# GLOBAL PRIVACY ASSEMBLY EXECUTIVE COMMITTEE JOINT STATEMENT ON THE USE OF HEALTH DATA FOR DOMESTIC AND INTERNATIONAL TRAVEL PURPOSES

## DATA PROTECTION AND PRIVACY AUTHORTIES HIGHLIGHT THE IMPORTANCE OF PRIVACY BY DESIGN IN THE SHARING OF HEALTH DATA FOR DOMESTIC OR INTERNATIONAL TRAVEL REQUIREMENTS DURING THE COVID-19 PANDEMIC

### Background

Governments around the world are implementing measures to stop the spread of COVID-19 whilst also planning for a return to full economic and social activity across borders. For many domestic or international passengers, this has meant sharing health information such as a negative COVID-19 test result or vaccination status as a prerequisite of travel. Digital 'health passports' and 'health codes' have also been proposed.

The potential sharing of these elements of health data, on a mass scale across borders, and across a range of entities, is unprecedented. Digital technology provides the opportunity to do this at speed and scale. Whilst such steps may potentially be justifiable on public health grounds, the sharing of this sensitive information can and should be done in a privacy protective manner. Technology will offer both risks and opportunities to build protections for individuals. Innovation can go hand in hand with privacy.

Since the start of the pandemic, members of the Global Privacy Assembly have advised governments, private enterprises, charities and non-governmental organisations on the design and development of systems that allow the processing of personal health data in a manner that best protects privacy. This statement seeks to complement efforts made at a national or regional level, and contribute to a positive, co-ordinated privacy outcome internationally, reflecting common global principles of data protection and privacy, including privacy by design and default.

### Building public trust by protecting privacy

In order to build trust and confidence in the way in which health data is processed for travel purposes, individuals need to be assured that: their data is handled securely; the data demanded of them is not excessive; they have clear and accessible information to understand how their data will be used; there is a specific purpose for the processing; their data will be retained for no longer than is necessary.

The Global Privacy Assembly Executive Committee recalls that while data and technology can be important tools to help fight the COVID-19 pandemic, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures and need to be part of a comprehensive public health strategy to fight the pandemic. The principles of effectiveness, necessity, and proportionality must guide any measure adopted by government and authorities that involve processing of personal data to fight COVID-19.[1]

The Global Privacy Assembly Executive Committee therefore urges governments, and other organisations responsible for processing health data for the purposes of international travel, to consider and pay due regard to the following principles, which reflect common global data protection principles and practice:

- The processing of health data as a prerequisite of international travel may be justifiable on the grounds of protecting public health, but considering privacy risks at the outset is vital.
- 'Privacy by design and default' principles should be embedded into the design of any system, app or data sharing arrangements regarding the processing of health data for the purposes of international travel. A formal and comprehensive assessment of the privacy impact on individuals before the commencement of any processing is the best method of ensuring data protection by design principles are implemented in practice and underlying risks are mitigated appropriately. Organisations should seek advice or consult guidance from data protection and privacy authorities on this issue.
- Personal data collected, used or disclosed to alleviate the public health effects of COVID-19 require a clearly defined purpose. The purpose should be specific within the broad context of the public health measure. Personal data must not be used in a manner incompatible with this purpose.
- All organizations must operate under relevant and appropriate lawful authority, ensuring that they only process health data when it is necessary and proportionate to do so.
- The data protection rights of vulnerable individuals, who may not be able to use, or may not have access to, electronic devices, must be protected, and alternative solutions should be considered to ensure that such individuals do not suffer discrimination. Similarly, the data protection rights of those who due to their age,

[1] https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Privacy-Data-Protection-Challenges-Arising-in-the-Context-of-Covid-19-Pandemic-EN.pdf



possible health risks or other underlying conditions cannot be vaccinated should also be protected.

- Individuals should be informed of how their data is being utilised, by whom and for what purpose, providing clear and accessible information, recognising the geographical, cultural and linguistic diversity of the people of society who will wish to travel.
- Organisations should collect the minimum health information from individuals or other sources that is necessary for their contribution to protection of public health.
- Measures should be used to address the risks of directly sharing information from health records for travel purposes – privacy by design approaches can include federated identity systems and device level processing.
- The cyber security risk of any digital systems or apps must be fully assessed, taking full account of the risks that can emerge from different actors in a global threat context.
- Organisations should consider carefully for how long data should be retained, and design a retention schedule for the safe deletion of information once it is no longer required.
- Sunset clauses should be built into the design of such schemes, foreseeing permanent deletion of such data or databases, recognising that the routine processing of COVID-19 health information at borders may become unnecessary once the pandemic ends. The schemes should also be reviewed periodically to ensure that the processing remains necessary and proportionate whilst the pandemic is ongoing.