ministry for Health, Coronavirus UY: this is the app designed for those who suspect they have Covid-19, in Spanish only, available at https://www.elpais.com.uy/informacion/salud/coronavirus-uy-asi-app-covid-presento-gobierno-hoy.html.
143. Explanation in the app stores about the purposes of the Watch COVID" (*COVİD izlə*) app for iOS and Android devices, for Apple available at https://apps.apple.com/az/app/covid-izle/id1511326016
144. *Politico*, Poland's coronavirus app offers playbook for other governments, 2 April 2020, available at https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/
145. Reuters, Poland rolls out privacy-secure coronavirus tracking app, 9 June 2020, URL: https://www.reuters.com/article/us-health-coronavirus-poland-tech-idUSKBN23G208
146. Translated in English, the app description is: "Anyone who has been placed in official home quarantine can decide whether they want to take advantage of the HKR system by continuously fulfilling remote monitoring requests through the application or by undertaking personal police control during the quarantine period without using the application." Hungary, HRK app information (in Hungarian only), available at https://hazikaranten.hu/

and the "Social Monitoring" service."[147] On installation the app collects to confirm the phone number, and the user must make a selfie. After that, the app continuously collects location data from the smartphone. The Moscow authorities combine these data with city video surveillance to enforce quarantine orders. If a patient refuses to use the service, he or she faces a fine of 4 000 rubles. In addition, the patient will be placed in an observatory or medical facility and will not be able to return to home treatment. The tracking data are stored on the city hall's server for one year.[148]

Similarly, the **Turkish** Ministry for Health created the '*Hayat Eve Sığar*' (HES) app (*Life fits inside the house*) as part of the Pandemic Isolation Tracking app.[149] If citizens in quarantine leave their house, they immediately receive a warning via SMS. Persons that wish to travel by train or plane between cities in Turkey have to show a code from the app. Only if the app confirms that they have not been infected with the virus will they be allowed to travel.

Liechtenstein does not use a mobile app, but is testing[150] an existing electronic bracelet that measures skin temperature, pulse, respiration and blood flow.[151] The Liechtenstein government funds the test on 2 200 of the 38 000 inhabitants of the principality, in the hope it can also detect Covid-19 infection in early stage.

According to the answer received, wearable technology is also used in **Cyprus**.

Even if the use of such wearable technology is strictly voluntary, data protection risks exist for the users, as people may feel pressured to demonstrably wear the bracelet, while the reliability of measurements has not been proven and the potential consequences of a wrong conclusion about the health of the wearer can be serious (mandatory quarantine, exclusion from the workplace, social exclusion, stigmatisation, discrimination, etc).

C. Public engagement and private sector involvement

Although **Sweden** did not launch any official government app, researchers at Lund University in Sweden have launched a free app to help map the spread of infection in Sweden and increase knowledge of the coronavirus.[152]

In **Germany** and in the **Netherlands**, there was a fierce public debate about the privacy risks of a contact tracing app. In Germany, the development of the CoronaWarn app was critically followed by the federal data protection authority (BfDI) that did not see any objection against its use.[153] Germany conducted and published a very detailed data protection impact assessment.[154]

17 countries conducted a DPIA to mitigate high risks, but the DPIA was only published in 9 countries: next to **Germany**, in **Austria, Ireland, Mauritius, the Netherlands, Norway, Liechtenstein, San Marino,** and **Ukraine**. The United Kingdom announced it will also publish the DPIA at the public launch.

A number of privacy academics and experts in the **Netherlands** created a manifesto 'Safe against Corona', with 10 conditions for the app to comply with. In addition to the above mentioned criteria from the Parliament of Luxembourg (protect privacy, disclose the source code, communicate with other European apps and not allow data identifying individuals to be collected centrally), the Dutch signatories demanded that the app could only be used for one purpose (controlling the virus), that it should be demonstrably effective, that the

147. https://www.mos.ru/news/item/73074073/ See also Human Rights Watch, Russia: Intrusive Tracking App Wrongly Fines Muscovites, available at https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites
148. Idem.
149. Human Rights Watch, Mobile Location Data and Covid-19: Q&A, section Mobile Apps to Enforce Quarantine and Social Distancing Orders, available at https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa See also: duvaR.english, Health Ministry's mobile app for travel may breach privacy law, experts warn, available at https://www.duvarenglish.com/health-2/coronavirus/2020/05/25/health-ministrys-mobile-app-for-travel-may-breach-privacy-law-experts-warn/ More information about the Pandemic Isolation Tracking Project is available on the official site of the Directorate of Communications, available at https://www.iletisim.gov.tr/english/haberler/detay/director-of-communications-altun-shares-a-post-on-pandemic-isolation-tracking-project
150. *Basler Zeitung*, Liechtenstein als Corona-Labor, Fruchtbarkeits-Armbänder gegen das Virus, 18 April 2020, https://www.bazonline.ch/das-liechtenstein-experiment-867253873911 See also the manufacturer information, https://www.avawomen.com/ava-bracelet-for-covid-19/
151. ICO Liechtenstein, What a COVID-19 Bracelet Says about Liechtenstein, 7 August 2020, https://www.ico.li/what-a-covid-19-bracelet-says-about-liechtenstein/
152. https://www.lunduniversity.lu.se/article/covid-symptom-tracker-app-launched-sweden
153. German magazine *Datenschutz Praxis*, Data protection with the Corona-Warn-App: The most important facts, 18 June 2020, (in German only) available at https://www.datenschutz-praxis.de/fachnews/datenschutz-bei-der-corona-warn-app-die-wichtigsten-fakten/
154. Corona Warnapp DPIA (in German only), 15 June 2020, available at https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf

results should be reliable and verifiable through publicly, user friendly, available source code that use of the app should be temporary and never imposed through coercion by governments or third parties.

The development of a contact tracing app by the Dutch Ministry for Health was preceded by an *appathon*, with public presentations by seven selected app developers (chosen out of 700 proposals).[155] Immediately after the weekend, the Dutch data protection authority reported that it could not assess the privacy impact because of the unclear legal requirements and purposes and the seven proposals were also criticised in a security audit.[156] In the end, none of the seven proposed apps met the data protection requirements and the Netherlands is currently working on a new contact tracing app, developed under full public scrutiny, with a chat module open for all interested people and a github repository where the source code is published.

A similar open development approach, with intensive collaboration between public authorities, volunteers and the private sector, was chosen in **Estonia** and **Senegal**. In March 2020, **Estonia** organised a *hackathon* (*Hack the Crisis*) to inventorise good ideas to contain the Corona virus.[157] One of the winning ideas was a health monitoring app which can be used to track the extent of an outbreak. As well as helping users identify their symptoms, the app also warns of nearby virus hotspots.[158] Since April 2020, nine Estonian companies and several government institutions are developing a decentralised, privacy-preserving contact tracing application.[159]

In **Senegal**, a platform of more than 450 volunteer digital experts was set up. This initiative, called *Daancovid19*, involves people from the private sector, civil society, and the research and innovation sector. The platform was initiated by the Organisation of Information and Communication Technology Professionals (OPTIC), and was adopted by the Ministry for Health and Social Action (MSAS) and the Ministry of the Digital Economy and Telecommunications (MENT).[160] The call for digital solutions resulted in 29 different solutions, ranging from different types of tracking apps to a remote controlled robot to assist with the care for infected patients. According to the students from the technical university that presented the idea, *Docteur Car* should be able to measure temperature and deliver medicine and food. The robot should be able to speak multiple languages such as Wolof, Pulaar, French and English.[161]

D. Transparency and Open source

As shown in table 4 below, many countries have made the source code of their apps open source in order to increase transparency and provide a higher level of trust amongst the general public. The Free Software Foundation Europe keeps track of the apps, and has for example called on Denmark to release the code of the app under a Free Software (Open Source) license.[162]

Table 4 – Countries that publish the source code of the apps

Country	Name of application	Open Source URL
Austria	Stopp Corona	https://github.com/austrianredcross
Belgium	In development[163]	To be published on github
Cyprus	COVTRACER	https://github.com/ct-report/CY
Czech Republic	eRouška ("eFaceMask")	https://github.com/covid19cz?q=erouska

155. Dutch Ministry for Health, Welfare and Sport, Health ministry to hold digital event to test coronavirus apps, 15 April 2020, https://www.government.nl/ministries/ministry-of-health-welfare-and-sport/news/2020/04/15/health-ministry-to-hold-digital-event-to-test-coronavirus-apps
156. Dutch DPA, Privacy corona-apps not demonstrated (in Dutch only), available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-corona-apps-niet-aangetoond
157. https://www.weforum.org/agenda/2020/07/estonia-hackathon-pandemic-covid19-technology/
158. https://www.velmio.com/corona-tracker
159. E-estonia, How do you trace Covid-19 while respecting privacy?, April 2020, https://e-estonia.com/trace-covid-19-while-respecting-privacy/
160. https://daancovid19.sn/
161. https://daancovid19.sn/communique-de-presse-daancovid19-29-solution-numeriques-referencees-dans-le-cadre-de-la-lutte-contre-le-coronavirus/
162. FSFE, Denmark keeps source code of Coronavirus tracing app secret, 29 June 2020, available at https://fsfe.org/news/2020/news-20200629-01.en.html
163. https://www.computable.be/artikel/columns/overheid/6963986/5658341/blyaert-betwist-geen-corona-app-voor-eind-september.html

Finland	Ketju In development[164]	https://github.com/ct-report/FI
France	STOPCOVID	https://github.com/ct-report/FR
Germany	Corona-Warn-App	https://github.com/ct-report/DE
Hungary	VirusRadar	https://github.com/ct-report/HU
Iceland	Rakning C-19 App	https://github.com/aranja/rakning-c19-app
Ireland	Covid Tracker	https://github.com/HSEIreland/
Italy	Immuni	https://github.com/immuni-app
Latvia	APTURI COVID	https://github.com/ApturiCOVID
Monaco	Uses French app	https://github.com/ct-report/FR
Morocco	Wiqaytna	https://github.com/Wiqaytna-app
Netherlands	Coronamelder In development	https://github.com/minvws
Norway	Smittestopp – suspended by DPA 6/16[165]	https://github.com/ct-report/NO
Poland	ProteGO Safe[166]	https://github.com/ProteGO-Safe
Slovak Republic	COVID19 ZostanZdravy	https://github.com/ct-report/SK
Switzerland	SwissCovid	https://github.com/ct-report/CH
United Kingdom	NHS Covid-19 contact tracing app	https://github.com/NHSX

The publication of the source code may help to build confidence in the system, as an important aspect of transparency, and provides means of control of the respect for the rights to privacy and data protection. According to a study about the acceptance of mock tracing apps by a researcher from the German university of Göttingen, arguments on societal benefits related to the use of apps were found among the most appealing elements even for the most sceptical and undecided persons.[167]

E. Users' expectations

Trust in such digital solutions is instrumental to the level of adoption, and thus the effectivity of the system. Users must be assured that their right to personal data will be respected and a lack of clarity in the purpose specification, mixed messages about the legal grounds, a failure to apply rigorous data minimisation and no fixed, or very long, retention periods seem to be amongst the common concerns of users.

In reply to the questionnaire, only 15 respondents indicate that the app data are exclusively provided to a national health authority bound by medical secrecy, with the explicit consent of users. The majority of countries that have answered share the data with other authorities too, on the basis of other legal grounds. These may be metadata[168] about the use of the app, or aggregated data. Similarly, data minimisations is only applied rigorously during collection and transmission in half of the responding jurisdictions, and only half of the respondents indicate that all data will be deleted after a fixed period of time.

An explicit legal sunset clause limiting the period of time of the use of the app is foreseen in **17 countries**. These are: **Bulgaria, Czech Republic, Denmark, Finland, Georgia, Italy, Latvia, Liechtenstein, Morocco, Norway, San Marino, Senegal, Slovak Republic, Netherlands, Tunisia, Ukraine and Uruguay**.

164. https://github.com/ct-report/summary
165. Idem.
166. https://koronazglowy.com/
167. Trang, Simon; Trenz, Manuel; Weiger, Welf H.; Tarafdar, Monideepa; Cheung, Christy. 2020. One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps, in: *European Journal of Information Systems*, available at https://www.tandfonline.com/doi/full/10.1080/0960085X.2020.1784046
168. Data that describes other data or an underlying definition or description of data (data about data). Metadata makes finding and working with data easier – allowing the user to sort or locate specific documents. Some examples of basic metadata are author, date created, date modified, and file size. Metadata is also used for unstructured data such as images, video, web pages, spreadsheets, etc.

To conclude, it is important to stress that this global health crisis was also a unique opportunity to join forces in combating the Covid-19 and exchanging information and experience. Regretfully, in spite of numerous calls for coordination and interoperability of digital solutions, countries have individually implemented widely diverging systems, thereby indirectly limiting the efficiency of the measures taken, and depriving themselves of a possible influence that together, they could have exercised on actors of the digital market.

Given the extremely tight time pressure imposed on all countries, scarce expertise and resources could have been more efficiently invested on research and development of common effective digital solutions. Measures that have been adopted and implemented in a haste have also affected the quality and effectiveness of the contribution and intervention of supervisory authorities and other competent advisory and oversight bodies. Supervisory authorities and other competent bodies should be given the means to carry out independent assessments of the elements provided to them by governments.

To mitigate the risks of ad hoc measures or fragmented approaches and to contribute to the effectivity of applications by a large uptake, it is essential for governments and other relevant stakeholders to build trust together, closely involving the civil society and the general public in the development of those digital solutions and investing in transparency measures (publication of the source code, dissemination of the findings of data protection impact assessments, organisation of *hackathons/appathons*, etc).

2020 has been a turning point on many grounds, including in respect of data protection.

Challenges faced worldwide by societies, governments and health care systems provided a unique opportunity to reaffirm our founding values of democracy, rule of law and human rights. When confronted with the Covid-19 health crisis, governments have been seeking to protect their populations and responding effectively to urgent and vital needs. Emergency measures were adopted that have affected the enjoyment of the rights to privacy and data protection. At the same time, the use of technologies providing distance communication in lieu of human contacts, and algorithms replacing human intervention simply exploded. Digital technologies used in public places to monitor population, at home, while teleworking or self-diagnosing, or when learning remotely, became the new 'normal' of our lives.

The manner in which the health crisis has been addressed prompts a reaffirmation of the resilience of the data protection principles as a key component of the effective functioning of our democracies. Greater awareness and compliance with those requirements contribute to increase the individuals' trust in actions taken by their governments and a greater acceptance of the measures adopted in the general interest. The future lies in our capacity to react promptly to new challenges without undermining our core values and putting our societies at greater risk on the longer term than do the present threats we have to address.

This report takes stock of the digital solutions adopted or planned in the context of the Covid-19 in over 50 countries from Africa, Europe and Latin America. It gives insights on the legal and technical measures that were adopted, and of their impact on data protection.

PREMS 120820

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE