COVID-19 APPS TOOLKIT

How can **Legislators,**
Policymakers,
App developers, operators, **commissioning public entities, &**
The general public

contribute to enhancing checks and balances and ensure that the tools deployed during a pandemic are fit-for-purpose?

Table of Contents

Introduction 1

1. Recommendations for Policymakers & Legislators 3

   For Contact Tracing Apps 4

   For All Types of Covid Apps 20

2. Recommendations for App Developers, Operators and Commissioning Public Entities. 27

   For Contact Tracing Apps 28

   For All Types of Covid Apps 34

Tools for Implementation 39

   Privacy By Design for Contact Tracing Apps 40

   Software Requirements Specification Template 43

   Data Flow Map for Immunity Passport App Template 44

   Privacy Notice for Contact Tracing App Template 45

   Data Protection/Privacy Impact Assessment Template 46

Introduction

Covid-19 prompted governments across the globe to apply measures ranging from traditional epidemiological measures, such as mask mandates and social distancing, to a number of unprecedented technological responses, most notably contact tracing and immunity passport apps.

The Covid App Project is a two-part civil society initiative that stemmed from a research interest in Covid-specific interventions.

Phase 1 of the project covered the use of contact tracing apps in Brazil, Colombia, India, Iran, Lebanon, and South Africa until July 2021, assessed the impact of their use from a public health efficacy perspective and analyzed function creep and unintended consequences, such as limited access to society. This shared research interest drew together six civil society organizations: ALT Advisory (South Africa), Internet Democracy Project (India), InternetLAB (Brazil), Karisma (Colombia), SMEX (Lebanon), and United for Iran. AWO, a data rights agency, provided coordination support.[1]

Phase 2 of the project incorporates technological applications developed since July 2021, most notably "immunity passports" (showing either vaccination status, test results or recovery certificates). Supported by a technical review of a globally representative sample of apps, this study looks at trends in policy, legal and technical approaches around the globe through a review and technical assessment of 11 Covid apps developed (or commissioned) mostly by governments but also by other actors, in Australia, Bahrain, Chile, Indonesia, Israel, the Netherlands, Tunisia, and Western Australia. These countries were selected to be representative of the different continents/regions of the world and to reflect the main trends observed during the research. Other apps reviewed are those developed with what could be considered to have a global reach: WEF's CommonPass and IATA Travel Pass.

The output of this second phase consists of the following:

- The "Covid-19 Apps: Policy, Legal & Technical Trends Report" (hereafter "Trend Report"):[2] Findings and recommendations from phase 2 are presented in this report. It considers approaches to app design and use in terms of public health efficacy and the degree of function creep and unintended consequences for individuals. This analysis informs a set of recommendations and best practices for relevant stakeholders to develop effective and sustainable public health practices.

- The "Report on the privacy risks of COVID-19 software (Part II)" (hereafter "Technical Report"):[3] This report provides an extensive technical review of the 11 selected apps by considering whether they adhere to best practices in data protection, including, but not limited to, privacy by design and data minimization. It also contains recommendations on how best to ensure effective and safe Covid-19 apps.

[1] The results of the Phase 1 research are available here: https://www.awo.agency/latest/covid-19-app-project/
[2] Available here: https://awo.agency/files/Covid-Apps-Policy-Legal-Tech-Trends.pdf
[3] Available here: https://awo.agency/files/Covid-19-Apps-Technical-Review-2022.pdf

- The "Covid-19 Apps Toolkit" (hereafter "Toolkit"): The Toolkit is written based on the findings and recommendations highlighted in both the Technical Report and the Trend Report. It also incorporates and builds on findings identified during phase 1 of the Covid project by the six civil society organization identified above. Overall, the document provides comprehensive best practices and accessible guidance as well as tools for implementation by all stakeholders involved in the pandemic response and/or concerned by such response: Legislators, Policymakers, App Developers, Operators and Commissioning Public Entities, and the Public.

The recommendations presented in this Toolkit focus on ways to enhance measures deployed as part of a pandemic response to ensure efficacy from a public health perspective. They also aim to provide practical guidance to stakeholders involved in the pandemic response to prevent function creep and unintended consequences when tech-based tools are deployed. If this Toolkit provides a baseline of good practices and recommendations, stakeholders may decide to tailor it so as to reflect and address all additional issues specific to their context.

Although these recommendations are divided by the stakeholders directly involved (e. g. Recommendations for Policymakers and Legislators), they are all relevant to all stakeholders.

Finally, the general public could benefit from becoming acquainted with the trends and recommendations presented in this Toolkit in order to raise their awareness of issues that concern them (e.g. What should I be looking for in the privacy policy of a Covid app?). To further facilitate such awareness, each of the two sections of this Toolkit starts with a brief summary for end users: it aims to clarify expectations the general public could have from stakeholders involved in the pandemic response, including regarding a proportionality-based approach respectful of their rights and ensuring public health efficiency.

To ensure global accessibility, the Toolkit is available in seven additional languages:

- Arabic[4]
- Farsi[5]
- French[6]
- Hindi[7]
- Portuguese[8]
- Russian[9]
- Simplified Chinese[10]
- Spanish[11]

[4] Available here: https://awo.agency/files/covid-app-toolkit-ar.pdf
[5] Available here: https://awo.agency/files/covid-app-toolkit-fa.pdf
[6] Available here: https://awo.agency/files/covid-app-toolkit-fr.pdf
[7] Available here: https://awo.agency/files/covid-app-toolkit-hi.pdf
[8] Available here: https://awo.agency/files/covid-app-toolkit-pr.pdf
[9] Available here: https://awo.agency/files/covid-app-toolkit-ru.pdf
[10] Available here: https://awo.agency/files/covid-app-toolkit-zh.pdf
[11] Available here: https://awo.agency/files/covid-app-toolkit-es.pdf

1. Recommendations for Policymakers & Legislators

What could the public expect from these stakeholders involved in the pandemic response and why?

Policymakers and legislators can introduce policies and legal frameworks based on relevant consultations and recommendations from the public health community. For the public, it is important to know that the introduction of such frameworks and safeguards would aim to ensure that the actions of policymakers and legislators are geared to ensuring public health efficacy while adopting a proportionality-based approach. Such an approach would lead to the development and provision of effective safeguards in the development and use of Covid-19 apps to ensure adherence to global best practices that respect people's rights. In practice, if a Covid app is used as an element of pandemic response by a country, the public health efficacy of such an app would become an element of a broader and coordinated Covid-19 strategy which is key to preventing unintended consequences.

End users of Covid-19 apps — including vulnerable communities such as refugees and migrant workers — must be able to maintain access to vital services. To ensure a holistic public health strategy that facilitates trust and is accessible for and easily understood by the public, the apps must be part of a broader evidence-based strategy. This means that if apps are introduced, this is coordinated among the different branches of government at federal and local levels and based on global technical standards, and that their use is combined with test and trace initiatives, social policies and public health policies, such as social distancing. The clear and coordinated use of the app should be combined with (social) media outreach increasing public awareness of and education about the app.

Ultimately, members of the public must be able to trust the government response, which entails the above as well as by preventing function creep or other unintended consequences. This can be achieved by developing and implementing appropriate legal regimes, transparency about data use and data-sharing agreements only to support the public health strategy — not to achieve other political or policy goals. This trust can further be built by ensuring the equal enforcement of public health measures across the country, with independent oversight, and by creating non-digital alternatives, or otherwise preventing punishment for not using the apps.

Public Health Efficacy		
Trend 1		
Contact tracing apps and technology-based measures are deployed in countries with poor or unequal access to the internet and mobile technology	**Evaluation**	Many governments introduced technological measures in response to Covid-19 despite pre-existing disparities regarding internet access and mobile technology adoption. The importance of this problem cannot be overstated since unequal access to smartphone technology can worsen existing inequities and give rise to ethical concerns. Furthermore, by making social security services available predominantly through online platforms, vulnerable communities that are more likely to have poor internet access and no mobile devices may be deprived of vital assistance.
	Recommendation	National authorities should maintain access to vital services for vulnerable populations (particularly refugees and migrant workers).
	How to implement the recommendation?	
	□ National authorities could identify the state of affairs regarding the distribution of critical internet infrastructure in their respective countries to identify areas in need of development. □ Investments could be made in critical internet infrastructure in the identified areas needing development. This could include subsidising mobile phone plans, providing free Wi-Fi hotspots and even digital literacy programmes.	

Public Health Efficacy		
Trend 2		
Apps were often disconnected from the broader public health response and affected by low uptake	Evaluation	The fate of contact tracing apps is closely tied to an uncoordinated pandemic response at national and local levels. Some apps were largely disconnected from the rather sporadic public health strategy, and governments did not prioritize using data effectively. This also meant that apps and other technological measures were not aligned with the needs of the public health system, made especially evident by the lack of data sharing between the central and local government authorities. This led some to argue that the adoption of a contact tracing apps was merely a box-ticking exercise in certain countries to show government engaging in tech-based responses to the pandemic.
	Recommendation	National authorities should develop a unified government response to Covid-19 (or any other pandemic), taking into account both national and local-level government bodies.
	How to implement the recommendation?	
	□ National authorities could embed contact tracing apps in the broader public health and test and trace infrastructure. The apps are most functional when used alongside traditional test and trace systems, which in turn are dependent on sufficient testing capacity and local, regional and national public health authority staff. □ Employ evidence-based policymaking to ensure a proportional and effective public health response.	

Public Health Efficacy		
Trend 3		
Multiple and multipurpose apps are deployed	Evaluation	In many countries, different contact tracing apps proliferated. Especially when developed by individual local governments, several different apps were released that ranged in functionality. In particular, some state governments deployed apps with functionalities beyond contact tracing, such as providing remote healthcare. This was sometimes as a consequence of limited inter-institutional coordination and decentralized public health systems. The array of Covid-19 official contact tracing apps in some countries possibly diluted their overall adoption.
	Recommendation	National authorities should develop a unified government response to the pandemic, taking into account both national and local-level government bodies.
	How to implement the recommendation?	
	□ Ensure a coordinated response among government entities and public health authorities. □ Adhering to global best practice standards for contact tracing apps, such as the GAEN (Google Apple Exposure Notification) API, supports developing a robust infrastructure.	

Public Health Efficacy		
Trend 4		
A lack of public trust and awareness affects contact tracing apps	Evaluation	Adoption of contact tracing apps was hampered by either a lack of public trust or low public awareness in all of the countries under review. Part of this stemmed from poor campaigning around the app, including the absence of focused and targeted communications from the government. Additionally, some apps suffered from concerns around surveillance and privacy, including in some countries the history of abuse of surveillance powers by law enforcement and intelligence services, impacting journalists, opposition leaders, judges, and human rights activists.
	Recommendation	National authorities should improve communication with and through the media. Content should be scientific and delivered in a professional manner to increase public awareness and education.
	How to implement the recommendation?	
	□ Contact tracing apps can only contribute meaningfully if people are aware of their existence and trust the app and the use of people's data by all relevant actors/stakeholders involved.[12] Using global best practices in app design prevents function creep or data leaks to increase the public's willingness to use the app. □ Make people aware of the app's existence and encourage use by different levels of government, public health authorities, media, and the private sector.	

[12] These actors are referred to as data controllers according to data protection laws. The definition is the following: "...a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf". The Organisation for Economic Co-operation and Development - OECD (11 July 2013). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereafter "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"). Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Public Health Efficacy		
Trend 5		
Alternative measures often have a greater public health impact than contact tracing apps	Evaluation	While contact tracing apps attract attention and public debate, alternative measures often have greater reach. Some countries mainly relied on mass screening, targeted testing and lockdown measures, which entailed mobilizing health workers to screen over millions of people. National lockdowns and quarantine measures seemed also significant in stemming the spread of Covid-19.
	Recommendation	National authorities should develop non-tech-based responses to the pandemic as alternatives to a tech-based response using apps.
	How to implement the recommendation?	
	□ Strengthen cooperation and coordination between the public and private sectors to ensure hospital preparedness and embed contact tracing apps in a broader public health strategy, including test and trace and accessible testing. □ Ensure social policies are in place that enable (potentially infected) people to follow policies and guidelines, e.g., prevent pandemic poverty by providing economic support during quarantine or isolating. □ Ensure personal protective equipment is made available to the public (e.g. masks).	

Function Creep and Unintended Consequences		
Trend 1		
Limited recourse to emergency laws, extended use of extraordinary powers	Evaluation	During the period of study, not all the countries of focus declared a national emergency. For those that did, the legal basis for implementing various measures derived from specific provisions within the country's constitution or legal framework. This typically means that, subject to certain conditions and rules, powers can be exercised by the state whilst derogating from the usual human rights standards. However, a state of emergency can negatively impact certain vulnerable communities, especially where the measures implemented entrench and exacerbate existing discriminatory practices. For those countries that did not declare a state of emergency, ordinary legislative provisions together with extraordinary powers were relied on. This differs from declaring a state of emergency given that the basis of such powers lies in pre-existing legislation, typically public health laws, permitting certain measures to be implemented without necessarily being tied to a type of emergency. This may not always be in accordance with explicit provisions in the constitution or legal framework, and therefore gives rise to the possibility that broad powers are exercised without the appropriate checks and balances in place.
	Recommendations	National authorities should introduce public health measures by appropriate legal instruments providing for effective safeguards for individual's rights, including when they are based on a legitimate declaration of an emergency. In future crises, national authorities should conduct human rights impact assessments which will inform the legal framework, including reflections on

		states of emergency and states of disaster, and what would be necessary and justifiable. In a process analogous to that designed to address serious human rights violations, it may be advisable to consider transitional mechanisms that assess the legacy of the practices and norms created during the Covid-19 pandemic and promote accountability and reconfiguration so that exceptionality is not perpetuated.
	How to implement the recommendations?	
	□ Introduce legislation and policies to face another wave of Covid-19 or a new pandemic to limit the need for a state of emergency. □ If a state of emergency is required for a rapid response, there must be a sunset clause stipulating that new public health measures should be strictly time-limited. □ Conduct human rights impact assessments on existing (and upcoming) public health laws before it is necessary to enforce them. The human rights impact assessments must be transparently conducted to ensure both adequate due diligence and public trust.[13] □ Employ evidence-based policymaking to guarantee a proportional and effective public health response. Prevent extended states of exceptionality by using global best practices for policy and impact assessments, supported by democratic adoption and oversight.	

[13] Guidance on how to conduct a human rights impact assessment is available here: https://www.business-humanrights.org/fr/big-issues/un-guiding-principles-on-business-human-rights/human-rights-due-diligence-impact-assessment/

Function Creep and Unintended Consequences		
Trend 2		
Countries have nascent, sometimes unenforced, data protection regimes	Evaluation	In the findings for Phase 1, comprehensive data protection laws during the pandemic were either not yet in force, were still going through the legislative process, or simply did not exist. In general, stronger data protection regimes may strengthen oversight across the countries in question.
	Recommendations	National authorities should expedite the process of bringing into effect data protection laws with the necessary provisions to cover all Covid-related apps and IT-enabled tools. Governments and their private partners should ensure rights-based and transparent regulatory and policy frameworks, with a particular emphasis on privacy rights. Legislation that relates to data protection should be reviewed and harmonized with any separately existing data protection laws.
	How to implement the recommendations?	
	□ Introduce or extend data protection frameworks for using data in the crisis response without introducing new risks. □ Develop a robust oversight infrastructure with an independent data protection authority.	

	□ Harmonize data protection legislation with neighboring countries and align it with global best practices.[14] □ Non-governmental organizations (NGOs), human rights groups and other organizations should continue to provide support to governments regarding enacting and/or better enforcing data protection legislation.

Function Creep and Unintended Consequences		
Trend 3		
Increased and non-transparent data sharing between public authorities	**Evaluation**	Public authorities collecting and sharing data in response to the pandemic is common across governments around the world. The main reason for this is to facilitate and approve applications for internal travel whilst quarantine measures are in place. This involves combining pre-existing datasets as well as those datasets generated specifically for Covid-19. However, the absence of comprehensive data protection laws or other regulatory checks gives rise to function creep and adverse impacts on certain vulnerable communities through the sharing of sensitive personal data with law enforcement and restricting the movement of those typically unable to access online platforms to apply for travel permissions.
	Recommendations	Public authorities and private entities that collaborate to process personal data in a pandemic should prepare and publish impact reports as a good practice of active transparency and accountability.

[14] These include the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" and the General Data Protection Regulation (GDPR) in the EU, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

All apps should be accompanied by critical legal documents such as terms of service and a privacy policy and these documents should be in the public domain.

Provide clear information regarding the type of data collected and for what purpose, where and for how long data will be stored, with whom the data will be shared and for what purposes, and the security protocols for all of these functions.

Privacy policies should list any third-party applications that have access to personal data.

How to implement the recommendations?

- ☐ Include clear sunset clauses in data-sharing agreements.
- ☐ Ensure that data obtained from the private sector is subject to data protection laws and due diligence, including when it is bought or shared voluntarily.
- ☐ Develop and publish data-sharing terms of service, privacy policies and information on what data will be used, by whom, and how.
- ☐ Privacy policies must be understandable and holistic and explain any third-party applications.

Relevant Tools for Implementation

- Privacy Notice for Contact Tracing App Template

Function Creep and Unintended Consequences		
Trend 4		
A lack of public trust and awareness affects contact tracing apps	Evaluation	Adoption of contact tracing apps was hampered by either a lack of public trust or low public awareness in all of the countries under review. Part of this stemmed from poor campaigning around the app, with the absence of focused and targeted communications from the government contributing to public confusion around certain apps. Additionally, some apps suffered from concerns around surveillance and privacy.
	Recommendations	Public authorities should use focused and targeted communication efforts, providing access to accurate and timely information about Covid-19. Content provided should be scientific and professional to increase awareness and education among the public and consequently improve the response to measures and restrictions. Public authorities should hold regular transparent, democratic, and scientific processes of consultation with civil society members.
	How to implement the recommendations?	
	□ Contact tracing apps can only contribute meaningfully to public health efficacy if they are broadly adopted by the public, which requires trust. Employing global best practice standards (e.g., data minimization, purpose specification) and generally preventing function creep are key elements of building and maintaining public trust. See the software requirements specification template further down in this Toolkit.	

Function Creep and Unintended Consequences		
Trend 5		
Discrimination against marginalized groups	Evaluation	Some of the countries under review deployed apps that allowed people to report lockdown violators to public authorities using features that allowed users to report mass gatherings and inter-state travellers in their area. However, this can have grave consequences for marginalized groups, with members of society asked to carry out surveillance on behalf of the state without the commitments to equality that states must usually follow. Users were thus given the opportunity to unfairly penalize certain individuals or even whole groups. While Covid-19 measures, particularly national lockdowns and stringent border controls, impact whole populations, migrants and refugees are at a heightened risk of exclusion or discrimination. Ensuring that vulnerable communities are protected from these risks is not always well-managed, as seen in a number of countries. Many people struggle with travel restrictions, especially when permission to travel could only be obtained via digital platforms. Some even have difficulties in finding housing in the midst of national lockdowns, as was the case in some countries. Covid-19 also intensified the challenges facing rural people and those in informal sectors of the economy, including for instance insufficient water supply and overcrowding. This is in addition to the contentious use of quarantine camps, where migrants were kept in isolation for weeks without being tested for Covid-19 and denied the opportunity to self-isolate.
	Recommendations	Public authorities should enforce public health measures evenly across the country.

		Public authorities should ensure that services for vulnerable populations (such as migrants and refugees) are maintained in order to ensure they can survive the ongoing difficulties associated with the pandemic. Such services include access to healthcare, economic assistance, and education. Public authorities should ensure that no individual is penalized, or denied access to any service, public or private, because of their non-use of Covid apps. Public health measures should be supported by an impact analysis that takes into account the possible consequences the measures could have on vulnerable groups.
	How to implement the recommendations?	
	□ Do not encourage or require people to report on Covid measures "violators", as this is the role of public authorities. □ Enforce public health measures evenly across the country and ensure independent oversight of enforcement as well as redress mechanisms. □ Ensure migrants and refugees are included in public health policies, social security and other support systems. □ Ensure paper-based (non-digital) alternatives for contact tracing apps for people without a smartphone or not willing to use apps. □ Ensure the continuation of asylum applications and clean and safe housing, taking into account novel options such as stays in hotels (that would otherwise have been empty due to the crisis). □ Public authorities should conduct human rights impact assessments which also take into consideration the potential impacts on different vulnerable groups.	

Function Creep and Unintended Consequences		
Trend 6		
Suppression of protests	Evaluation	In some of the countries under review, protests broke out in response to the limited aid provided by national and local governments to address the problems caused by lockdowns and other Covid-related measures. In some cases, this led to law enforcement using disproportionate force to suppress protests, also impacting children, sick, and elderly people. In another country review, it became apparent that protests escalated in response to the government's alleged mishandling of the economic crisis during the pandemic. Protests were also fueled by the lack of government support during national lockdowns, exacerbating the downturn experienced by many. Demonstrations led to casualties during clashes with security forces as authorities attempted to suppress protests, including during national lockdowns.
	Recommendations	Governments should not use anti-Covid policies to intimidate and crack down on political dissidents, nor should policies be used to punish imprisoned dissidents.
	How to implement the recommendations?	
	□ Public health policies and legislative action must be evidence-based and have clearly set goals to combat the spread of Covid-19 and allow social and economic activity to continue as much as possible, and fundamental rights to be fully enjoyed within these confines.	

	□ If they do not exist yet, redress mechanisms should be put in place or maintained in case of violations of fundamental rights during a pandemic. If they do exist, they should be implemented effectively.

Function Creep and Unintended Consequences		
Trend 7		
The tech-based Covid-19 response exacerbated the digital divide and inequalities	Evaluation	The disparities in relation to internet access and the use of mobile technology have an impact on individuals' access to society during the pandemic. This proves to be a critical issue since unequal access to such resources can exacerbate existing inequities and raise ethical concerns. Furthermore, by making social security services available predominantly through online platforms, vulnerable communities, many of whom lack adequate internet access and have few mobile devices, may be deprived of essential services. However, even where platforms are physically accessible, their design can have negative implications that extend beyond vulnerable communities. For instance, some contact tracing apps were only made available in English despite the many local languages that be spoken by its users.
	Recommendations	Digital materials must be developed and made accessible. These materials must be clear and appropriate, accompanied by training and tools that address how to use the relevant app as well as highlighting key data privacy issues. Digital literacy training should be provided to government staff, community health workers, and app users. Public authorities should develop alternative, non-digital means for movement requests and vaccination registration.

	How to implement the recommendations?
	□ Ensure paper-based (and non-digital) alternatives for all Covid-19 response policies and initiatives, including, but not limited to, contact tracing, contact tracing apps and accessing social security. □ Address the issue of remote education which disadvantages children in economically precarious settings. □ Ensure policies and funding to prevent the digital divide from creating a (bigger) gap between children.

Public Health Efficacy		
Trend 1		
Lack of engagement with evidence-based policymaking	Evaluation	Policies and measures attempting to address an emergency should have a sound underlying rationale to ensure that they are effective. Thus, in the context of the Covid-19 pandemic, any public health interventions should be adapted to the specific conditions of the country or region, and supported by relevant scientific research. Governments had varying success at involving public health authorities and other relevant experts in the decision-making process for developing a response to the Covid-19 pandemic.
	Recommendations	Governments should make certain that the relevant critical infrastructure is in place to ensure that, if technology is part of the pandemic response, the technological measures introduced are as effective as possible. Especially in the context of mobile apps or other web-based services, internet infrastructure should be developed so that internet access is sufficiently distributed across the population to support the network usage that such interventions may require. Technological measures used in response to a public health emergency should have an underlying rationale based on relevant scientific research to ensure that such measures address the emergency effectively. Public health authorities or other bodies composed of relevant experts should be adequately involved in the decision-making process so that policymakers can ensure and demonstrate that their interventions are based

on relevant research and are appropriate for the particular circumstances of the emergency being addressed.

How to implement the recommendations?

□ National authorities should identify the state of affairs regarding the distribution of critical internet infrastructure in their respective countries to identify areas in need of development.

□ Investments should be made in critical internet infrastructure in the areas identified as needing development. This could include subsidizing mobile phone plans, providing free Wi-Fi hotspots and even running digital literacy programs.

□ Prior to deployment, policymakers and legislators should verify with experts whether the technology adds substantial value to the fight against Covid-19 or generates too much collateral damage to justify its existence. The outcomes of such debates could be presented in the form of recommendations and submitted to the decision-making committee mentioned below. In any event, these recommendations should be made available to the public on open sources.

□ Set up a committee with decision-making powers composed of: the independent public health sector (epidemiologists), tech specialists, policymakers, and data protection authorities. Ensure that decisions taken by the committee are subject to checks and balances.

Public Health Efficacy

Trend 2		
Lack of public awareness around scientific research underpinning Covid measures	Evaluation	Covid-19 spread rapidly across the world and presented a novel type of risk for most people. The learning curve was therefore steep for governments and citizens alike, and – particularly early on – required taking action with limited knowledge. Many places also saw a surge in conspiracy theories surrounding the disease. There is growing evidence that adherence to social distancing and quarantining, as well as vaccination incentives, is strongly influenced by well-designed public awareness campaigns. In a number of places, these campaigns contributed to more proactive adherence to public health measures, local production of facemasks, where these were not available, and willingness to be vaccinated.
	Recommendation	Create "coalitions of the willing" with broad representation from civil society. Awareness campaigns, both on- and offline, can facilitate adherence to public health measures and prevent loss of trust. Take into account the different demographics, particularly of marginalized communities, and work with trusted groups within those communities.
	How to implement the recommendation?	
	□ Community-based intervention partnerships can effectively increase awareness among marginalized groups.[15]	

Public Health Efficacy

[15] See: https://apps.who.int/iris/rest/bitstreams/1277158/retrieve; https://www.ajtmh.org/view/journals/tpmd/105/4/article-p879.xml; https://www.cdc.gov/pcd/issues/2020/20_0408.htm

Trend 3		
Lack of efficacy of public procurement during Covid-19	Evaluation	Some legal frameworks make provision for expedited versions of the procurement process that allow governments to acquire the resources needed to respond quickly and effectively to the emergency at hand. However, where comprehensive expedited processes for public procurement are not in place or followed, there may be a range of problems, including shortages of essential equipment.
	Recommendation	Have in place permanent, as opposed to ad hoc, rules for public procurement during emergencies to ensure a more efficient acquisition of goods or services. This could also be coupled with advance purchasing arrangements to quickly secure goods and services that may be needed to address the emergency in question.
	How to implement the recommendation?	
	□ Introduce draft public procurement legislation that reflects the relevant parts of the UNCITRAL Model Law on Public Procurement or another similar international standard, paying special attention to those provisions pertaining to public procurement in cases of extreme urgency. These provisions may include, for example, that: • Single-source procurement is permissible where there is an urgent need to do so due to a catastrophic event in which other methods of procurement would be impractical because of the time involved in using those other methods (reflects Article 30.5(b) of UNCITRAL). • Negotiations should be held with the supplier to determine the proposal and price unless the circumstances of the procurement are such that negotiations are not feasible (reflects Article 52 of UNCITRAL). • Goods or services may be procured from certain suppliers in urgent cases in accordance with agreements concluded between the state and those suppliers prior to the emergency causing the urgency.	

Function Creep and Unintended Consequences		
Trend 1		
Lack of legal framework for the deployment and use of Covid apps	Evaluation	In some of the countries of focus, the apps and measures to combat Covid-19 were often deployed without legal frameworks in place to regulate their use or permitting national authorities to create and deploy Covid apps. In some cases, there was no legislation in place regarding the processing of personal data required for the Covid apps to function. Because of these legislative omissions, function creep became an increasing possibility, meaning that national authorities could use these measures and personal data for initiatives beyond Covid-19.
	Recommendation	Implement a comprehensive legal framework that provides a basis for the development of measures forming part of an emergency response. A provision should be made in the country's constitution or legal system to invoke a state of emergency that, for a limited time, establishes modified roles for the different organs of the state during the emergency to maintain sufficient oversight and safeguards to protect individual rights.
	How to implement the recommendation?	
	□ Introduce draft legislation making provision for the following: • The executive/government may declare a state of emergency under certain conditions, stipulating that the declaration must be sanctioned by the state legislature. • The legislature and the judiciary maintain oversight during the emergency. • The government may only pass measures in response to the declared emergency when the nature and scope of these measures are clearly specified.	

	• The measures implemented in response to the emergency are consistent with existing laws, including but not limited to the data protection law. • The government ensures any derogation from the individual rights that exist within its legal system or constitution passes the proportionality test. • The measures passed in response to the declared emergency are subject to post facto review and approval by the legislature. • The state of emergency and the measures implemented in response to the emergency must adhere to a strict time limit and any extension is subject to ex ante approval by the legislature.

Function Creep and Unintended Consequences		
Trend 2		
Reduced and unequal access to society	Evaluation	Sometimes in a public health emergency, governments enact measures that may result in certain groups being discriminated against. In the context of the Covid-19 pandemic, certain measures were made mandatory despite there not being sufficient resources or support for people to comply with them. For example, some countries required people to be vaccinated against Covid-19 before being given access to public venues or to travel, despite access to vaccines being limited and/or large sections of the population still not being vaccinated.
	Recommendation	Governments should ensure that mandatory public health measures during a public health emergency are backed up with the necessary resources and facilities available so that people can comply with such measures and not be unfairly denied access to society.
	How to implement the recommendation?	

	□ Ensure that the requirements for access to society are widely available to the population, including vaccinations, testing and paper-based alternatives for apps. □ Vaccination centers and testing locations must be accessible in both urban and rural areas, and paper-based/non-digital alternatives to apps should be easily available.

2. Recommendations for App Developers, Operators and Commissioning Public Entities

What could the public expect from these stakeholders involved in the pandemic response and why?

It is important for the public to know that app developers and operators as well as public entities commissioning the Covid-19 apps can take a number of steps to ensure the effective and sustainable use of the apps. These steps, consisting of development and design choices, safeguards and procedural actions together facilitate trust and the success of the use of Covid-19 apps, as part of a broader public health strategy.

In practice, Covid apps' technical features and design have an impact on the collection and use of people's personal data, and on the enjoyment of fundamental rights, including the right to privacy.

For instance, making the code of the app publicly available fosters civil society and public trust. Employing privacy by design principles can prevent function creep and other unintended consequences, preventing loss of trust or harms resulting from the introduction of the app. This also includes limiting the use of unnecessary data, such as location data, for which alternatives usually exist. The handling of (personal) data must be clearly defined, with special attention paid to purpose, the sensitivity of the data, storage, security, and sharing limitation. Any type of data-sharing, particularly with the private sector, must serve a clear role in public health strategy, with the possible exception of research data, particularly for instructing future public health policy.

Within these rights-respecting frameworks, the apps must also be futureproof by anticipating potential fraud. The functioning of the app can only be guaranteed if any fraud that does occur can be effectively and transparently addressed.

Public Health Efficacy		
Trend 1		
Not all apps make their code publicly available	Evaluation	There are deficiencies in terms of transparency in all the analyzed apps, though there are significant differences between them. Only three make their source code available for inspection. The majority use code obfuscation, reflection and other anti-analysis techniques that make it difficult to reliably determine or confirm the presence of some behaviors. Such measures negatively impact trust and are misaligned with international transparency and privacy engineering recommendations.
	Recommendation	Make all existing Covid-related apps open source on all platforms. By making the server-side codes publicly accessible and auditable, people can collaborate, check the codes for vulnerabilities, and start a peer-review system.
	How to implement the recommendation?	
	□ Publish source code to GitHub or another similar open-source website/platform □ Do not use any obfuscation techniques to conceal or distort the source code, which make it difficult to inspect the code independently.	

<table>
<tr><th colspan="3">Function Creep and Unintended Consequences</th></tr>
<tr><th colspan="3">Trend 1</th></tr>
<tr><td rowspan="4">Deployment of technological solutions in collaboration with the private sector</td><td>Evaluation</td><td>Some of these partnerships come in the form of data-sharing arrangements. Other partnerships revolved around private companies helping governments to conduct surveillance operations. A major drawback of these partnerships is the omission of appropriate regulatory checks. Moreover, all of the countries under review lack a comprehensive data protection framework, which further undermines the legitimacy of these public-private partnerships, creating opportunities for function creep and unbalanced use of power.</td></tr>
<tr><td>Recommendation</td><td>Clearly frame data-sharing practices between different government entities and the private sector.</td></tr>
<tr><td colspan="2">How to implement the recommendations?</td></tr>
<tr><td colspan="2">□ Consult the relevant software requirements specification to determine whether data sharing is necessary for the functioning or features of the app or system.
□ Create data flow maps and records of processing operations to document the data being shared with government entities and the purposes for which those data are being shared. See the template provided below in the "Tools for Implementation" section for an example of what such documentation could contain.
□ Consult legal experts to draft clauses regarding the data to be shared with government entities, the purposes of such sharing and other relevant obligations that should apply to it. These should be included in any contract between the developer and the government for the provision of services.</td></tr>
</table>

Relevant Tools for Implementation
• Software Requirements Specification Template • Data Flow Map for Immunity Passport App Template

Function Creep and Unintended Consequences		
Trend 2		
Most countries choose to adopt centralized systems for their contact tracing apps	Evaluation	Centralized systems arguably comply less with the concept of privacy by design than decentralized systems. In a centralized system, most of the required processing takes place on a central server operated by a public authority, making sensitive personal data more accessible to those authorities. In contrast, with a decentralized system, most of the processing takes place on the user's device with most sensitive personal data also remaining locally and only pseudonymized data being shared with other devices and the central server. This is the case with the countries that use GAEN API.
	Recommendation	Approach application development using a privacy by design framework.
	How to implement the recommendations?	
	☐ Develop a software requirements specification for the software development process that sets out the proposed functions of the Covid app in line with the relevant privacy principles or legal requirements. See the template provided below in the "Tools for Implementation" section. ☐ Seek the advice of an independent third-party expert to assess the data protection or privacy risks of Covid apps during their development to ensure that data protection and privacy principles are	

	properly interpreted and implemented at each stage of the development cycle prior to deployment.
Relevant Tools for Implementation	
• Software Requirements Specification Template	

Function Creep and Unintended Consequences		
Trend 3		
Common use of location data	**Evaluation**	Collecting location data allows the national authorities to track users and carry out more intrusive surveillance that extends beyond public health needs. This is of particular concern when location data can reveal "users' habits, home address, workplace data, and even religious beliefs (i.e., place of worship)."
	Recommendations	Minimize the amount of data collected to what is strictly necessary, particularly personal or identifiable data; this includes eliminating the need for GPS location. Remove requests for location data from any contact tracing applications to protect privacy. Offer a clear and easy-to-access option to delete an account and information from the app, as well as from the server.
	How to implement the recommendations?	
	□ Carry out regular code reviews during the process of turning high-level design into lines of code.	

	□ Involve data protection and privacy experts or specialists to ensure that the app functioning complies with the software requirements specification containing the applicable legal requirements or principles.

Function Creep and Unintended Consequences		
Trend 4		
Common use of tools for tracking and analytics	Evaluation	The principle of privacy by design is not completely followed with respect to the SDKs deployed in the countries of focus. In particular, the use of the Google Firebase Library, or indeed other SDKs, is not clearly outlined in the respective privacy policies. As such, it cannot be fully determined how Google Firebase is being used, in particular whether it is limited to installation analytics or used for broader tracking purposes that are more privacy-intrusive.
	Recommendations	Provide clear information regarding the type of data collected and for what purpose, where and for how long data will be stored, with whom the data will be shared and for what purposes, as well as the security protocols for all of these functions. Publish more detailed privacy policies (written in all local languages) and explicitly name any third parties who have access to data.
	How to implement the recommendations?	
	□ Carry out vendor assessments of the third parties providing the SDKs and other software libraries to be used in the Covid app. These assessments should include a review of the privacy policies and	

	other related data protection documentation as well as an inspection of the third-party code being imported into the workspace for the development of the app.

<table>
<tr><th colspan="3">Public Health Efficacy</th></tr>
<tr><td colspan="3">Trend 1</td></tr>
<tr><td rowspan="4">Fraud to obtain Covid certificates</td><td>Evaluation</td><td>Partially due to the misinformation and conspiracies surrounding Covid-19, there are cases where people attempted to obtain fraudulent QR codes to be able to access venues or to travel. In some countries, the number of fraud cases ran into the tens of thousands.</td></tr>
<tr><td>Recommendations</td><td>Anticipate fraud attempts and ensure adequate vetting of all parties involved, including private sector partners.
Within the principles of privacy by design, allow for the removal of fraudulently obtained certificates, ensuring this process is integrated into the privacy statement in a transparent manner.</td></tr>
<tr><td colspan="2">How to implement the recommendations?</td></tr>
<tr><td colspan="2">☐ Carry out verification testing to ensure that the system performs according to the requirements. This should cover unit testing (addressing individual functions and system components), integration testing (addressing the interactions between groups of components), system testing (addressing the completed portions of the whole system), and acceptance testing (providing the system to selected users, i.e., alpha and beta testing).</td></tr>
</table>

Function Creep and Unintended Consequences		
Trend 1		
Lack of privacy by design in Covid apps	Evaluation	Covid apps have varying levels of success in terms of achieving privacy by design. If this concept is not adhered to, users may be disproportionally harmed. Such harms can often translate into app developers, as well as the governments soliciting their services, failing to uphold the privacy and data protection rights of individuals properly. Some apps use SDKs that process data for other purposes disconnected from the main purpose of the app (public health) or share the data with third parties. In addition, most app developers are not transparent about the third-party SDKs or software libraries used on their apps or do not publicize or otherwise obfuscate their source code. In addition, most Covid apps are deployed without a data protection or privacy impact assessment being carried out beforehand to identify and mitigate potential data protection or privacy risks. However, some countries did make an effort to provide data protection guidance to public venues required to collect certain personal data for contact tracing purposes.
	Recommendations	Only use SDKs that process personal data necessary for the purpose of the app (i.e., contact tracing and/or displaying health information). Produce privacy notices that inform app users in clear and concise language about how their data are collected and processed, and deliver such notices in a user-friendly manner. Make the source code for the apps open source to allow for independent verification of the app's functions and data processing operations.

When public venue organizers process personal data (for example with both digital and manual contact tracing), provide guidance on how to process such data in a responsible manner conducive to good data protection.

Carry out data protection or privacy impact assessments before deployment to identify potential data protection or privacy risks, and develop appropriate mitigation measures for the risks identified.

How to implement the recommendations?

☐ Seek the advice of an independent third-party expert to assess the data protection or privacy risks of Covid apps during their development to ensure that data protection and privacy principles are properly implemented at each stage of the development cycle prior to deployment.

☐ Develop a software requirements specification for the software development process that sets out the proposed functions of the Covid app and is in line with the relevant privacy principles or legal requirements. See the template provided below in the "Tools for Implementation" section for an example of what such documentation could contain.

☐ Carry out vendor assessments of the third parties providing the SDKs and other software libraries to be used in the Covid app. These assessments should include a review of the privacy policies and other related data protection documentation as well as an inspection of the third-party code being imported into the workspace for the development of the app.

☐ Draft full privacy notices accompanied by a short form notice to be provided when users first use the app and accessible thereafter. See the template provided below in the "Tools for Implementation" section.

☐ Publish source code to GitHub or another similar open-source website/platform.

	□ Do not use any obfuscation techniques to conceal or distort the source code, which make it difficult to inspect the code independently. □ Draft data protection guidance for venue operators including (i) what data they should be collecting and why, (ii) how that data should be collected and stored, (iii) the requirement to keep that data confidential, and (iv) data should only be shared with certain third parties related to the purposes of its collection. □ Use the template provided below in the "Tools for Implementation" section as a starting point for data protection or the privacy impact assessment to be completed during the app development.
Relevant Tools for Implementation	
• Template Software Requirements Documents • Template Privacy Notice for Contact Tracing App • Template Data Protection/Privacy Impact Assessment	

Function Creep and Unintended Consequences		
Trend 2		
Rise of public-private partnerships and lack of transparency	Evaluation	Governments tend to leverage their relationships with private sector entities to achieve various policy ends. Covid-19 is no exception; many governments choose to use the Google/Apple Exposure Notification system to build their digital contact tracing apps; some countries look to telecommunications companies to acquire data to create heat maps and track the spread of the virus; governments also install camera systems to monitor compliance with quarantine rules, thus expanding the state surveillance apparatus. However, often these partnerships are cloaked in secrecy or, in the context of Covid-19, exploit the emergency context to escape the usual regulatory constraints that serve to ensure that rights are protected.
	Recommendation	Release into the public domain the terms of the partnership for all apps that have been developed in public-private partnership.
	How to implement the recommendations?	
	□ Governments should ensure transparency of public-private partnerships (e.g. by granting freedom-of-information requests).	

Tools for Implementation

Below are templates as well as examples of good practice to facilitate implementing some of the recommendations presented in the Covid-19 Apps Toolkit.

Privacy By Design for Contact Tracing Apps

This example presents a model of a privacy-enhancing contact tracing app, which generates its own QR code to be used by individuals (giving their consent) to check in and out of venues that have registered with this app ("Registered Venues").

These apps should be designed only to facilitate entry-exit recording by Registered Venues while protecting privacy and personal data, meaning that:

a. The app processes the minimum amount of personal data possible;
b. Personal data are encrypted to the fullest extent possible and may only be decrypted by the Public Health Authority if a positive Covid case is detected;
c. The Public Health Authority only receives the data necessary to trace specific individuals present at a specific venue within a specific timeframe where a risk of Covid-19 transmission has been identified;
d. All entry-exit data are deleted as soon as they are no longer relevant for contact tracing purposes — after 14 days.

Data access and transfers

- The app developer/operator must not access any personal data collected from the individual, processed by Registered Venues or transferred to the Public Health Authority.
- Those venues that use the app to record the entry and exit of individuals have strictly limited access to personal data, which is only visible at the point of entry to facilitate identity checks where needed. Only authorized personnel at the venue have access to this data.
- The Public Health Authority is authorized to receive data about individuals who have visited a registered venue at the same time as someone with a Covid-19 diagnosis (for the purposes of contacting them).

Specified purpose

Personal data may be processed for the purposes of:

a. Providing individuals with a QR code.
b. Providing the venue with a secure means of collecting data about those present.
c. Providing the Public Health Authority with the data it needs to identify and contact individuals who may have been in the proximity of someone diagnosed with Covid-19.

Data processed

1. On individuals using the app:
    a. Name and surname and year of birth, used for identification and contact tracing purposes.
    b. Mobile phone number, used to receive the app QR code and be contacted by the Public Health Authority, if necessary.
    c. QR code-based entry and exit stamps at the venue, stored on an individual's device and the app servers, decrypted and used for tracing purposes in the event of disclosure by a venue following a request from the Public Health Authority.

2. By Registered Venues

    a. Email, username, password of account holder, used for account creation and management.
    b. Name, email and phone number of three venue contact points, used by the Public Health Authority to communicate disclosure requests for contact tracing purposes.

3. By the Public Health Authority
    a. Name and surname, year of birth and mobile phone number of people present at a specific venue in a specified timeframe, for the purposes of identifying and contacting those persons to prevent the spread of Covid-19.

Data retention and deletion

1. Registered individuals and QR codes:
    a. The personal data provided for the purposes of registration and receipt of the QR code are deleted as soon as the individual has received the link to the QR code.
    b. The QR code containing the encrypted personal data about the individual is retained in two places:
        i. On the individual's device, to enable scanning by venues.
        ii. On the app developer/operator's server, to enable individuals to download the image via the SMS link.
    c. Users can delete their QR code/the link between themselves and their QR code at any time, though any entry-exit recordings of that QR code will still be retained for 14 days for contact tracing purposes.
    d. All QR codes and the means to decrypt them will be deleted when the Public Health Authority rescinds the legal requirement for venues to collect entry-exit data.

2. Data on venues and their visitors:
    a. The personal data related to a venue will be retained until:
        i. The venue deactivates their account (in which case the data about the venue and the associated entry-exit data will be retained for 14 days for the purposes of contact tracing prior to deletion), or
        ii. The Public Health Authority rescinds the legal requirement for venues to collect entry-exit data and all accounts are deleted.
    b. Registered Venue entry-exit data are automatically deleted after 14 days.
    c. Data disclosed to the Public Health Authority for contact tracing are processed in accordance with applicable national regulations, policies and procedures.

3. SMS data are deleted by the app and the processors it uses to send the messages delete the data from their servers as soon as they have been delivered.

Disclosure of data to the Public Health Authority

1. Individuals' data are encrypted in their QR code. The data are linked to the venues visited when they scanned their QR code. The Public Health Authority may only access and decrypt the data if it is necessary for contact tracing.

2. In the event that someone with a Covid-19 diagnosis is traced to a venue, the Public Health Authority may request the disclosure of information from that venue concerning persons present at the same time. The venue may authorize the transfer of data concerning the relevant individuals, or request further information from the Public Health Authority if this is needed to validate the request.

3. Disclosure authorization allows the Public Health Authority to access data on relevant individuals only – those present at the venue during the specified timeframe.

Information security

1. Information security is achieved through data segregation, robust access controls and encryption. The information security features, architecture and code base have been audited and verified by independent computer scientists.

Cookies

1. The app website deploys the following strictly necessary cookies for the purposes of facilitating account creation and ensuring data security:
    a. "csrftoken" is used to protect the service against cross-site request forgery.
    b. "sessionid" is used for the correct attribution of the sessions by the server to authenticated users with access to the dashboard.

Software Requirements Specification Template

A software requirements specification is a document that details all of the requirements that the app or system being developed should meet. This document can include both technical and legal requirements. Below is an example of a section of a software requirements specification that sets out a legal requirement that a contact tracing app should implement.

<table>
<tr><td>Requirement ID</td><td>REQ-31</td></tr>
<tr><td>Requirement Statement</td><td>The application shall use the Google/Apple Exposure Notification Framework for the contact tracing model</td></tr>
<tr><td>Author</td><td>[Name]</td></tr>
<tr><td>Revision</td><td>1.1</td></tr>
<tr><td>Release Date</td><td>[Date]</td></tr>
<tr><td>Keywords</td><td>Decentralized contact tracing, data minimization</td></tr>
<tr><td>Legal Requirement</td><td><i>FIPPs Collection Limitation Principle</i> – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means, where appropriate, with the knowledge or consent of the data subject.</td></tr>
<tr><td colspan="2"><u>Scenario Description</u>
Apps using GAEN generate random IDs (cryptographic tokens called rolling proximity identifiers) that change every 10-20 minutes to reflect the location of the device. When the user comes into close contact with another device with an app using the GAEN system, the two devices exchange and record their respective random IDs via Bluetooth. Users also enter their positive Covid-19 test results into the app, and a list of the random IDs that their device has recorded in the past 14 days is communicated to a central server operated by a public authority. The mobile device will then periodically compare the random IDs it has recorded against a database of random IDs associated with a positive Covid-19 test result. If a match is found, then the app will notify the user that they may have been exposed to someone with Covid-19 and advised to follow the guidance of the relevant public authority such as taking a Covid-19 test and/or self-isolating for a certain period.

<u>Design Assumptions</u>
Cryptographic tokens on the device are changed regularly and in accordance with device location.
The central server operated by the public authority only maintains pseudonymous personal data of users (cryptographic random IDs).</td></tr>
</table>

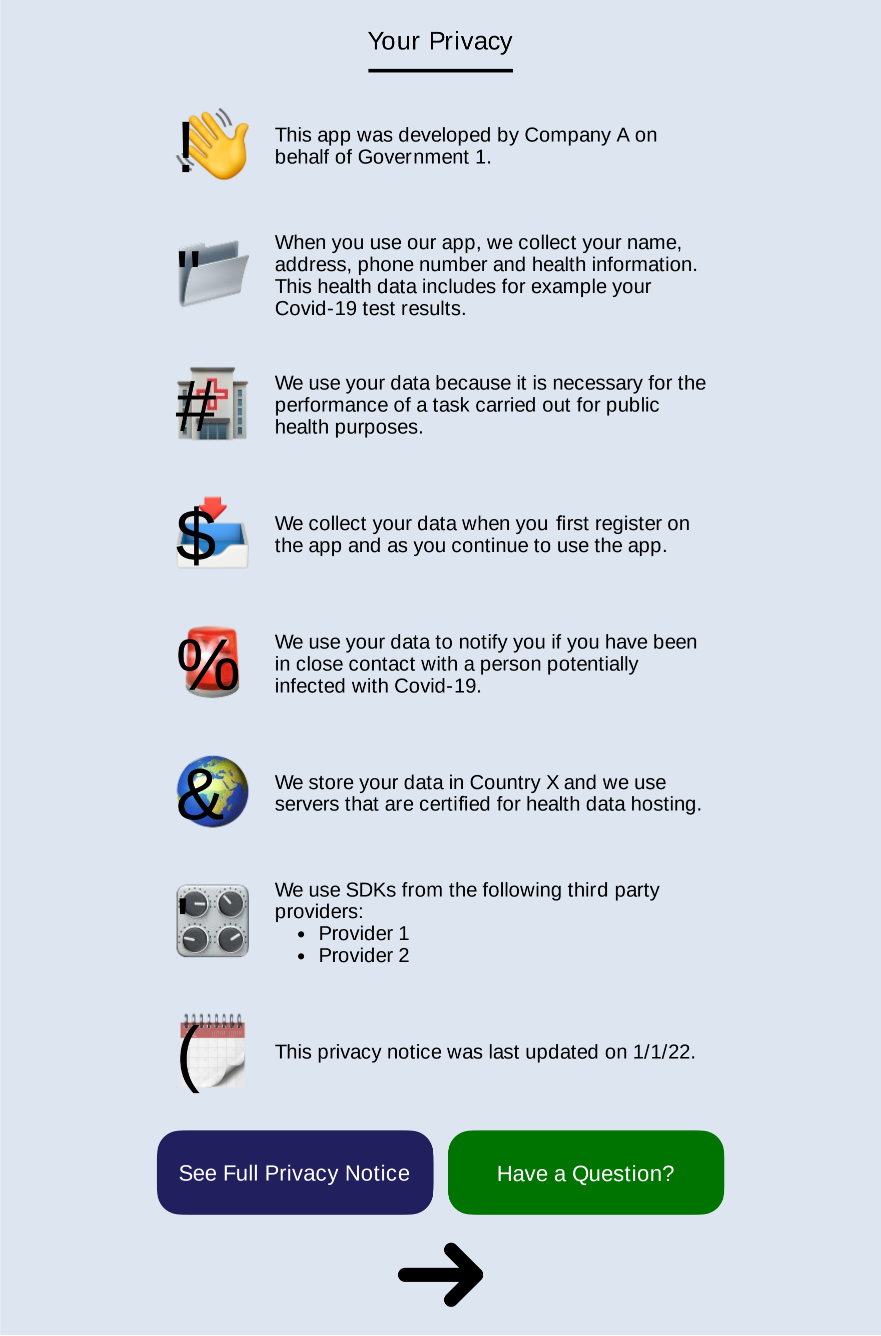
Data Flow Map for Immunity Passport App Template

A data flow map can be used to connect legal requirements to specific stages of the data lifecycle to ensure that the requirements are fully complied with when data are collected and processed. Below is an example of a data map that outlines the specific legal requirements that apply at each stage of the data lifecycle and the appropriate functionality that the app should have as a result. The Requirement ID should correspond with the ID specified in the relevant Software Requirements Specification for the app, an example of which can be seen above.

Data Lifecycle for User Health Information		
Data Lifecycle Stage	**Requirement ID**	**Requirement Statement**
Collection	REQ-51	The application will process the user's Covid-19 vaccination status, Covid-19 test results and information on Covid-19 natural immunity. This health information will be collected on registration and subsequently when the user enters the information into the application.
Use	REQ-78	The application will convert the user's health information into a QR code that the user can display to venue organizers to gain entry into the venue.
Disclosure	REQ-09	The user's QR code will be generated for venue operators to scan.
Retention	REQ-12	The user's health information is retained for as long as the user keeps the application downloaded on their device. The application will not retain data regarding the location at which the user's QR code was scanned.
Destruction	REQ-34	The user's health information will be destroyed when the application is deleted.

Privacy Notice for Contact Tracing App Template

Below is an exemplar of a short form privacy notice that can be used for contact tracing apps and presented to users when they first register on the app. The aim is to deliver the most important information about the processing carried out by the app, with the option to view the full notice or submit a question to the developer.



Your Privacy

This app was developed by Company A on behalf of Government 1.

When you use our app, we collect your name, address, phone number and health information. This health data includes for example your Covid-19 test results.

We use your data because it is necessary for the performance of a task carried out for public health purposes.

We collect your data when you first register on the app and as you continue to use the app.

We use your data to notify you if you have been in close contact with a person potentially infected with Covid-19.

We store your data in Country X and we use servers that are certified for health data hosting.

We use SDKs from the following third party providers:

- Provider 1
- Provider 2

This privacy notice was last updated on 1/1/22.

Data Protection/Privacy Impact Assessment Template

Below is a template of a data protection/privacy impact assessment that should be completed before an app is deployed.

System/App	[...]
System/App Version	[...]
Date of DPIA	[...]

Development Project Background	
What is the system/app being developed?	[...]
Why is the system/app being developed?	[...]
Who is involved in the development of the system/app?	[...]
What kind of testing has been done on the system/app?	[...]
What is the planned date for full deployment?	[...]

Description of Processing Operation	
What personal data are being used by the system/app?	[...]
What purposes are the personal data being used for?	[...]
Who are the personal data disclosed to?	[...]
What SDKs or other third-party software libraries are being used to develop the system/app?	[...]

Risk Identification			
Threat	**Vulnerability**	**Event**	**Risk**
[...]	[...]	[...]	[Low, Medium or High]

Risk Management			
Risk	**Response**	**Response Type**	**Rationale**
[...]	[Accept, Transfer, Mitigate or Avoid]	[Technical, Organizational or Contractual]	[...]