

Version 14 April 2020

Ensuring data privacy as we battle COVID-19

Key messages

- Many governments are taking unprecedented measures to track, trace and contain the spread of the novel coronavirus (COVID-19), by turning to digital technologies and advanced analytics to collect, process and share data for effective front-line responses.
- While the exceptional measures implemented or envisaged in some countries may ultimately prove effective in limiting the spread of the virus, some approaches have proven controversial in terms of their risk of violating privacy and other fundamental rights of citizens, particularly when such measures lack transparency and public consultation.
- Privacy enforcement authorities have generally endorsed a pragmatic and contextual approach at times of crisis or a state of emergency, and exercised enforcement discretion recalling that respect for fundamental data protection and privacy principles do not stand in the way of necessary and proportionate front-line responses to COVID-19.
- Policy makers, in consultation with privacy enforcement authorities, must assess the possible trade-offs in data utilisation during this crisis (reconciling the risks and benefits), but must ensure that any extraordinary measures are proportionate to the risks and are implemented with full transparency, accountability and a commitment to immediately cease or reverse exceptional uses of data when the crisis is over.

Some digital responses to the crisis have precipitated novel data governance and privacy challenges

Governments are taking unprecedented measures to track and contain the spread of the novel coronavirus (COVID-19), and are harnessing the power of data to drive digital solutions. Of particular importance to an effective front-line response is data concerning the spread of the virus, such as the location and number of new confirmed cases, rates of recoveries and deaths, and the source of new cases (international arrivals or community transmission). Data is also crucial to assess and improve the capacity of health care systems, and to evaluate the effectiveness of containment and mitigation policies that restrict the movement of individuals. Many governments are turning to digital technologies and advanced analytics to collect, analyse and share data for front-line responses, in particular, (i) geolocation data that are user-derived from mobile call data records or collected from mobile applications; and (ii) biometrics, particularly facial recognition data.

Timely, secure and reliable data access and sharing are thus critical to understanding the virus and its spread, improving the effectiveness of government policies, and fostering global co-operation in the race to develop and distribute therapies and vaccines.

But some responses to the crisis are giving rise to novel data governance and privacy challenges. For instance, contact-tracing technologies can be useful as they provide critical information to limit the spread of the virus, but if left unchecked, they can also be used for extensive collection and sharing of personal data, mass surveillance, limiting individual freedoms and challenging democratic governance.

Few countries have frameworks in place to support the extraordinary contact-tracing and population-wide surveillance measures envisaged

The measures envisaged in some countries have already proven to be controversial in terms of their risk of violating privacy and other fundamental rights of citizens, particularly when such measures lack transparency and public consultation. Even when the personal data is anonymised, recent research suggests that individuals may still be identified by a limited set of data points – four spatio-temporal points may be enough to uniquely identify 95% of people in a mobile phone database of 1.5 million people and to identify 90% of people in a credit card database of 1 million people.

Few countries have frameworks in place to support these extraordinary measures in ways that are fast, secure, trustworthy, scalable and in compliance with existing privacy and data protection regulations. As a result, many countries recently have passed or are about to pass laws specifying how data collection will be restricted to a certain population, for what time, and for what purpose. For instance:

- The Italian government published a Decree to create a special legal framework for collecting and sharing personal data related to health by public health authorities and by private companies that are part of the national health system for the duration of the state of emergency.
- The German government has proposed to amend the Infection Protection Law to allow the Federal Ministry for Health to require “risk” persons to identify themselves, and to provide information about their travel history and contact details. The original proposal, giving broader authorities to use technical means to identify potential sick persons and obtain geolocation data from telecommunications providers, has been withdrawn partly due to strong criticism from the Federal Privacy Commissioner.
- French senators during the examination of the emergency law project proposed an amendment 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 amendment was rejected as being too great of an incursion on privacy rights.

Other governments have collected and processed geolocation data related to COVID-19 without the need to adopt new legislation. For instance:

- Authorities in the Republic of Korea already have extraordinary powers to collect personal data if "necessary to prevent infectious diseases and block the spread of infection" (Infectious Disease Control and Prevention Act, Article 76-2).
- In Singapore, relevant personal data can be collected, used and disclosed without consent during an outbreak to carry out contact tracing and other response measures.
- In Israel, the government has issued emergency measures that allow the use of technology developed for counterterrorism purposes to track infected persons by monitoring mobile phones.

Privacy enforcement authorities have a key role to play as governments enact emergency legislation and data controllers seek legal certainty

Despite the scale of the public health and economic challenges posed by the COVID-19 pandemic, it is crucial that governments and private sector actors do not back-track from fundamental data governance and privacy principles. Privacy enforcement authorities (PEAs) have a key role to play in advising on proposed new government legislation and providing clarity regarding the application of existing privacy and data protection frameworks. PEAs may need to offer innovative and forward-looking solutions, particularly when it comes to important questions of deletion and retention of personal data, reversibility of new government controls, and the exercise of their audit and investigative powers.

As of mid-April 2020, PEAs in Argentina, Australia, Canada, Finland, France, Germany, Ireland, New Zealand, Poland, Slovakia, Switzerland and the United Kingdom have published general guidance for data controllers and processors about the application of their privacy and data protection laws in the crisis. PEAs have generally endorsed a pragmatic and contextual approach, and exercised enforcement discretion recalling that respect for fundamental data protection and privacy principles do not stand in the way of necessary and proportionate front-line responses to COVID-19. The European Data Protection Board and the Council of Europe have released similar statements explaining that the General Data Protection Regulation (GDPR) and Convention 108 do not hinder measures taken in the fight against the pandemic, but do require that emergency restrictions on freedoms be proportionate and limited to the emergency period.

Some PEAs have published specific guidance, such as which rules apply to the use of information on social media for tracking potential carriers (e.g. Hong Kong, China), and what the government is doing in relation to coronavirus scams and unsupported claims about products that can treat or prevent the virus (e.g. in Spain and the United States).

In other cases, PEAs are responding in innovative ways. The United Kingdom Information Commissioner's Office has, for example, announced that it will recognise the urgent public interest in the application of its data protection law and enable data controllers to balance their obligations with their capacity to respond to subject access requests. The Global Privacy Assembly, a worldwide consortium of privacy and data protection regulators, has established a dedicated resources page that collates the latest guidance and information from its members.

Key recommendations

Policy responses are evolving rapidly in an environment with limited reliable evidence or opportunity for robust internal or multilateral consultations. However, all countries urgently need data to inform regulatory and policy responses as the crisis unfolds. The following considerations, which build on OECD data governance and privacy principles, should guide those data collection and sharing practices.

- **Governments need to promote the responsible use of personal data**. There appears to be an increasing trend towards the use of more invasive collection, processing and sharing of large-scale personal health and behavioural data that involves targeted monitoring of individuals to contain the spread of COVID-19. While some of these measures may prove effective in helping contain the outbreak, governments should ensure these tools are implemented with full transparency, accountability

and a commitment to swiftly cease or reverse exceptional uses of data when the crisis is over. Data controllers must still have a lawful and fair basis to collect and use personal data.

- **Governments should consult PEAs *before* introducing measures that risk infringing on established privacy and data protection principles**. PEAs should be consulted in the front-line response efforts to ensure that incursions into privacy rights are accompanied by appropriate safeguards. PEAs and governments must dedicate expert resource to enable these assessments.
- **PEAs should address regulatory uncertainties**. They should adopt a pragmatic and contextual approach in responding rapidly to requests for advice and clarifying how data protection and privacy frameworks in each jurisdiction apply to the collection and sharing of personal data in this crisis. Doing so will likely foster compliance with these frameworks, and enable efficient internal and trans-border data flows.
- **Subject to necessary and proportionate safeguards, governments should support national and international co-operation in collecting, processing and sharing personal health data for research, statistics and other health-related purposes in managing the COVID-19 crisis**. This includes the adoption of privacy-preserving solutions for data access and sharing and, where appropriate, engaging in and leveraging public-private partnerships to facilitate data sharing.
- **Governments and data controllers should be transparent and accountable for all actions they take in response to the crisis**. Governments should ensure the engagement and participation, notably through public consultation, of a wide range of stakeholders with a view to ensuring that the collection, processing and sharing of personal data serves the public interest and is consistent with societal values and the reasonable expectations of individuals.

Further reading

OECD (2020), "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics (COVID-19)", OECD, Paris.

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en.

OECD (2017), *Recommendation of the Council on Health Data Governance*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433.

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

The OECD is compiling data, information, analysis and recommendations regarding the health, economic, financial and societal challenges posed by the impact of coronavirus (COVID-19). Please visit our dedicated page for a full suite of coronavirus-related information.

This paper is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at http://www.oecd.org/termsandconditions.