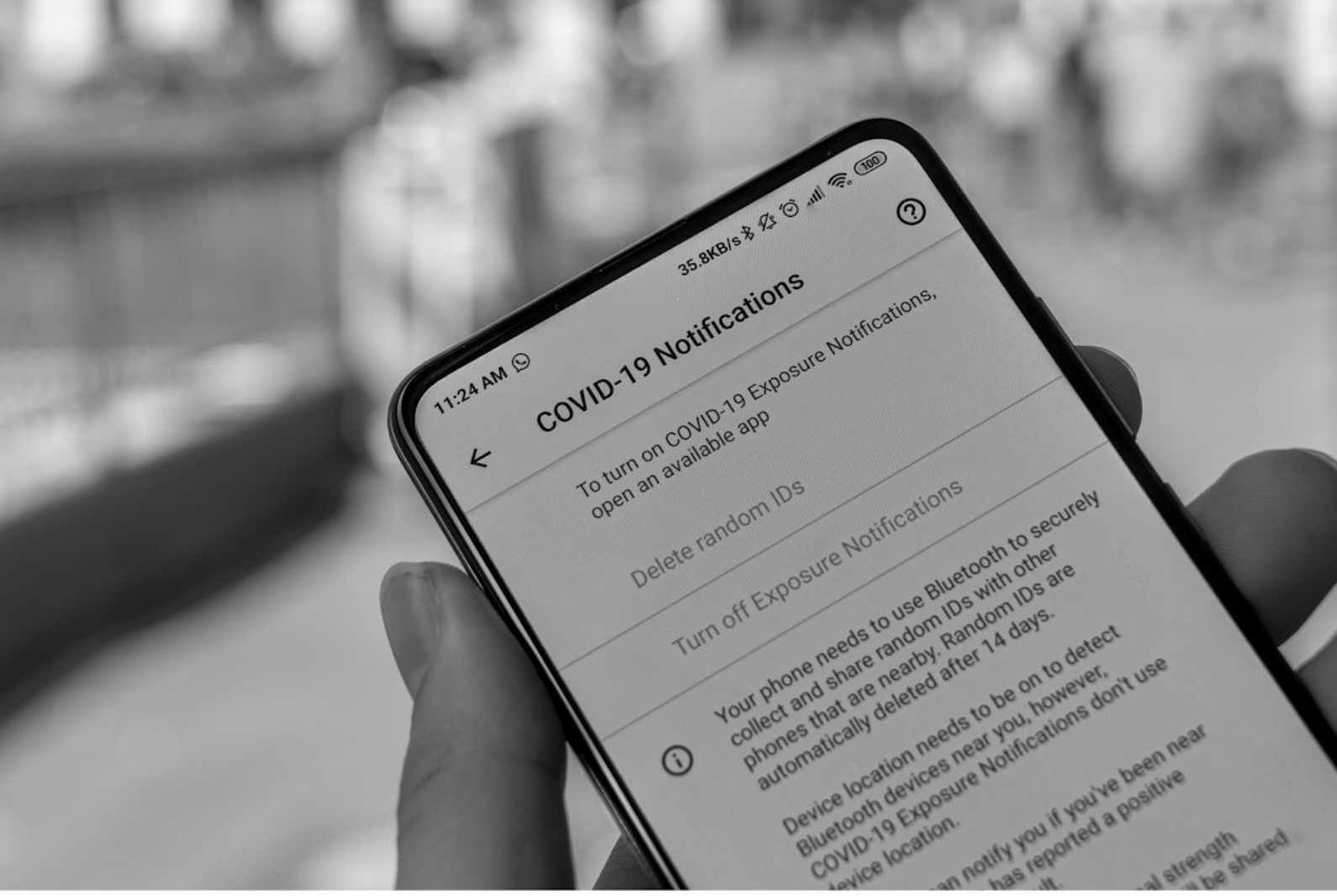


# COVID-19 POLICY BRIEF

## Data & Privacy

WORLD WIDE WEB FOUNDATION

webfoundation.org

# Introduction

Accurate data is absolutely essential when faced with the spread of an infectious disease. In 19th century London, physician John Snow challenged the prevailing belief that polluted air was behind a cholera outbreak by plotting where the disease was spreading. He found that cases were clustered around a water pump in the Soho area of the city and, identifying that as the source, removed the pump handle — one of the earliest cases of epidemiology.

Today we produce more data than ever before, driven partly by the digital devices we keep in our pockets, on our wrists and in our homes. The wealth of information we're creating can be used to understand how and where Covid-19 is spreading and to develop strategies to tackle it. We need innovative and responsible approaches to using this data to help tackle this public health crisis, and we need to be able share that data, insights and knowledge, across borders.

Of course, this is just one part of a response that must also include sound policies, clear communication, well-resourced healthcare systems, manual contact tracing and much besides. But "good" data — including personal data — can give health authorities, doctors and researchers critical insight to inform strategies to limit the spread of the disease.

The good news is this doesn't have to mean putting people's human rights on pause or lowering the bar for privacy. The recommendations outlined in this brief are designed to make sure that people's data is protected while still being used to fight the spread of Covid-19.

## Data can help us fight the pandemic

Different types of data are needed to fight the pandemic, and this data must be accurate and timely. In some cases, the data can and should be aggregated or anonymised, for instance to create heat maps to help public authorities understand population movements and to monitor how the public is responding to social distancing orders, or to model the geographic spread of epidemics.

In other cases we will also need data at the individual level. This could include data gathered by contact tracing apps, but also personal data collected manually, for example by human contact tracers or medical professionals treating patients. In these cases, strong privacy protections are particularly critical.

## Privacy and public health do not have to be at odds

This debate is often framed as a "trade off" between privacy and public health. In order to beat the disease and end the crisis, the argument goes, we should accept some exceptional compromises to our privacy. But this debate unhelpfully presents the right to privacy as incompatible with the need for strong action to protect public health in an emergency.

Privacy should always be prioritised when data is collected and used. And effective privacy laws and frameworks are designed to allow for the use of data when essential to public health and in the public interest, while guarding against improper intrusions to our privacy.

In other words, privacy rules are designed to work in exceptional circumstances, not just business as usual. Countries that have robust privacy frameworks on the books, and who enforce those laws effectively, are not in unchartered territory.

Therefore we should push back on governments or companies who seek to use Covid-19 as an excuse to collect and use people's data in ways that are inconsistent with human rights and the rule of law. Equally, when critics and advocates argue against the use of data on the basis that there are no or few legal, policy or technical principles and protections for people's data, we should point to the frameworks that exist to facilitate data sharing while protecting privacy.

Of course, many countries — including the United States — do not have comprehensive privacy frameworks. They should pass comprehensive privacy laws as an urgent priority. In the meantime, there are a number of global and regional privacy frameworks and principles that governments, companies and civil society can look to, such as the APEC Cross-Border Privacy Rules, the OECD Privacy Guidelines, the General Data Protection Regulation (GDPR) or Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

## Strong privacy rules enable data use in a protective way

Far from being burdensome blockers to using data, good privacy frameworks are intended to provide guidance for the safe and appropriate use of data when it's most needed. Covid-19 has underlined the importance for all countries to adopt comprehensive privacy rules.

Far from lifting or relaxing privacy laws, governments must observe laws where they exist and pass laws where they don't. As the Global Privacy Assembly (GPA) — the group of global privacy regulators — has said:

*"We are confident that data protection requirements will not stop the critical sharing of information to support efforts to tackle this global pandemic. The universal data protection principles in all our laws will enable the use of data in the public interest and still provide the protections the public expects. Data protection authorities stand ready to help facilitate swift and safe data sharing to fight COVID-19."*

The GPA is also publishing guidance, tools and best practices showing how Data Protection Authorities around the world are using data for public health purposes within the bounds of data protection safeguards.

Data protection is not about locking down data entirely, only to roll back all protections to release data when there's an emergency. They set guidelines for the proper use of data according to the purpose and surrounding circumstances.

## Public trust is essential to ensure support for using data

When asked to use a contract tracing app, alert authorities to developing symptoms or consent to their data being used, the public must have trust in such initiatives. If people don't trust governments and companies to treat their data properly, compliance will be too low and therefore ineffective.

Strong data protection rules provide clarity and help build trust in a population that their data will be used appropriately. This can help educate people about data protection issues and mitigate overreaction and resistance to data being used in critical situations.

In recent years we've seen swings in public opinion on data privacy. The Snowden revelations and then Cambridge Analytica sparked anger about how governments and companies were abusing personal data. This drove helpful momentum for privacy legislation, but also prompted a backlash against the sharing of data across platforms where it could actually benefit individuals. Now there's a swing in the other direction as people see that their data can be critical for promoting public health, and are therefore willing to "give up" privacy protections. Rather than let public understanding of and support for data use rise and fall with external events, we need clear, consistent rules around how our data is used. This can help build support for the collection and use of personal data with the appropriate safeguards in place.

# Definitions

| |
|---|
| **Personal data**: Information about a person where that person can be identified by details like their name, identification number, location or one or more details related to their physical, physiological, genetic, mental, economic, cultural or social identity (based on GDPR Article 4(1)). |
| **Aggregated data**: Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data (UK ICO code of practice: "Anonymisation: managing data protection risk code of practice").<br><br>*For example:* statistical data published by public health authorities noting that a certain percentage of the population is overweight |
| **Anonymised data**: Information that doesn't relate to a specific person, or information treated in a way that the person is not or no longer identifiable (based on GDPR Recital 26).<br><br>This means a person cannot be identified directly by name, by using "indirect" identifiers like their phone number or email address, or by using inferred data like location history or internet search history (Irish Data Protection Commission's Guidance Note on Anonymisation and Pseudonymisation).<br><br>Anonymised data is often out of scope of privacy laws like the GDPR. |
| **Pseudonymised data**: Information that can no longer be linked to a specific person without the use of additional information, as long as that additional information is kept separately and is protected (based on GDPR Article 4(5)).<br><br>In other words, pseudonymisation means replacing information that could identify a specific person with a value which doesn't allow a person to be directly identified.<br><br>*For example:* a person's name in a medical record could be replaced with a new identifier like "Patient 12345," but the individual could still be re-identified by the medical professional or anyone else who can access the "key" linking the name to the new identifier.<br><br>Pseudonymised data is often still subject to privacy laws like the GDPR. |

# Policy Recommendations

These recommendations apply to governments, companies and other bodies when collecting and using data for any purpose. Examples include contact tracing apps, aggregated heat maps, manual contact tracing efforts, or collection and use of health data by medical professionals.

---

**Adopt a "privacy by design" approach**

- Privacy considerations should be built in from the very beginning of the development of any product or service.
- For example, determine in early design stages how much data is actually needed to provide the service (data minimisation), rather than collecting lots of data and then deciding how to use it.
- See Contract for the Web, Principle 5 (2)

**Carry out privacy impact assessments**

- Assessments should be conducted to evaluate risks to individuals' privacy and other fundamental rights.
- These assessments should be done regularly and kept up-to-date as the data collection and use continues.
- A version of these assessments, at least at a high-level, should be published so the public has access to the privacy choices made and how their rights may be impacted.
- See Contract for the Web, Principle 6 (1)

**Consult with affected communities**

- A wide range of communities should be consulted — during development and after the release of technologies — to help ensure the rights and interests of all users are considered, factoring gender, race, age, ethnicity, and other intersectionalities.
- See Contract for the Web, Principle 6 (2)

**Employ privacy-preserving technical measures**

- Privacy-preserving measures should be adopted, where appropriate, to help safeguard user privacy. For example, we're encouraged by efforts from MIT and jointly by Google and Apple to develop contract tracing apps that employ privacy-preserving Bluetooth technology.
- Such privacy-preserving technical measures should be considered alongside other factors. Where these would reduce the ability to process data and meet public health goals, the organisation should carefully weigh the risks and benefits.
    - This is consistent with the GDPR's guidance that data protection should be "balanced against other fundamental rights, in accordance with the principle of proportionality" (GDPR Recital 4).

**Be clear about how data will be collected and used**

- There should be clear and transparent communication to users and the broader public about the purposes for which data is collected and used, how long the data will be retained, and the control users have over their data.
- This information should be communicated in multiple ways, including in clear, accessible privacy statements and policies and just-in-time privacy notices.
- Data should only be used for the purposes communicated to and agreed by users.
- Data collected to tackle Covid-19 should only be used for public health or public interest purposes. It shouldn't be used for other forms of surveillance or law enforcement, advertising/marketing, or other incompatible purposes.

**Only collect data that is necessary**

- The collection of personal data should be minimised so that only data essential to achieve the purposes at hand is collected.
- For example, the UK Information Commissioner's Office recommended with respect to contact tracing apps that they should "only collect or otherwise process information that is required for the core purpose (e.g. excluding location data, other device identifiers beyond any that are strictly necessary for the purpose, and personal data such as user account information, etc.)"

**Give people control over how their data is used**

- Users should have control over how their data is collected and used, where appropriate.
- People should be able to opt in/opt out according to the type of data collected.
- They should also be able to access their data where it's being held at the individual level, and edit or delete it.

**Retain data only for as long as necessary**

- Data should be deleted or anonymised when it is no longer needed at the individual, identifiable level.
- If data is to be used for further research or other purposes in the public interest, appropriate privacy protections should be taken, including anonymising data wherever possible.

**Keep personal data safe**

- Ensure there are security measures in place to protect the integrity of the collected data — from external breaches as well as unauthorised internal access and use.

**Ensure strong oversight and governance**

- There must be oversight of how governments and companies are using data in the Covid context, including judicial and regulatory oversight.

---

Suggested Citation: Emily Sharpe. (2020). Covid-19 Policy Brief: Data & Privacy. London: World Wide Web Foundation.

Cover Photo by Mika Baumeister on Unsplash.