Organisation for Economic Co-operation and Development

DSTI/CDEP/DGP(2021)12/FINAL

Unclassified English - Or. English

22 December 2021

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Data Governance and Privacy in the Digital Economy

OECD-Global Privacy Assembly Online Workshop: "One Year Later: Addressing the Data Governance and Privacy Implications of the COVID-19 Pandemic and the Road to Recovery"

Draft Summary of Main Points

JT03487789

Table of Contents

1. Background and key messages

1. During the COVID-19 pandemic governments took drastic measures to curb the spread of the virus. The use of data, and in many cases personal data, has been vital to some of these measures, but raised significant privacy and data governance challenges. Over this period, the OECD has sought to support governments, and other stakeholders by providing jointly with the Global Privacy Assembly a forum to collectively consider and address the privacy and data governance aspects of the measures put in place to limit the spread of the virus and contain the COVID-19 pandemic. In particular the OECD took the following actions:

- Hosted a workshop, with the support of the Global Privacy Assembly (GPA) on 15 April 2020, which considered "Addressing the Data Governance and Privacy Challenges in the Fight against COVID-19".[1]
- In the same month, released two policy briefs:
  - The first brief examined data privacy issues arising from the fight against COVID-19 (OECD, 2020[1]).
  - The second policy brief analysed the use of digital technologies by governments in tracking and tracing COVID-19, in particular mobile and biometric applications (OECD, 2020[2]).
- Following-up on the first workshop, on 16 September 2020, an additional workshop was held jointly with the GPA to discuss "The road to recovery: Lessons learned and challenges ahead; addressing the data protection and privacy challenges raised by COVID-19".[2]

2. In order to reflect on a number of the lessons learned over a year after the outbreak of the pandemic, and to continue these important multi-stakeholder discussions, the OECD organised another virtual workshop with the support of the GPA titled "One Year Later: Addressing the Data Governance and Privacy Implications of the COVID-19 Pandemic and the Road to Recovery" (see the agenda in Annex B). The event was held on 21-22 June 2021. It was organised back-to-back with an online workshop of the United Nations Special Rapporteur on the Right to Privacy, which took place on 23 June 2021. The OECD-GPA workshop was also organised as a contribution to Phase III of the OECD Going Digital Project, which aims to provide policymakers with the tools they need to design and implement better data policies to promote growth and well-being.

3. The OECD-GPA workshop was comprised of three sessions focusing on the following main topics: *i)* the different legal and policy frameworks which enabled the exceptional surveillance and contact tracing efforts during the COVID-19 pandemic, as well as lessons learned; *ii)* data privacy aspects in the workplace during the pandemic; and *iii)* vaccination programmes and COVID-19 "travel passports". This report aims to summarise the background materials that set the stage for the event, as well as the topics

[1] The first workshop focused on early lessons learned on: (i) how best to address data protection and privacy challenges in front-line responses to COVID-19; (ii) how to facilitate data access and sharing between organisations including within the public sector and across jurisdictions to ensure that all relevant stakeholders have the information needed, while minimising potential risks to stakeholders; and (iii) how to better inform and engage all stakeholders to build and reinforce data sharing partnerships and trust across society.

[2] The second OECD workshop provided a platform for governments, data protection authorities, academics and other stakeholders to discuss how the lessons learnt from the early stages of the COVID-19 can help countries prepare for future data protection and privacy challenges that arise in the road to recovery.

presented and discussed during the workshop. It is structured along the key themes that were covered during the three sessions.

4. The following main messages emerged from the event:

Actions by governments and PEAs:

- Secure, reliable and timely data access and sharing has been key in learning about COVID-19 and its spread, in gathering evidence to evaluate the effectiveness of policies, and supporting response including the development and distribution of vaccines.
- Few OECD countries had the information infrastructures and data governance frameworks in place to support the significant contact-tracing and population-wide data collection measures envisaged. Accordingly, many countries introduced amendments to existing laws or developed new laws and policy frameworks in support of their response to the COVID-19 pandemic.
- PEAs provided essential guidance to support the safe and swift data access and sharing during the pandemic, whilst strongly advocating for the upholding of fundamental privacy and data protection principles.

Public perceptions towards privacy:

- Public perception evolved during the COVID-19 pandemic. Individual concerns about risks to privacy and fundamental freedoms increased alongside a growing awareness of the role that personal data played in facilitating health and safety measures.

Data privacy in the workplace:

- To establish safe and secure working environments and support business continuity during the pandemic, employers utilised a wide variety of technologies to monitor and track the health of workers, contractors and visitors. The use of these technologies has generated important privacy concerns, particularly in the context of more people working remotely and the blurring of the boundaries between business and personal activities.
- A number of PEAs issued guidance on the lawful processing of data to protect the health and safety of individuals in the workplace and at the same time safeguard the fundamental rights and interests of the data subjects.
- The sudden transition to increased remote working and ubiquitous monitoring, has raised however, special challenges to which policy response has been uneven. The intensification of monitoring can be privacy-intrusive and may also result in mental health problems for employees among other concerns. It is important to ensure full understanding of the mental health implications of surveillance and electronic performance monitoring.

COVID-19 "travel passports":

- Many OECD countries have introduced COVID-19 "travel passports" to assess an individual's COVID-19 health status. Whilst such "travel passports" may help to lift travel restrictions, and support the wider

economy, they also risk exacerbating existing inequalities, discrimination, and may raise ethical and privacy concerns.

- A number of guidance documents were released to address these concerns and facilitate safe international travel during COVID-19, including by the GPA and the OECD (Global Privacy Assembly, 2021[3]) (OECD, 2021[4]).

2. Reflecting on the varying policy and legal frameworks in response to the COVID-19 pandemic

The first session reviewed how governments in a selected number of countries have approached the COVID-19 crisis and the legal and policy frameworks that were developed in support of the exceptional measures taken to track, trace and contain the spread of the COVID-19 pandemic.

Data access and sharing has been key to understanding COVID-19 and its spread

5. Timely, secure and reliable data access and sharing has been essential in understanding COVID-19 and its spread, helping to improve the effectiveness of government policies, and enhancing global co-operation in the development and distribution of vaccines (OECD, 2020[1]). In particular, lessons from previous outbreaks have highlighted the importance of data concerning the spread of the virus (OECD-Harvard Global Health Institute, 2017[5]) (OECD, 2020[6]) (OECD, 2020[2]). This may include the number of new confirmed cases, location data, source of new cases and the rates of recoveries and deaths (OECD, 2020[6]).

6. Understanding how a virus mutates as it moves through the population is also essential. Such information may help policymakers to learn changes in the transmissibility or severity of the disease, its amenity to diagnosis and its responsiveness to vaccine (OECD, 2020[6]). Data on population movements may help governments to monitor the progression of the virus of the outbreak and its spread, decide on the priorities for interventions and develop effective containment measures (OECD, 2020[6]).

7. Accordingly, during the pandemic, governments have turned to a wide array of digital technologies and advanced analytics to collect, analyse and share data to inform front-line responses to the COVID-19 crisis. Above all, most countries leveraged the wide-spread use of mobile phones for contact tracing. Mobile applications (apps) for COVID-19 response have proliferated, with varying degrees of success.

8. Nonetheless, in developing digital contact tracing apps, countries faced a range of issues, from accuracy problems to interoperability, as well as privacy challenges. Implementation was also a challenge for many countries, dependent on their pandemic response structure (such as centralised vs decentralised or local data governance).

Countries had to develop policy and legal frameworks to facilitate the extraordinary data access and sharing during the pandemic

9. Privacy frameworks generally facilitate data access and sharing in the interests of public and national security, such as public health and welfare (OECD, 2020[6]). However, OECD work suggests uneven policy guidance in regard with few OECD countries reporting data governance structures in place that can facilitate extraordinary data collection and sharing through measures that are secure, fast, scalable and trustworthy, and in compliance with the relevant data protection and privacy regulations (OECD, 2020[6]) (OECD, 2019[7]).

10. Accordingly, many countries needed to introduce new legislation to support the extraordinary COVID-19 measures (OECD, 2020[1]). These initial developments aimed to establish good practice for the collection of personal data related to COVID-19 (for instance for contact tracing apps), including for what purpose and for what time duration. Starting from 2021, a number of countries also developed policies and legislation on the

use of COVID-19 "health passes" and "travel passports" (as further discussed under "Vaccination programmes and travel passports"). In this regard, Annex A includes relevant country-specific examples of policy and legal frameworks that were developed in response to the COVID-19 pandemic.

Privacy Enforcement Authorities played an essential role in upholding fundamental privacy and data protection principles during the pandemic

11. In all cases PEAs have played a key role as governments enacted emergency legislation and data controllers sought legal certainty (OECD, 2020[1]). In particular, a number of PEAs published guidance to enable swift and safe data sharing during the pandemic, while upholding fundamental privacy and data protection principles (Global Privacy Assembly, 2021[8]). Prior and ongoing involvement of PEAs in the development and assessment of contact tracing apps was essential in ensuring compliance with privacy and data protection measures (European Union Agency for Fundamental Rights, 2020[9]).

12. For instance, in Belgium, France, Germany, and the Netherlands, PEAs were consulted in advance of the development of a contact tracing app, which in some cases led to significant changes to the design of the app (Council of Europe, 2020[10]). Ms Florence Raynal (Deputy Director, Head of Department of International and European Affairs, CNIL) highlighted that in France the CNIL conducted thirteen investigations to check whether the country's COVID-19 app was compliant with the GDPR and issued a formal opinion on its use. In Mexico, upon the release of the "COVID-19 MX" contact tracing app, the government asked the National Institute for Transparency, Access to Information and Personal Data Protection to assess the privacy features of the app. In Korea, the Personal Information Protection Commission conducts a monthly inspection of local government webpages to ensure that they are privacy compliant when they release data about COVID-19 patients (as further discussed in Annex A). In Italy, the government and the Garante collaborated closely during the COVID-19 pandemic to uphold privacy and data protection principles. In the United States, the Federal Trade Commission took a number of actions to protect the public from harms that resulted directly or indirectly from the COVID-19 pandemic (as discussed in Box 1 below).

Box 1. The Federal Trade Commission's actions to protect the public from harms resulting from the COVID-19 pandemic

In the United States, the Federal Trade Commission (FTC) undertook a range of actions to protect consumers during the COVID-19 pandemic. As highlighted by Mr Daniel Kaufman (Acting Director, Bureau of Consumer Protection at the FTC) concerns ranged from misleading COVID-19 treatment claims to privacy and data security issues.

The agency developed a public dashboard to track and alert the public about COVID-19 related reportings from consumers, identify and respond to emerging risks, and identify law enforcement targets (Federal Trade Commission, 2021[11]). Mr Daniel Kaufman highlighted that identity theft emerged as a major area of concern. The FTC received over sixty thousand reports in this regard during the COVID-19 pandemic, with a large number of these incidences reported in the context of unemployment insurance benefits. Another major area of concern is related to deceptive claims made by marketers about COVID-related products and

services. For instance, the FTC (in co-operation with other federal agencies) had to issue hundreds of warning letters to sellers or marketers of products that claimed to prevent or treat COVID-19. The overwhelming majority of those who received such warning letters from the FTC removed the claims.

The FTC also focused on privacy enforcement actions which were related to the increased use of digital technologies, including videoconferencing and health apps. For instance, the FTC conducted an investigation against the claims made by a major videoconferencing platform about how users' information was being handled. The settlement resolving this issue asks the platform to stop making a wide-variety of misleading or false allegations and orders it to implement an information privacy and security program (Federal Trade Commission, 2021[11]) (Federal Trade Commission, 2020[12]). In another case, which was related to a period and fertility-tracking health app, the FTC investigated allegations that the developer shared the health information of its users with external data analytics providers. The main outcome of the settlement in this case was that the developer of the app had to notify its users about the disclosure of their data and instruct any third party that received users' health data to destroy it.

Mr Daniel Kaufman underlined in his presentation that during the pandemic the FTC sent out more than one hundred alerts to inform consumers about COVID-19 scams, reminded businesses about their responsibilities in regards to advertising practices, and alerted companies about scams targeting them. In addition, the FTC also urged companies to consider privacy protective measures and technologies as they develop their products.

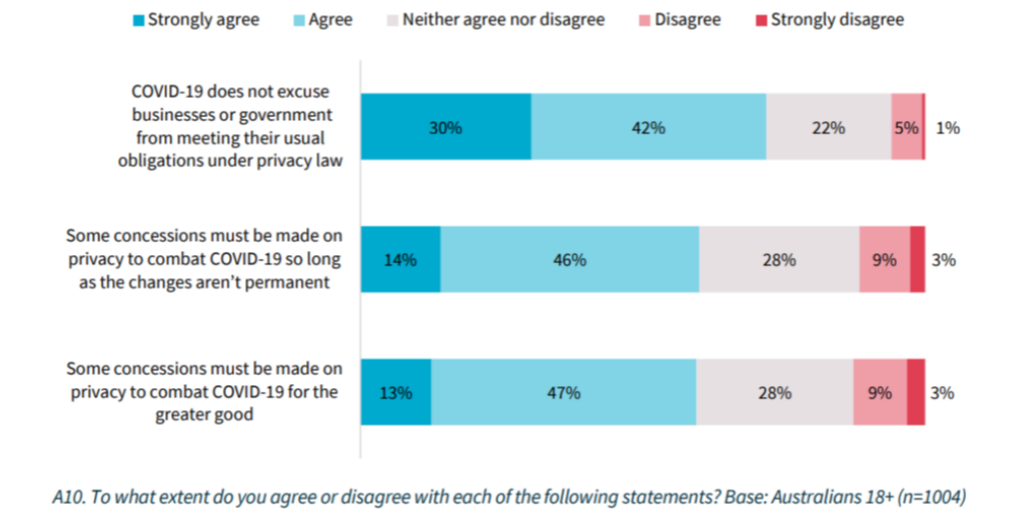
(*Source:* Mr Daniel Kaufman, OECD-GPA Workshop)

Public perception towards privacy has changed during the pandemic

13. The public perception towards privacy evolved during the COVID-19 pandemic. As reported by Mr Guido Scorza (Office of the Garante, Italy), individual concerns about risks to privacy and fundamental freedoms sharply increased during the pandemic alongside a growing awareness of the role that personal data played in facilitating health and safety measures.

14. The Office of the Australian Information Commissioner conducted a survey in 2020 to provide insights on Australians' attitudes towards privacy. Results indicate that half of the survey respondents felt that their privacy was more at risk during the COVID-19 pandemic (Office of the Australian Information Commissioner, 2020[13]). As noted by Ms Elizabeth Hampton (Deputy Commissioner, Office of the Australian Information Commissioner), the survey revealed that location tracking, government surveillance and workplace privacy ranked higher as concerns in the context of the COVID-19 pandemic. The survey also highlighted that Australians are aware of the need to balance privacy and data protection with other priorities, including public health and the need for safer workplaces. Furthermore, a majority of respondents believed that some concessions must be made on privacy to address the COVID-19 pandemic, as long as the changes are not permanent (as illustrated below in Figure 1):

Figure 1. Australian survey results about the privacy concessions that must be made during the COVID-19 pandemic



Source: (Office of the Australian Information Commissioner, 2020[13])

A case study from the private sector

15. Representing the private sector in Session 1, Mr Gary Davis (Global Director of Privacy and Law Enforcement Requests, Apple) presented Apple's COVID-19 response (see below in Box 2).

Box 2. Case study from the private sector: Apple's COVID-19 response

i) The Apple-Google exposure notifications system

On 10 April 2020, Apple and Google announced that they had jointly developed an exposure notifications system that uses Bluetooth technology to support contact tracing efforts on smartphones. Before the launch of the initiative, Google and Apple held a number of consultations with Public Health Authorities, Privacy Enforcement Authorities, privacy advocates, the media and the general public in order to be fully transparent and to gain the trust of users. The exposure notifications system is a decentralised initiative which does not share the identity of the user with other users or with Google and Apple. In addition, the system does not track the location of its users and users can switch off the exposure notifications system anytime they wish to do so. Users may decide whether they wish to report a positive COVID-19 diagnosis or not.

On 27 April 2020, the UK Information Commissioner's Office (ICO) released an opinion on the joint Apple and Google initiative. The opinion stated that the initiative appeared to be "aligned with the principles of data protection by design and by default" (Information Commissioner's Office, 2020[14]). The opinion also underlined that organisations that develop contact tracing apps need to ensure that their app complies with data protection laws where it processes data (Information Commissioner's Office, 2020[14]).

ii) Apple's venue check-in feature

Mr Gary Davis noted in his presentation that in response to requests from Governments, Apple and Google updated the Exposure Notifications Framework to allow users to check-

in to a venue without having to share their identity with the venue and crucially without having to share their location with the venue, the Government, and Apple and Google. The update allows for subsequent notificiations if an individual was exposed to a positive COVID-19 individual who was at the same location at the same time as the user. Mr Davis highlighted that Apple had set out a number of key policies in relation to this on-device venue check-in feature: *i)* location data on exposure notifications would not be collected; *ii)* the app does not share with any external party the user's check-in data or any other data associated or derived from the check-in without the user's explicit and informed consent; *iii)* the Public Health Authority app must protect all venue information by using a cryptographic one way hash function; *iv)* checking-in to a venue using the app is optional; *v)* the venue should not collect data about the check-in; *vi)* check-in data should be held locally on the device; *vii)* readable list of locations must be visible to the user to be able to delete the check-in if they wish; and *viii)* users must separately consent to be matched with a potential COVID-19 exposure.

(*Source:* Mr Gary Davis, OECD-GPA Workshop)

3. Data privacy aspects in the workplace during the pandemic

Session 2 examined the practices for managing COVID-19 in the workplace, and the data protection and privacy challenges. In particular, this session provided an opportunity for panellists to discuss the balancing of employee privacy and other fundamental rights with public health and occupational health and safety obligations. It also examined the implications of the increased scope of monitoring and surveillance practices.

Balancing employee rights and public/occupational health and safety rights in the management of COVID-19 in the workplace

16. To provide safe and secure working conditions and enable business continuity during the COVID-19 pandemic, employers collected (and continue to collect) a significant amount of data on their employees (Champetier de Ribes, 2021[15]). Data collected include symptom checks, temperature checks, travel history, location data, COVID-19 testing results and vaccination records.

17. Some of the most common technologies utilised to ensure social distancing and for contact tracing include thermal imaging technology, and smart wristbands using Bluetooth and GPS technology (ETUC, 2020[16]). The use of these technologies can allow employees to return to the workplace and provide them with assurance that they can carry out their duties safely. However, as noted by Ms Marguerita Lane (Labour Market Economist, OECD) in her presentation, the use of devices that give alerts to workers in case they breached social distancing may cause privacy concerns. In particular, there is a risk that after the COVID-19 pandemic businesses might wish to keep these devices and possibly use them for other purposes, such as learning when employees talk to each other (based on their proximity) or how many steps they take during work to observe their productivity.

18. Reflecting on these issues, Mr Andrew Pakes (Research Director, Prospect Union) noted that while some social distancing devices that alert workers if they are too close to each other store data locally, others send the data to a central database, prior to notifying the workers. Mr Andrew Pakes noted that Prospect Union (which is a trade union representing 150 000 members in the United Kingdom) questioned the lawful basis of the use of such devices under the GDPR. In particular, concerns surround the use of a central database when there is the possibility that data could be kept locally. In this regard, Mr Pakes pointed out that the Prospect Union would like to see better guidance to the implementation of the GDPR in addressing the new challenges which the COVID-19 pandemic brought with teleworking and increased surveillance of employees.

19. Employers are also seeking to take measures to protect employees from colleagues or visitors who have COVID-19 symptoms or have been exposed to someone with symptoms and may be contagious (Annerau, 2020[17]). Employers need to be especially attentive to employees at higher risk, or who share a household with vulnerable individuals (Annerau, 2020[17]). Some employers require a "health or immunity passport", a certification from a physician or authorised health care giver that the worker has been vaccinated or has tested negative to allow physical access to company's facilities.

PEAs issued varied guidance on how employers can provide a safe workplace while complying with data protection requirements

20. While employers have a duty to provide a safe environment as employees return to work, individual privacy must also be respected and data collection should be necessary, justified, and proportionate. A number of PEAs have issued guidance, but there are differing views on how employers should provide a safe workplace while complying with data protection requirements, depending on the jurisdiction (Mole et al., 2020[18]).

21. Notably, in France and Italy the CNIL and the Garante have stated that employers cannot mandate reporting and systematically collect health information about their employees (Mole et al., 2020[18]). Meanwhile, in Hungary, the Hungarian National Authority for Data Protection and Freedom of Information indicated that employers should encourage employees to report possible COVID-19 risks (Mole et al., 2020[18]). In Denmark, the Danish PEA also issued guidance on whether employers can collect (and in some cases disclose) information about employees in relation to COVID-19. The guidance notes that in some cases personal data, including sensitive data may be collected (and possibly disclosed), but underlines the importance of assessing whether the processing is limited to what is necessary (Mole et al., 2020[18]). In Australia, the Office of the Information Commissioner advised that only the minimum amount of personal information from employees reasonably necessary to maintain a safe workplace should be collected, used, or disclosed (as discussed in Box 3 below).

Box 3. Recommendations of the Office of the Australian Information Commissioner regarding the privacy of employees during the COVID-19 pandemic

Ms Elizabeth Hampton (Deputy Commissioner, Office of the Australian Information Commissioner) provided an overview of recent developments in relation to the privacy of employees during the COVID-19 pandemic.

In Australia, the Privacy Act treats public and private sector employee records differently. Notably, the handling of employee records by a private sector employer is exempt from the Privacy Act if it is directly related to a current or former employment relationship (Office of the Australian Information Commissioner, n.d.[19]). This means that a private sector employer does not have to grant a current or former employee access to their records under the Privacy Act (whilst Australian Government administration employee or past employee can access the personal information in their employee record under the Privacy Act) (Office of the Australian Information Commissioner, n.d.[19]). The Privacy Act is only applicable to a private sector employee record if the employer handles the personal information in the record for a purpose that is not directly related to the employment relationship (Office of the Australian Information Commissioner, n.d.[19]).

The Privacy Act is currently being reviewed by the Australian Government. The Office of the Australian Information Commissioner has recommended that the employee records exemption is removed. Ms Elizabeth Hampton noted that removing the exemption may address certain risks related to the handling of the personal information of employees, remove regulatory uncertainties, and create benefits for employers by increasing trust in their information handling practices.

The Office of the Australian Information Commissioner advised that employers should only collect the minimum amount of personal information about their

employees reasonably necessary to maintain a safe workplace during the pandemic and that they should inform staff about how their personal information is handled. In addition, the OAIC also recommended that employers should ensure that they keep the personal data of their employees secure.

(*Source:* Ms Elizabeth Hampton, OECD-GPA Workshop)

22. In the United Kingdom, the ICO has issued guidance for employers on collecting, storing and sharing personal information setting out six key, overarching steps in regard to data protection and employee health data collection during the pandemic. In particular, employers should:

i.) only collect and use data which is necessary;

ii.) keep data collection to a minimum;

iii.) be clear, open and honest with staff about their data;

iv.) treat people fairly - carefully consider decisions which are based on the health information collected;

v.) keep people's information secure and keep it only as long as necessary; and

vi.) employees must be able to exercise their information rights (Information Commissioner's Office, 2020[20]).

Changing monitoring and surveillance practices as a result of working from home

23. During the COVID-19 pandemic, working from home has become the new normal in many countries. To adapt to this sudden shift to online remote working, many companies had to implement new digital tools such as smart applications on personal and company-owned devices, webcams, and video-conferencing platforms. Some features of these various tools and platforms can have a significant impact on employees' privacy as they can lead to an ever increasing collection, processing and retention of personal data.

24. Employers may be tempted to systematically monitor their employees with the goal of ensuring appropriate work behaviour and enhancing productivity and efficiency (Cater and Heikkila, 2021[21]). Even before the COVID-19 pandemic, many companies had started to rely on workplace data analytics. For instance, a 2018 Gartner report revealed that of 239 large corporations, 50% were monitoring the content of employee social media accounts, emails, gathering biometric data and activity data to understand employees' use of the online workspace (Blackman, 2020[22]) (Kropp, 2019[23]). Another survey of C-suite executives concluded that 62% of their organisations were leveraging new digital tools to collect data on their employees (Blackman, 2020[22]) (Accenture, 2019[24]).

25. Companies that offer remote monitoring software have reported a surge of interest in their products (Connolly, 2020[25]). For instance, employers can install time-tracking software that may take desktop screenshots, alongside other functions such as activity status, keyboard monitoring and timesheets (Trade Union Congress, 2020[26]). Issues have also been raised about where data from video-conferencing calls is stored, and whether it is shared with other companies (Connolly, 2020[25]). Video-conferencing recordings may include the participants' voices, chats, and faces but also their private surroundings. In this regard, as highlighted by Mr Chris Calabrese (Senior Director, Privacy and Data Policy,

Microsoft) to better protect the privacy of its users Microsoft introduced blurred backgrounds on its videoconferencing platforms.

26. These trends have further accelerated during the COVID-19 pandemic. A survey conducted by the Trade Union Congress in 2020 revealed that 16% of trade union representatives noticed workers being subject to new productivity and performance monitoring technologies, for instance some videoconference platforms allowed event hosts to analyse their participants' attentiveness in real time, others to have participation recorded and stored (Trade Union Congress, 2020[26]). In relation to this, Mr Andrew Pakes noted that for instance an internal survey among the members of the Prospect Union concluded that *i)* only one in five workers were consulted about such surveillance technologies; and *ii)* a third of the workers revealed that their mental health was affected by the use of these technologies.

27. Ms Marguerita Lane further highlighted concerns surrounding the excessive monitoring of employees, also noting that some businesses that switched to teleworking also deployed surveillance software to monitor their workers. In particular, she confirmed that such software can monitor time spent on specific applications and may even take screenshots of an employee's activities. Ms Marguerita Lane underlined that such surveillance may raise serious privacy risks for employees, for instance in those cases when the screenshots can be read by the employer. Excessive monitoring may also cause stress for workers, especially in those cases when employers provide little information to employees about how their data is being collected and how it is being used. Such extensive monitoring may end up being counterproductive if employees start to believe that their employers do not trust that they are doing their work as required. In addition, performance monitoring technologies may be privacy-intrusive and counterproductive if the measurement does not capture the real value of what an employee contributes.

28. Mr Chris Calabrese noted that Microsoft has developed a "productivity score" feature. This tool, which was originally released in 2019, was designed to support businesses by providing insights about how the organisation uses Microsoft365 (Microsoft, 2021[27]). The organisation's score reflects "people and technology experience measurements" and can be compared to benchmarks from organisations that have a similar size (Microsoft, 2021[27]). However, critics of the tool noted that it allowed managers to gain data about individual employees and to learn about those who participate less in group chat conversations, fail to collaborate in shared documents, or send fewer emails (Hern, 2020[28]). Mr Chris Calabrese noted that the feedback which Microsoft received highlighted that the tool allowed employers to access too much information about their employees. Accordingly, Microsoft decided to change the settings of the tool and employers now may only access aggregate data about their employees.

29. To address the changing monitoring and surveillance practices at the workplace, the ICO in the United Kingdom is currently updating its Employment Practices Code (Baines, 2021[29]). If employers are considering monitoring staff, they should do this in a way that is compliant with data protection law and conduct a privacy impact assessment to assess the risks and apply mitigations. In the European Union, most member States have issued guidance of wide applicability covering all types of employees monitoring and processing which have been adapted over time (Riso, 2020[30]). One particular area of focus is the use of intrusive technologies, including biometrics and GPS tracking (Riso, 2020[30]) (Aloisi and Gramano, 2019[31]).

4. Vaccination programmes and travel passports

Along with the rolling out of national vaccination programmes, many countries introduced or started considering the introduction of COVID-19 "travel passports". Session 3 explored the ethical and privacy issues of this measure.

COVID-19 "travel passports" can help to lift restrictions and support the wider economy, but raise ethical and privacy concerns

30. There are a number of different terms that describe COVID-19 "travel passports", including "green passes", "immunity certificates", or "vaccine passports" (Renieris, 2021[32]). The underlying concept behind these terms is the same – to develop and provide a digital or physical document that certifies an individual's COVID-19 health status, including whether the individual was vaccinated against, recovered from, or tested negative for the virus (Renieris, 2021[32]). COVID-19 "travel passports" usually require a combination of identity verification tools, health information, and a mechanism to present the certificate (for instance in a QR code) (Renieris, 2021[32]). Mr Alan Butler (Executive Director and President, Electronic Privacy Information Center) highlighted in his presentation that most COVID-19 "travel passports" incorporated important features that limit the disclosure of personal data.

31. Supporters of COVID-19 "travel passports" underline that such certificates can help lift current restrictions to national and international travel, protect transport users, support transport operators, and the wider economy. This is particularly important for the tourism sector which has been significantly impacted by travel restrictions (OECD, 2021[4]). OECD countries where tourism is one of the most important contributors to the economy – such as Mexico, Spain, Portugal and Greece – are also among those that experienced the greatest fall in GDP in 2020 (OECD, 2021[4]).

32. Even in light of these advantages, COVID-19 "travel passports", raise serious ethical issues, particularly when also required to demonstrate an immunity status in daily life activities, such as for return to work, or for leisure and social activities. In particular, COVID-19 "travel passports" that are solely available in a digital format may risk the exclusion of significant portions of the population, such as older people who may not have smartphones or disadvantaged people who cannot afford them (Muscato, 2021[33]). Concerns around COVID-19 "travel passports" include not just exclusion, but possible exacerbation of existing inequities and discrimination against individuals who may not have access to health care or the vaccine, and those who cannot or do not wish to take it.

33. Mr Frank Ulrich Montgomery (President, Standing Committee of European Doctors) highlighted that whilst most of the vaccines offer a high-level of protection against COVID-19, there are still considerable scientific questions around the duration of protection or efficacy of the vaccines, including against new mutations of the virus (Ada Lovelace Institute, 2021[34]). Governments also need to agree on which of the several COVID-19 vaccines would be accepted for the purpose of COVID-19 "travel passports" (Bacchi, 2021[35]). Opinions also differ on whether individuals who recovered from COVID-19 are protected from a new infection, and if so, for how long (Bacchi, 2021[35]). COVID-19 "travel passports" that are based on negative test results may also be problematic, as individuals can be infected any time after taking the test (Bacchi, 2021[35]).

A number of organisations issued guidance to enable safe international travel during the COVID-19 pandemic

34. Building public confidence and trust in "travel passports" particularly regarding their privacy and data governance features remains a challenge (Ada Lovelace Institute, 2021[34]). Whilst the collection and processing of data for enabling safe travel may be justifiable on public health grounds, the sharing of sensitive data should be done in a privacy protective manner (Global Privacy Assembly, 2021[3]). In this regard, Mr Alan Butler emphasised in his presentation that strong privacy protection mechanisms are essential to gather public trust for COVID-19 "travel passports". He also noted that the implementation of such systems require co-ordination to ensure that COVID-19 "travel passports" are interoperable, fair and equitable.

35. To enable safe international travel during the pandemic, a number of guidance documents were released. Notably, the GPA released guidance on the use of health data for domestic and international travel purposes (see details below in Box 4, which outlines ten recommendations from the GPA reflecting established privacy principles (Global Privacy Assembly, 2021[3])).

Box 4. The Global Privacy Assembly's guidance on privacy issues emerging from the COVID-19 pandemic

The GPA provided continued guidance to more than 130 PEAs on data protection and privacy issues that emerged from the COVID-19 pandemic. As noted by Melissa Mathieson (Head of High Priority Investigations and Intelligence, Information Commissioner's Office, United Kingdom), in March 2020 the GPA released a statement noting the challenges brought by the COVID-19 pandemic (GPA, 2020[36]).

To provide guidance to governments and other organisations in processing data for international travel, the GPA released global data protection principles and good practice, which included the following:

i.) 'privacy by design and default' should be embedded into the design of any system, data sharing arrangement or app that processes health data for international travel. To ensure that data protection by design principles are implemented in practice, the GPA it is recommended to conduct "a formal and comprehensive assessment of the privacy impact on individuals" before the processing of any data. Consulting data protection and privacy authorities and their guidance is advisable.

ii.) the collection, use and disclosure of personal data should have a clearly defined purpose;

iii.) all organisations should ensure that they only process health data with lawful authority and when it is necessary and proportionate to do so;

iv.) the data protection rights of vulnerable individuals should be protected;

v.) individuals should have clear and accessible information about how their data is being utilised and by whom;

vi.) organisations should collect the minimum health information from individuals;

vii.) measures should be used to address the risks of directly sharing information from health records for travel purposes;

viii.) the cybersecurity risks of any digital systems or apps should be fully assessed;

ix.) organisations should carefully consider how long data should be retained and design a retention schedule for deletion of information that is no longer required;

x.) sunset clauses that foresee the permanent deletion of data once the pandemic ends should be built in by design.

Source: Ms Melissa Mathieson, OECD-GPA Workshop and based on (Global Privacy Assembly, 2021[3]).

36. In addition, the OECD developed a Blueprint Initiative to promote safe international travel during COVID-19, which OECD Ministers endorsed at the OECD's Ministerial Council Meeting, held from 31 May – 1 June 2021 (see below in Box 5).

Box 5. The OECD Initiative for Safe International Mobility during the COVID-19 Pandemic

Mr Frederico Guanais (Deputy Head of the Health Division, Directorate for Employment, Labour and Social Affairs, OECD) presented the OECD Initiative for Safe International Mobility during the COVID-19 Pandemic. As highlighted by Mr Frederico Guanais, the OECD Initiative proposes:

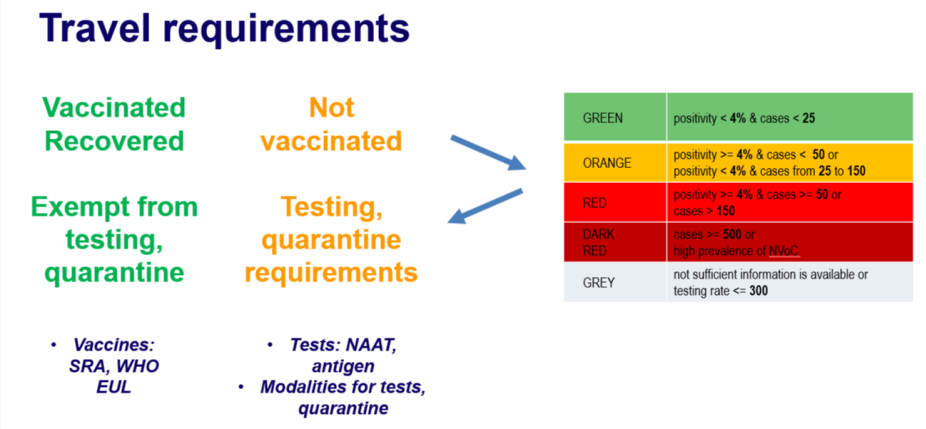
i.) a temporary, cross-sectoral forum for knowledge sharing related to international travel; and

ii.) a voluntary, flexible, and temporary blueprint which is in line with recent certificate initiatives and seeks to provide policy guidance on measures for safe international travel with recommendations on tests, vaccinations, certification and data exchange (OECD, 2021[4]).

In terms of data protection, the initiative highlights interoperability, security and privacy protection by design which are recognised as key principles (OECD, 2021[4]). The OECD blueprint also proposes that the system should draw on existing tools and mechanisms for sharing information, and should strictly collect only the necessary data (data minimisation). The blueprint also recommends that in case countries decide to use COVID-19 "travel passports", these should be based on a common set of information elements and agreed measures for digital security.

In relation to travel requirements, the blueprint proposes that those individuals who have been fully vaccinated or recovered from COVID-19 should be exempt from testing and quarantine mechanisms. For those travellers who have not been vaccinated the blueprint proposes a "traffic-light" system of testing and quarantine requirements (as illustrated below in Figure 2).

Figure 2. The proposed measures of the OECD blueprint for safer travel



Source: Mr Frederico Guanais, OECD-GPA Workshop and (OECD, 2021[4]).

37. The Council of Europe has also issued a statement highlighting that data protection principles should be central to the technology used for COVID-19 "travel passports" due to their privacy-invasive nature. The statement noted that it is crucial that data subjects are informed about the processing of their personal data (Council of Europe, 2021[37]). In addition, the statement emphasised the need for proportionality and minimisation in data collection and processing, called for decentralised solutions (e.g. in the storage of data on users' mobile devices) and recommended a privacy-by-design approach (Council of Europe, 2021[37]). In addition, as noted by Ms Alessandra Pierucci (Chair of the Committee of Convention 108 of the Council of Europe) an impact assessment should be carried out prior to the processing of data with a particular focus on the "efficiency of the intended processing and the possibility of resorting to less intrusive measures" (Council of Europe, 2021[37]). The statement indicates that data should be deleted when the "specified storage period has expired" and that digital tools (such as contact tracing apps or self-diagnosis tools) should be temporary (Council of Europe, 2021[37]).

38. Additionally, the Standing Committee of European Doctors (CPME) which represents national medical associations across Europe, released a statement regarding the European Union's Digital Green Certificate (Standing Committee of European Doctors, 2021[38]). Their statement called on the EU to ensure no discrimination against persons who have not yet been able to get vaccinated and those who cannot be vaccinated. The statement also underlined the need for strong data protection safeguards on patient data. In this regard, Mr Frank Ulrich Montgomery recalled that the immunity of individuals against COVID-19 cannot be fully assessed. He emphasised that the Certificate should remain voluntary and noted that until all EU citizens had a chance to get vaccinated against COVID-19, the Certificate may pose a risk of discrimination.

5. Conclusions

39. In her concluding remarks, Ms Elettra Ronchi (Head of Data Governance and Privacy Unit, OECD) thanked the moderators and all speakers for their interventions. She highlighted the following key takeaways from the workshop:

- Privacy and data protection has often been framed during the COVID-19 pandemic as an "all or nothing proposition" in which stakeholders need to decide between individuals' privacy or their health and safety. Nevertheless, the OECD's work on enhancing access to and sharing of data has proved this narrative to be misleading. This piece of work has revealed that securing multiple aims and fundamental rights is possible through well-designed data governance frameworks and data protection regimes.
- Critical debates about the privacy, data governance and health-related implications of the COVID-19 pandemic often take place in silos. Governments, PEAs, academia, civil society, international organisations and other stakeholders should work in partnership to break these silos and to ensure transparency and fairness in the debates surrounding the COVID-19 pandemic.
- There have been changes during the COVID-19 pandemic regarding the level of privacy protection that people expect. As highlighted by a number of speakers during the workshop, as a result of a "take it or leave it" perception, some individuals have started to view privacy as a right that has to be partially or even fully sacrificed in order to facilitate and comply with exceptional COVID-19 measures.
- Countries reported different experiences in their responses to COVID-19 and concluded that there is no "one-size-fits-all" solution to the pandemic. In particular, contact-tracing is not a "silver-bullet" and should be complemented with additional measures by public authorities. The outcome of different COVID-19 measures may depend on the social, cultural and economic environments in which they are deployed.

40. Mr Joe Cannataci (United Nations Special Rapporteur on the Right to Privacy) likewise thanked the organisers, speakers and participants of the workshop. He concluded in his remarks that the OECD-GPA workshop was a particularly important event as it helped to break the silos between different stakeholder groups that are working on addressing the challenges of the COVID-19 pandemic.

Annex A. Country case studies - examples of policy and legal frameworks developed in response to the COVID-19 pandemic

Italy

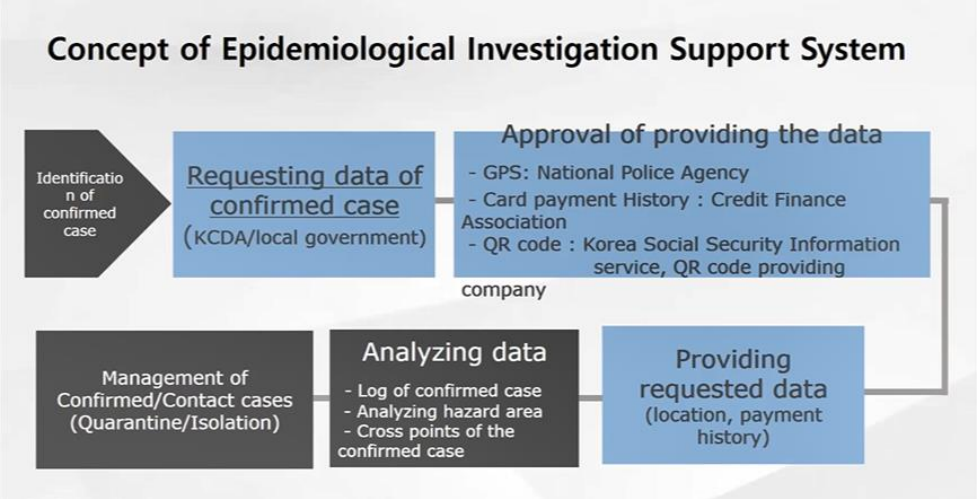
- Mr Guido Scorza (Office of the Garante, Italy) highlighted that in March 2020, the Italian government passed a legislative decree to establish a special legal framework for collecting and sharing personal data by public health authorities and by private organisations that are part of the Italian health system for the duration of the COVID-19 emergency (OECD, 2020[1]) (Della Repubblica Italiana, 2020[39]).
- In April 2020, Italy passed another legislative decree (Decree 28/2020) outlining specific standards that must be followed in the development of a voluntary contact tracing app.
- Following-up on these measures, in April 2021, the Italian government approved the "Italy reopens" decree which introduced a "Green Pass" that initially aimed to ease safer movements between regions and to access certain public venues (European Data Protection Board, 2021[40]) (Pizzoli, 2021[41]).

Source: Mr Guido Scorza, OECD-GPA Workshop

Korea

- Mr Sangwoo Tak (Korea Disease Control and Prevention Agency) noted that in July 2015 Korea enacted an "Infectious Disease Control and Prevention Act" as a result of the 2015 Middle East respiratory syndrome outbreak in the country. The legislation aimed to establish a legal framework for the disclosure of information during a public health emergency. The law dictates that the government has to inform citizens about infectious disease outbreak situations, as well as about the prevention and control measures being taken. It also states that government should promptly disclose relevant information to the public (Infectious Disease Control and Prevention Act, 2015[42]).
- In light of the COVID-19 pandemic, the law was revised in August 2020 to exclude personally identifiable information, such as gender, age, and nationality from information disclosure.
- Mr Sangwoo Tak further noted in his presentation that the "Infectious Disease Control and Prevention Act" provided the legal basis for Korea's contact tracing system called "Epidemiological Investigation Support System". In particular, the law states that the Korea Disease Control and Prevention Agency and local governments may ask suspected infectious disease patients to provide personal information (including name, address, and telephone number) in order to obtain the movements of confirmed cases. In addition, the Korean National Policy (when requested by the Korea Disease Control and Prevention Agency or a local government) may request a telecommunication service provider to share the location information of suspected and confirmed cases of infectious disease patients. Figure 3 provides details about the "Epidemiological Investigation Support System":

Figure 3. The Korean Epidemiological Investigation Support System



Source: Mr Sangwoo Tak (Korea Disease Control and Prevention Agency), OECD-GPA Workshop

- Korea developed guidelines to ensure that when data is disclosed about a COVID-19 patient, there is no personally identifiable information shared. In particular, the government only releases the following information in relation to the COVID-19 patient (for fourteen days after the diagnosis): *i*) the address of public venues that the patient visited; *ii)* the time of exposure (contact); *iii)* the time and use of public transportation; and *iv)* the decontamination status of the affected facility. The patient's name, gender, age, nationality, and home residence address are not released. Information about the patient's company is only disclosed in exceptional cases (for instance in case of concern about a "super-spreading event").
- The Korean Personal Information Protection Commission also conducts a monthly inspection of local government webpages to ensure that they are privacy compliant when they release data about COVID-19 patients. In this regard, the Korean Personal Information Protection Commission uses three criteria during its inspection: *i)* checking whether there is any personally identifiable information released about the COVID-19 patient; *ii)* checking whether the information about the COVID-19 patient was removed after 14 days; *iii)* checking that the location data cannot be linked to the COVID-19 patient. Based on the investigation, the Personal Information Protection Commission and the Korea Disease Control and Prevention Agency may ask the local government to make corrections and report back after the correction was made to the Korea Disease Control and Prevention Agency.

Source: Mr Sangwoo Tak, OECD-GPA Workshop.

Mexico

- Mr Vitalio Ruiz Bernal (National Institute for Transparency, Access to Information and Personal Data Protection) highlighted in his presentation that Mexico passed two laws (one for the private sector and the other one for the public sector) on the collection and processing of health and location data during the COVID-19 pandemic.

- In particular, these laws state that the COVID-19 patient needs to provide consent for the processing of his or her data. However, in exceptional cases this consent may be waved. Additionally, they provide that only a minimum amount of personal data should be collected in the context of the COVID-19 pandemic (and that this data should not be used for other purposes).
- In April 2020, The Mexican Ministry of Health also introduced its own contact tracing app called "COVID-19 MX". In addition, local governments were also allowed to release their own contact tracing apps. The use of all of these apps is voluntary for citizens. Mr Vitalio Ruiz Bernal further noted that the "COVID-19 MX" app requests some mandatory information from the user (including age, gender, telephone number, vulnerability group, state) and also some voluntary information (including name). The app does not allow the transfer of personal data to third parties.

Source: Mr Vitalio Ruiz Bernal, OECD-GPA Workshop.

Singapore

- Mr Yeong Zee Kin (Personal Data Protection Commission of Singapore) highlighted in his presentation that Singapore followed a centralised contact tracing strategy co-ordinated by the Ministry of Health. In this regard, the Singaporean government develop two separate apps:
  - i) "Safe Entry" – this application allows citizens in Singapore to record when they check-in and out of places that they visited.
  - ii) "Trace Together" – this application's primary aim is to track individuals who have been exposed to COVID-19. This information is used to identify close contacts based on the duration and the proximity of the encounter between the two users (OECD, 2020[2]). The app then alerts those who came in contact with someone who tested positive for COVID-19. Once an individual is confirmed to be infected with COVID-19, they can allow the Ministry of Health, hospitals and third parties to access data in the app to help identify close contacts.
- Mr Yeong Zee Kin pointed out in his presentation that in terms of privacy protections, both of these apps are embedded with privacy-by-design.[3] Privacy-by-design aims to deliver the highest degree of privacy by ensuring that personal data protection are built into the system, by default (OECD, 2020[2]). The data that is collected through these apps is held by the Singaporean Public Health Department.

Source: Mr Yeong Zee Kin, OECD-GPA Workshop.

[3] Privacy-by-design aims to deliver the highest degree of privacy by ensuring that personal data protection are built into the system, by default (OECD, 2020[2]).

Annex B.

Agenda of the OECD-GPA Online Workshop on "One Year Later: Addressing the Data Governance and Privacy Implications of the COVID-19 Pandemic and the Road to Recovery"

Day 1

11:40 – 12:00	**Meeting registration and check-in**
12:00 – 12:10	**Opening and welcome remarks** • Elizabeth Denham CBE, Chair of the Global Privacy Assembly, Information Commissioner, UK • Andrew Wyckoff, Director for Science, Technology and Innovation, OECD
12:10 – 13:40	**Session 1: Reflecting on the varying policy and legal frameworks in response to the COVID-19 pandemic** This session seeks to review one year later how governments have approached the COVID-19 pandemic and the policy and legal frameworks that were developed in support of their response, in particular of contact tracing and containment efforts. It will examine how and in what ways governments have evaluated their approaches and what changes were deemed necessary. It will build on lessons learned from countries across world regions and explore possible lessons that can be learned for future crises. This session will focus on questions such as: • What policy and legal frameworks were developed to enable the exceptional surveillance measures (e.g. contact tracing apps) in combatting the COVID-19 pandemic? • Have these policy and legal frameworks changed throughout the pandemic? If so, why and in what ways have countries evaluated their contact tracing and containment approaches one year after the pandemic? • What lessons can be learned from these countries' approaches to the COVID-19 pandemic and their road to recovery? **Moderator:** Raymund Enriquez Liboro, Privacy Commissioner and Chairman, Philippines National Privacy Commission and Chair of the GPA COVID-19 Taskforce **Lead discussants** [8 mins each]**:** • Discussant 1 – Daniel Kaufman, Acting Director, Bureau of Consumer Protection (US) • Discussant 2 – Guido Scorza, Office of the Garante (Italy) • Discussant 3 – Sangwoo Tak, Director, Division of Risk Assessment, Korea Disease Control and Prevention Agency (Korea)

	• Discussant 4 – Vitelio Ruíz Bernal, Director-General of Investigation and Verification of the Private Sector, National Institute for Transparency, Access to Information and Personal Data Protection (Mexico) • Discussant 5 - Yeong Zee Kin, Deputy Commissioner, Personal Data Protection Commission (Singapore) • Discussant 6 - Gary Davis, Global Director of Privacy & Law Enforcement Requests, Apple **Followed by open discussion**
13:40 – 13:50	**Short Break**
13:50 – 15:15	**Session 2: Data privacy aspects in the workplace during the pandemic** Throughout the pandemic, employers have collected a greater level of data on their employees in an attempt to ensure business continuity, including symptom checks, temperature checks, travel history, testing for COVID-19 and vaccination records. In this session panelists will discuss the balancing of employee rights and public/occupational health and safety rights in the management of COVID-19 in the workplace. They will also discuss how the shift to working from home may be changing monitoring and surveillance practices. The session will focus on questions such as: • What data are employers permitted to collect about their employees during the pandemic? • Have PEAs issued guidance to employers on the data protection and privacy challenges arising from employers responses to COVID-19? • What role should governments and PEAs play to ensure that measures and necessary and proportionate and provide sufficient data protection and privacy protections for employees during the crisis? • Has the agency of the employee been diminished as result of provisions introduced in the workplace in response to the pandemic? **Moderator:** Anna Byhovskaya, Senior Policy Advisor, TUAC **Lead discussants** [8 mins each]**:** • Discussant 1 – Marguerita Lane, Labour Market Economist, OECD • Discussant 2 – Elizabeth Hampton, Deputy Commissioner, Office of the Australian Information Commissioner (Australia) • Discussant 3 – Andrew Pakes, Research Director, Prospect Union (UK) • Discussant 4 – Chris Calabrese, Senior Director, Privacy and Data Policy, Microsoft **Followed by open discussion** **Close of Day 1 – 15:15**

Day 2

11:40 – 12:00	**Meeting registration and check-in**
12:00 – 12:10	**Opening and welcome remarks** • Steve Wood, Deputy Commissioner (Policy), UK ICO and Chair of the WPDGP
12:10 – 12:25	**Presentation by ICO-GPA on joint statement for international travel** ICO/GPA will present on the joint statement on sharing of health data for domestic and international travel. • Melissa Mathieson, Head of High Priority Investigations and Intelligence, ICO UK **Followed by Q&A**
12:25– 12:40	**Presentation on the OECD Initiative for Safe International Mobility during the COVID-19 Pandemic** The OECD will present its initiative for Safe International Mobility during the COVID-19 Pandemic (including Blueprint). • Frederico Guanais, Deputy Head of the Health Division, Directorate for Employment, Labour and Social Affairs, OECD **Followed by Q&A**
12:40 – 12:50	**Short Break**
12:50 – 14:30	**Session 3: Vaccination programmes and travel passports** This session will focus on the challenges raised as governments embark on national vaccination programmes, including questions surrounding the extent of data required to measure the effectiveness of vaccines. In particular, as more and more countries, as well as the EU, are considering the introduction of COVID-19 "travel passports", this session will explore the ethical and privacy issues of this measure. These concerns may include inequality, exclusion and discrimination particularly in relation to those individuals who do not have access to the vaccine, do not wish to take it, or cannot take it. The session will focus on questions such as: • How are governments monitoring the effectiveness of vaccination programmes? Are they leveraging data collected during contact tracing to assist vaccination efforts? • What are the privacy and data governance implications of COVID-19 "travel passports"? • What role should PEAs play in introducing guidance to governments on travel passports?

	• What public and private partnerships are emerging to enable these initiatives? • What potential privacy concerns may these initiatives raise? **Moderator:** Steve Wood, Deputy Commissioner (Policy), UK ICO and Chair of the WPDGP **Lead discussants** [10 mins each]**:** • Discussant 1 – Alessandra Pierucci, Chair of the Committee of Convention 108 of the Council of Europe • Discussant 2 – Florence Raynal, Deputy Director/Head of Department of International and European Affairs, CNIL (France) • Discussant 3 – Frank Ulrich Montgomery, President, Standing Committee of European Doctors • Discussant 4 – Alan Butler, Executive Director and President, Electronic Privacy Information Center (EPIC) **Followed by open discussion**
14:30 - 15:00	• Elettra Ronchi, Head of Data Governance and Privacy Unit, OECD • Joe Cannataci, United Nations Special Rapporteur on the Right to Privacy **Close of Meeting** • Steve Wood, Deputy Commissioner (Policy), UK ICO and Chair of the WPDGP

References

Accenture (2019), *More Responsible Use of Workforce Data Required to Strengthen Employee Trust and Unlock Growth, According to Accenture Report*, https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.htm. [24]

Ada Lovelace Institute (2021), *Checkpoints for vaccine passports*, https://www.adalovelaceinstitute.org/wp-content/uploads/2021/05/Checkpoints-for-vaccine-passports_requirements-for-governments-and-developers_Ada.pdf. [34]

Aloisi, A. and E. Gramano (2019), *Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3399548. [31]

Annerau, S. (2020), *Employee monitoring in the context of COVID-19*, https://globaldatahub.taylorwessing.com/article/employee-monitoring-in-the-context-of-covid-19. [17]

Bacchi, U. (2021), *Coronavirus vaccine passports: everything you need to know*, https://www.weforum.org/agenda/2021/04/coronavirus-covid19-vaccine-passports-travel/. [35]

Baines, J. (2021), *ICO Employment Practices Code to be updated*, https://www.mishcon.com/news/ico-employment-practices-code-to-be-updated. [29]

Blackman, R. (2020), *How to Monitor Your Employees - While Respecting Their Privacy*, https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy. [22]

Cater, L. and M. Heikkila (2021), *Your boss is watching: How AI-powered surveillance rules the workplace*, https://www.politico.eu/article/ai-workplace-surveillance-facial-recognition-software-gdpr-privacy/. [21]

Champetier de Ribes, C. (2021), *COVID-19: Guidance for Employers in France*, https://www.twobirds.com/en/news/articles/2020/france/covid19-guidance-for-employers-in-france. [15]

Connolly, R. (2020), *The pandemic has taken surveillance of workers to the next level*, https://www.theguardian.com/commentisfree/2020/dec/14/pandemic-workers-surveillance-monitor-jobs. [25]

Council of Europe (2021), *CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA*, https://rm.coe.int/t-pd-bur-2021-6rev2-statement/1680a25713. [37]

Council of Europe (2020), *Digital Solutions to Fight COVID-19*, https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c. [10]

Della Repubblica Italiana (2020), *Gazzetta Ufficiale*, https://www.gazzettaufficiale.it/eli/gu/2020/03/09/62/sg/pdf. [39]

ETUC (2020), *COVID-19 Watch ETUC briefing on new technologies allowing more surveillance at work*, https://www.etuc.org/sites/default/files/publication/file/2020-10/20200930_covid-19%20Briefing%20on%20survelliance%20technologies%20%28002%29.pdf. [16]

European Data Protection Board (2021), *Italian DPA: Green light from the Italian SA subject to adequate safeguards*, https://edpb.europa.eu/news/national-news/2021/italian-dpa-green-light-italian-sa-subject-adequate-safeguards_en. [40]

European Union Agency for Fundamental Rights (2020), *Coronavirus Pandemic in the EU - Fundamental Rights Implications: With a Focus on Contact-Tracing Apps*, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf. [9]

Federal Trade Commission (2021), *Protecting Consumers During the COVID-19 Pandemic: A Year in Review*, https://www.ftc.gov/system/files/documents/reports/protecting-consumers-during-covid-19-pandemic-year-review/covid_staff_report_final_419_0.pdf. [11]

Federal Trade Commission (2020), *Decision and Order, In re. Zoom Video Comms., Inc., Docket No. C-4731 (FTC)*,, https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf. [12]

Global Privacy Assembly (2021), *COVID-19 Resources Library*, https://globalprivacyassembly.org/covid19/covid19-resources/. [8]

Global Privacy Assembly (2021), *GPA Executive Committee joint statement on the use of health data for domestic or international travel purposes*, https://globalprivacyassembly.org/gpa-executive-committee-joint-statement-on-the-use-of-health-data-for-domestic-or-international-travel-purposes/. [3]

GPA (2020), *Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic*, https://globalprivacyassembly.org/gpaexco-covid19/. [36]

Hern, A. (2020), *Microsoft productivity score feature criticised as workplace surveillance*, https://www.theguardian.com/technology/2020/nov/26/microsoft-productivity-score-feature-criticised-workplace-surveillance. [28]

Infectious Disease Control and Prevention Act (2015), , https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=172762&viewCls=engLsInfoR&urlMode=engLsInfoR&chrClsCd=01020#0000. [42]

Information Commissioner's Office (2020), *Apple and Google joint initiative on COVID-19 contact tracing technology*, https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf. [14]

Information Commissioner's Office (2020), *Data protection and employee data during coronavirus - six data protection steps for organisations*, https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-six-data-protection-steps-for-organisations/. [20]

Kropp, B. (2019), *The Future of Employee Monitoring*, https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring. [23]

Microsoft (2021), *Microsoft Productivity Score*, https://docs.microsoft.com/en-us/microsoft-365/admin/productivity/productivity-score?view=o365-worldwide. [27]

Mole, A. et al. (2020), *COVID-19 in the Workplace: differing guidance from data protection authorities*, https://www.twobirds.com/en/news/articles/2020/global/covid19-in-the-workplace-guidance-from-data-protection-authorities. [18]

Muscato, L. (2021), *Got your covid shots? You might have to prove it*, https://www.technologyreview.com/2021/04/09/1021934/got-your-covid-shots-you-might-need-vaccine-passport/. [33]

OECD (2021), *OECD initiative for safe international mobility during the COVID-19 pandemic (including blueprint)*, https://read.oecd-ilibrary.org/view/?ref=1095_1095916-dq6euk2mq6&title=OECD-initiative-for-safe-international-mobility-during-the-COVID-19-pandemic-including-blueprint&_ga=2.136032625.1179630561.1633272271-718873817.1564141664. [4]

OECD (2020), "Ensuring data privacy as we battle COVID-19", https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/ (accessed on 10 March 2021). [1]

OECD (2020), *OECD Digital Economy Outlook 2020*, https://www.oecd-ilibrary.org/docserver/bb167041-en.pdf?expires=1631290554&id=id&accname=ocid84004878&checksum=3863479526713E24B5DF6E6B449FAAB9. [6]

OECD (2020), "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics", http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/ (accessed on 10 March 2021). [2]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use Across Societies*, https://www.oecd-ilibrary.org/docserver/276aaca8-en.pdf?expires=1631546813&id=id&accname=ocid84004878&checksum=ACC78DAC390B68BC71878C8EE80AF5C8. [7]

OECD-Harvard Global Health Institute (2017), *Expert Consultation on "Mobile Technologies Based Services for Global Health and Wellness: Opportunities and Challenges*, https://one.oecd.org/document/DSTI/CDEP/SPDE(2017)10/en/pdf. [5]

Office of the Australian Information Commissioner (2020), *Australian Community Attitudes to Privacy: Survey 2020*, https://apo.org.au/sites/default/files/resource-files/2020-09/apo-nid308960.pdf. [13]

Office of the Australian Information Commissioner (n.d.), *Your employee record*, https://www.oaic.gov.au/privacy/your-privacy-rights/employment/your-employee-record/. [19]

Pizzoli, P. (2021), *Italy: New government decree sets a path to reopening*, https://think.ing.com/articles/italy-new-government-decree-sets-a-path-to-reopening. [41]

Renieris, E. (2021), *What's Really at Stake with Vaccine Passports*, https://www.cigionline.org/articles/whats-really-stake-vaccine-passports/. [32]

Riso, S. (2020), *Employee monitoring and surveillance: The challenges of digitalisation*, https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20008en.pdf. [30]

Standing Committee of European Doctors (2021), *CPME Statement on the Digital Green Certificate*, https://www.cpme.eu/index.php?downloadunprotected=/uploads/adopted/2021/5/CPME_AD_EC_19052021_043.FINAL_.CPME_.Statement.on_.Digital.Green_.Certificate.pdf. [38]

Trade Union Congress (2020), *Technology managing people: The worker experience*, https://www.tuc.org.uk/sites/default/files/2020-11/Technology_Managing_People_Report_2020_AW_Optimised.pdf. [26]