2 June 2020

Looking Beyond COVID-19:
Future Impacts on Data Protection and the Role of the Data Protection Authorities

Observations by the Centre for Information Policy Leadership (CIPL)

These observations are solely those of CIPL's leadership team and do not represent the views of any particular CIPL member. We have based them on our expertise, experience and discussions we have been having with different stakeholders in the past month. Our objective is to anticipate the main impacts, challenges and opportunities of the COVID-19 crisis on organisations, data protection authorities (DPAs) and individuals through the lens of data protection in the post-COVID-19 world. The observations herein should be read together with our 14 April 2020 op-ed "Covid-19 Meets Privacy: A Case Study for Accountability."

I. INTRODUCTION

The COVID-19 crisis is imposing a wide range of immediate and likely long-term impacts on organisations, governments, regulators, people and society at large. Many of them are likely to stay with us beyond the immediate crisis and change the way we all live, work and interact going forward. These impacts likely will also be felt in data privacy – from how we perceive this right in light of other rights to how we behave and what we expect. They will also change the way organisations and governments collect, use and share data (not just in the COVID-19 context, but generally).

In this paper, we examine some of these trends from the point of view of organisations, DPAs and society. We also try to anticipate how these trends may force all of these actors to adapt and change in the post-COVID-19 world, including and particularly DPAs. We also suggest that organisational accountability – championed, encouraged and enforced by DPAs – will be essential to mitigating any challenges that such changes might pose for data protection.

II. DATA PRIVACY IMPLICATIONS AND THE ROLE OF ORGANISATIONS IN A COVID-19 AND POST-COVID-19 WORLD

The COVID-19 pandemic has forced organisations to refocus their activities both to secure their own business operations and to assist public authorities' decision-making and emergency response activities with their relevant technologies, tools, resources and personal data. Most of these actions have privacy and data protection implications. Organisations have had to assess and quickly decide how to pursue new and beneficial uses of data consistent with applicable data protection requirements. In the pre-COVID-19 world, these would have required multi-stakeholder prior assessments and reviews, including by DPAs.

Unfortunately, while DPAs have issued guidance on certain COVID-19-related topics and efforts, there is currently no general playbook or precedent for organisations to effectively adapt their interpretations of applicable data protection requirements to new data uses in times of crisis. Traditional analyses and interpretations of legal requirements, as well as specific data protection tools and measures, will still have to be adapted and updated (during the pandemic and after) to enable these new and beneficial data uses. This will continue even after the current crisis.

Organisational accountability will have to play a key role in ensuring effective and robust data protection in this context. In addition, where existing legal requirements are ill-adapted to the current

needs to use data effectively and accountably (even when interpreted flexibly), stakeholders, including DPAs, should not hesitate to call for necessary shifts in interpretation and reforms. Any new or amended rules should enable greater flexibility by organisations to use data for the social good without sacrificing appropriate privacy protections. Here too, organisational accountability – if properly understood and implemented through such laws – can provide the necessary framework to make this possible.

1. **Addressing the immediate crisis and business continuity**

Most organisations have had to quickly refocus their strategies and resources to ensure business continuity following governmental lockdown orders. All organisations, both in the private and public sectors, have had to **reimagine their workforce practices and patterns**. This includes organising efficient and secure telework; protecting the health of on-site employees and any third parties; protecting the health and wellbeing of employees working from home; ensuring support to their workforce in the ongoing lockdown and health crisis; and enabling responsible return to work. They also had to upgrade their security processes and tools **to respond to increased cybersecurity threats and scams** created by the crisis.

These changes have resulted in new business processes and different needs for processing personal data, including sensitive personal data, of employees, contractors and job candidates. These new data processing trends are particularly relevant in countries where employee data is considered "personal data" whose processing must comply with applicable data protection laws. Such new processes include: utilising novel employee prescreening and recruitment practices; using work shift management systems to reduce density, schedule breaks and reduce other bottlenecks so that employees can safely return to work; adopting temperature and immunity checks and tests; dealing with individuals who have, or are suspected to have contracted, COVID-19; tracing internal contacts; employing ongoing management of all employees' health and wellbeing; providing counselling; supporting remote workers' mental health; and enhancing monitoring of devices, networks and activities to detect and prevent security vulnerabilities, threats and data breaches. All of these have raised novel data protection compliance challenges or increased their scale. They have also raised the level of importance of existing topics that data protection officers (DPOs) and privacy teams have had to deal with immediately.

An additional, common challenge for global organisations has been the need to ensure consistent rules and processes in fighting COVID-19 for all of their global entities and workforce, when applicable laws, data protection rules and guidance differ from country to country or when their interpretation is inconsistent. This challenge has become even more pronounced as employees worldwide expect and demand organisations to take proactive measures to ensure their health and wellbeing.

In particular, when data protection laws require a legal basis to process personal data, organisations have struggled to decide on the most appropriate choice of legal basis for processing of employees' personal data. This is especially true when the relevant DPA interpretation of the legal basis has been narrow. This problem is exacerbated when the data is considered "sensitive" and subject to additional limitations that may impede certain processing that may be necessary for health or employment purposes. Indeed, organisations are struggling to identify the appropriate grounds for processing sensitive data when such grounds are very limited and interpreted narrowly by DPAs. For example, as it relates more specifically to the GDPR, would employees' consent be valid (i) in a potentially imbalanced employment relationship and (ii) where an employee's entry into the premises is conditioned on her/his consenting to a temperature check? Or, would it be better to rely on other

grounds, such as legitimate interest, vital interest, legal obligation or even a public interest, given that organisations are often acting in the public interest or as a result of an employer's duty of care?

Over time, organisations will rely increasingly on technology and data to ensure their own safety and resilience. Many of these emerging practices of monitoring their on-site and remote workforce, systems and devices will become the new normal. They are likely to remain permanent features and even develop further for all organisations post COVID-19. In fact, some leading technology organisations and cloud platforms are developing new products and software to assist their clients and navigate work and the workforce during and after the pandemic. These include monitoring, reporting, scheduling and other types of products. Depending on their nature, they may bring data privacy compliance challenges that organisations have faced during the pandemic into even sharper focus. CIPL believes that the whole topic of processing personal data in the employment context will be brought into sharper focus in the future and may have to be reconsidered and redesigned in light of these experiences, particularly in jurisdictions in which employee data is covered by data protection law.

2. **Adapting to new and changing customer demands and behaviours**

Many organisations have had to **reimagine and even create new business processes, models and services** to continue to operate and to respond to the new COVID-19 reality, customer demands and behaviours. They have had to reinvent the manufacture and delivery of their services and products, their distribution and supply chains, and to seek new opportunities and partners. Most of these changes have been enabled by technology and data. For example, organisations have had to make use of, or provide, new data and technology and develop new services to survive during the pandemic; shift traditional brick-and-mortar establishments to online models (retail, cinemas, pharmacies and doctors, groceries, restaurants, gyms); substantially increase their online presence and further transform their digital capabilities; and refocus their priorities towards staying connected with customers and adding health and safety features in order to address the crisis.

For instance, Uber has developed services to deliver over-the-counter pharmaceuticals and to transport healthcare staff and patients. In the health sector, some patients now require remote healthcare and medicine because they either cannot or do not want to physically access it. These shifts have triggered new services, new relationships with practitioners and more convenient ways for patients to engage with the healthcare system. For pharma companies, for example, this has meant a completely different positioning vis-à-vis individuals, as they have historically been further removed from patients. Finally, in the future, numerous private and public organisations may also have to implement health monitoring and checks in their customer-, user- or patient-facing facilities, including retail shops, transport, hospitals, etc.

The crisis has significantly accelerated the digital transformation, online presence and capabilities of many businesses. With an explosion in demand for everything online – purchases, delivery services, video streaming, gaming products, spiritual content, health and wellbeing, and social interaction – existing businesses have grown and new ones have emerged. Many of these rely on personal data as they offer personalised services and/or are supported by advertising. Many businesses will see it as essential to preserve these business models so that the world can continue to benefit from them even beyond the crisis.

While COVID-19 represents opportunities for some industry sectors and larger organisations, many SMEs have been heavily impacted. There are concerns that many will be unable to resume their

businesses after the crisis. There may be loud calls from industry, politicians and policymakers for relaxing rules regarding data protection and access to data for SMEs (as well as for larger organisations) to enable them to help kick-start the digital economy in the post-COVID-19 world.

All these shifts and changes in customer behaviour and organisational models are likely to stay in the post-COVID-19 world. Organisations' and society's appetite for data-driven innovation and beneficial products, services and projects will only grow. The positive experiences of digitalisation and datafication will embolden even the most traditional and risk-adverse businesses. This permanent shift will raise central issues of data protection compliance (some old, but many new). Questions will be asked about how data protection requirements should be interpreted and adjusted to respond to these new behaviours, expectations and realities. Both organisations and DPAs will have to be ready to address and provide answers to these questions.

3. **Using data for good**

Organisations are working on building tools, apps and solutions using their expertise and AI capabilities to help address the COVID-19 crisis. Others have chosen to invest and participate in wider projects, offering some of their services to the public for free, or collaborating with public sector bodies and academic institutions on tools and technologies. Some organisations have even undertaken actions that are traditionally within the remit of public authorities, such as developing apps that use Bluetooth or location data to alert individuals of possible contamination. They will need to observe public authorities' guidelines such as the ones recently drafted by the European Commission concerning a toolkit for the development of mobile applications used to combat COVID-19.

The role of some organisations in society is therefore likely to evolve, especially for tech companies and platforms with network effect, as well as biotech, health and pharma companies. Society may expect them to continue these new projects after COVID-19, and these may even be required by law in some countries. This could trigger a redefinition of the notion of public services, and some private organisations may be considered essential to society, akin to public utilities or critical infrastructure. This may require new ways for organisations to manage their new responsibilities and expectations, as well as new ways for regulators and policymakers to perceive and engage with them. New private-public partnerships and joint activities might emerge, which will include business-to-government and government-to-business data sharing.

Data protection laws, principles and their interpretation will need to be flexible enough to adapt to these new forms of collaboration and "technology/data for good" initiatives, while ensuring trust and compliance of the entire ecosystem. Key requirements commonly present in data protection laws that will need such flexibility include:

a. **Vital interests and public interest as legal bases for processing** (or equivalent legal bases under applicable national laws and DPA interpretations). The COVID-19 crisis has brought the significance of these legal bases into focus as enablers of the use of personal data for social good. In the EU, the European Data Protection Board (EDPB) recently clarified that, under the GDPR, private entities involved in the fight against COVID-19 may rely on the "public interest" derogation for cross-border transfers of data used for research. Moving forward, organisations may rely more on the vital interest and public interest (or similar) legal bases, and may have to consider previously unforeseen data processing scenarios when deciding

what legal bases to rely upon. Of course, consent could also be considered as a legal basis for processing where it is practicable and effective in protecting individuals.

b. **Principles of data minimisation and not using data for incompatible purposes**. These principles are present in many data protection and privacy laws and may have to be recast and reinterpreted to enable beneficial uses of data for good and data processing that brings value to people and society. It will be important to create new protocols to allow for further processing of personal data, including sensitive data, in more instances than has been the case to date, especially in the fields of research, health and biotech. In many instances, these new uses may involve using anonymous or pseudonymous data, which will enable risks and harms to be mitigated appropriately. Such new protocols will also need to be created where personal data (as opposed to anonymous or pseudonymous data) has to be used, as the objectives of processing may not be able to be fulfilled by the use of anonymous data.

c. **Principles of accuracy, relevance and adequacy**. Data protection laws generally require that data be accurate, relevant and adequate to the stated purpose for which it was collected. These principles also apply in the context of data for good and data for the purpose of addressing the COVID-19 crisis. For example, the EU Commission and the European Data Protection Supervisor (EDPS) advised that tracing apps should be voluntary. However, there are concerns that not enough people will sign up to use such apps, which may result in inaccurate and biased results due to the insufficient amount of data collected. Ultimately, this may render the entirety of processing of the tracing app unfair under data protection laws for impacting people adversely, based on a decision made on incomplete, biased or otherwise compromised modelling. In other words, making such measures or apps voluntary (i.e. requiring consent) is directly relevant to the data's accuracy, relevancy and adequacy. Similarly, there are indications that businesses will require the use of tracing apps or spot tests in the workplace; that airlines, transport and airport-operating organisations will require immunity or other health checks; and that even visitors to public and private sector buildings will have to enter through the temperature check portals. There has to be a robust public debate, informed by privacy practitioners, experts and DPAs, to socialise the use of new apps and technologies and to build and implement them with accountability and privacy by design, particularly should they become mandatory. It is perfectly possible to have a fully privacy protective and compliant tracing app that is also mandatory, or a mandatory temperature check or facial recognition technology at airport check-in and security. Of course, this presupposes sound accountability frameworks and measures applicable to both the public and private sectors involved in such data processing.

4. **Sharing data to inform decisions**

The COVID-19 crisis is a "wake-up call" for how data can be used strategically to address health and economic crises at several levels. For instance, data held by the tech and telecom sectors can be helpful to track people's movements, predict the spread of the virus and anticipate public health needs. Data held by banks, payment processors or insurers can be helpful to make the most efficient decisions to rebuild the economy. However, as noted above, data sets used for some of these purposes must include data of a sufficient number of people to make it representative and reliable, to avoid biased or inaccurate results.

This crisis has seen an increase in demand for data sharing, and companies now have to respond to data-sharing requests from public authorities or academic institutions and researchers around the

world. There has also been an increase in public expectations that decisions made by public authorities are based on facts and data. In this context, organisations have faced technical challenges and have had to consider developing specific tools to enable such data sharing, which highlights the importance of interoperability.

Also, some organisations are proactively engaging in projects with other organisations and public bodies to develop solutions to address the COVID-19 crisis, which may require the sharing of data. Other organisations may choose to share data proactively with authorities or even make it publicly available on their websites, often anonymised or aggregated, to help understand patterns, predict trends or inform decisions – for instance, Google and Apple have published mobility reports based on aggregated data. Publicly available data held by governments and public bodies are being used for similar purposes – for instance, the IBM Weather Channel brings together trusted data from governments, the World Health Organization (WHO) and the US Centers for Disease Control and Prevention (CDC) to give more than 300 million monthly visitors access to detailed virus tracking.

Organisations still report reticence and caution when embarking on data-sharing projects, for fear of breaching applicable data protection laws or due to a lack of clarity on what regulators and the public may accept. Many report the need for a broader interpretation of data protection provisions that enable the use of personal data for statistical and research purposes. Some organisations are trying to create accountability frameworks for responsible data sharing, but all admit the need for a wider debate and alignment.

CIPL expects data sharing to increase and remain firmly on the agendas of many governments, policymakers and organisations after the COVID-19 crisis. Data sharing may be turned into a legal obligation for some "essential/critical data sets" – see for example the current EU data strategy. This will have consequences for data protection, business strategies, intellectual property, etc. Countries may also come up with national laws providing for specific safeguards and derogations concerning the use of personal data for research and statistical purposes as a way to enable speedier use of data to combat future crises.

Finally, there is a need for a bottom-up, clear and efficient data-sharing accountability framework to enable these practices and properly balance data protection principles and fundamental rights of individuals and society. In our above-mentioned article on COVID-19 and data privacy, CIPL has attempted to spark the debate by proposing the 12 accountability steps that organisations, governments and academic and research institutions can take to engage in responsible data sharing.

III. CONSIDERATIONS REGARDING THE ROLE OF DPAS IN A COVID-19 AND POST-COVID-19 WORLD

1. Smart regulators

All DPAs will have to **re-examine their role during and post COVID-19** to continue to be informed, relevant and in touch with technology developments, business trends and public opinion and expectations. In the short to medium term, this means re-prioritising strategies and activities to provide pragmatic, flexible, risk-based and outcomes-based support to regulated organisations. It also means being a strong yet realistic voice in national planning and debates about the tools and ways to fight the pandemic and enable the return to work and rebuilding of the economy. DPAs must define priorities for guidance to be provided, as well as review and prioritise their oversight and enforcement strategies and be transparent about how they will undertake and prioritise enforcement.

DPAs will also need to act in a collaborative and constructive manner with organisations and other regulators, governments and public authorities around the world. This includes engaging with the global DPA community through the Global Privacy Assembly (GPA) and aiming for globally harmonised or consistent positions. Striving for global convergence on how to effectively use and protect data in cross-border contexts is especially important in the face of the current trend towards de-globalisation and resurgence of state sovereignty, which may only escalate further as a result of the current pandemic. DPAs should push back against such fragmentation as much as possible and promote internationally accepted accountability-based solutions, championing both privacy and responsible use of data. Leveraging the concept of organisational accountability to its fullest extent will create the necessary preconditions for economic recovery and growth on national, regional and global levels, all of which depend on cross-border data flows and thus globally consistent data protection rules.

In short, DPAs have an important role to play in facilitating a shift in how we think about privacy and data protection principles and laws so that they do not unnecessarily inhibit important data uses for the social good and public welfare. This role includes raising awareness of any necessary changes for individuals and society at large with respect to how and for what purposes we use data and may also include advocating for changes in the law where necessary.

2. **Enabling trust of all stakeholders**

DPAs will play an important gatekeeper role to maintain and ensure individual trust in both private and public sector processing activities that have intensified or emerged. As seen above, the efficacy of technology and collaborative apps to help fight COVID-19 will depend on how many users are willing to download them and share their personal data. Therefore, data protection and digital trust will be key elements of the development process.

DPAs must insist that any stakeholder (including public authorities) involved in using technology and data to fight COVID-19 must be transparent about how the data will be used, for what purposes, with what safeguards and when it will be deleted. DPAs may also require completion and, in some instances, publication of DPIAs for large-scale data collection, use or sharing initiatives, with a high likelihood and severity of risks to individuals. Finally, DPAs should educate on and raise awareness of the difference between personal and non-personal data as well as acceptable data anonymisation and pseudonymisation techniques and standards.

3. **Promoting accountable data use and sharing**

DPAs should proactively call for, and encourage, both public and private sector organisations adopting accountability measures to enable responsible data use and sharing. They should work with stakeholders to define a clear accountability framework establishing responsibilities and roles for data sharing between and among private and public organisations – including business-to-business, business-to-government and government-to-business. Supporting responsible and trusted uses of personal data by private and public organisations will enable the sharing of data essential to address the crisis, as well as new growth opportunities and data-driven innovation in the post-COVID-19 world. This also includes addressing specific needs of SMEs and start-ups.

4. **Reframing key privacy concepts and updating traditional interpretations**

The COVID-19 crisis is a real-life case study for the application of many key provisions of global privacy laws. It highlights the need to further consider the balance between individual and collective interests

and the relationship between competing rights. Some of the more specific pressure points among the most common data protection requirements that should be tested and may need to be readjusted include:

a. **The role of risk assessments and consideration of real harm to individuals.** Risk assessments must include assessment of the benefits of processing and impact on other fundamental rights as well as of reticence risk (the lost opportunity or benefit due to not processing personal data). These should be balanced against the risks and harms to individuals. Risk assessments must also determine the severity and likelihood of harms to individuals from proposed processing, as opposed to looking at harms in a more abstract and theoretical way.

b. **Appropriate legal bases for processing beyond consent, including for sensitive personal data.** As mentioned above, it may be appropriate in certain circumstances to rely on other grounds for processing data, such as legitimate interest, public interest, vital interest or legal obligation of a controller. DPAs would have to support a broader and more innovative and flexible interpretation of these legal grounds than they have in the past.

c. **Concept of anonymous and pseudonymous data.** The notion of anonymous data must be preserved, otherwise all data processing will always be subject to the requirements of data protection laws, which is not sustainable in the long term and would stop many beneficial uses of anonymous and aggregate data. DPAs should promote best practices, risk mitigations and additional pragmatic safeguards for anonymisation, similar to those articulated by the US Federal Trade Commission, for instance. These should clearly establish when personal data can be considered anonymous data and therefore fall outside the scope of data protection laws.

d. **Data minimisation and compatible purposes.** There is a need for a broader interpretation of what constitutes a compatible (or not incompatible) purpose. Organisations should be able to use personal data for new and beneficial purposes even when such purposes are different from the original purpose for which the data was collected and were not envisaged at the time of collection – providing they adopt all the other accountability measures. Similarly, data minimisation should not be interpreted by default as "no personal data", or "delete all personal data", as some regulators and privacy practitioners have been doing in the past. Data minimisation is linked to proportionality. It must be seen as relative to what is necessary and relevant to the purpose at hand, including any new and not incompatible purpose.

e. **Scientific research exemption must be made more broadly available to private sector organisations.** DPAs should confirm that when data protection laws provide that scientific research is exempted from some of the data protection law requirements (such as Article 89 of the GDPR), this exemption extends to all organisations for data analytics, research and algorithmic training purposes.

5. **Adopting modern and agile regulatory responses**

COVID-19 has shown that crisis situations demand speedy and agile responses not only from organisations but also from DPAs. Many organisations have praised some DPAs' quick reaction, resources and materials, which provide guidance and key information for organisations – see for instance the Information Commissioner's Office's (UK ICO) Data Protection and Coronavirus Information Hub. Also, organisations appreciated some DPAs' transparency and decisiveness in publishing the adjusted regulatory and enforcement strategy and forbearance policy.

DPAs will need to develop strategies to react quickly to urgent situations, including prioritising their activities and adapting to fast-paced environments. This may also include issuing public assurances that some data processing practices in the COVID-19 context are considered acceptable if they meet certain principles and criteria (e.g. the CNIL practice of issuing "referentials" setting out a presumption of compliance of processing activities' meeting certain criteria). Such a development will likely also generate benefits for DPAs from a workload management perspective as DPAs can use lessons learned from COVID-19 to adapt their current ways of working to a more fast-paced external environment. For instance, DPAs may be expected to provide quicker responses to prior consultations, enabling rather than delaying the development of innovative products.

Also, the concept of a **"regulatory sandbox"** may prove to be a useful model to enable responsible innovation and regulatory feedback in a time of crisis. Data protection authorities that are currently using or are about to use regulatory sandboxes include the U.K. ICO, the Singapore PDPC, and the Norwegian Datatilsynet. With boosted staffing, resources and deadlines, a regulatory sandbox could be a perfect mechanism for developing and building trust in some of the high-impact complex projects such as tracing apps or future immunity passports.

Finally, there may be benefits to DPAs in encouraging further accountability, governance and oversight by internal and external data review boards, or similar advisory bodies. If appropriately set up (particularly for high-risk projects), they may provide an additional expert layer of advice and oversight over private and public sector organisations' data use and sharing. They would also reduce the regulatory burdens of DPAs by providing front-line review and "checks and balances" in the first instance.

6. **Re-focusing priorities**

As explained in Section I above, it is hard to argue with the benefits of technology and data in dealing with emergency situations. The taste of the benefits brought by data-driven innovation in all fields will remain with us beyond this crisis. We will see increased calls for leveraging the power of data and data sharing in all areas of business and government. Many of the services that have been considered essential during the crisis, and/or demanded by customers, were powered by data, provided for free, and often enabled by online advertising. It is safe to say that people – consumers, citizens, employees – will expect the same services in the post-COVID-19 world.

DPAs will need to **consider this new atmosphere post-COVID-19 and re-prioritise their actions, including enforcement actions,** accordingly. They should expressly acknowledge the benefits of data- and advertising-driven business models, but also demand that such business models operate on the basis of demonstrable accountability, and specifically call for and encourage such accountability. Modern privacy laws increasingly incorporate accountability as a requirement, but how this requirement can be effectively implemented through comprehensive privacy programmes is still subject to substantial uncertainty amongst organisations. Thus, there is significant scope for DPAs to improve privacy protections as well as facilitate beneficial uses of data by proactively demanding, explaining, encouraging and enforcing organisational accountability. Indeed, Commissioner Wilson of the U.S. Federal Trade Commission recently highlighted the particular relevance of accountability in designing privacy programs for technologies assisting in the fight against COVID-19.

DPAs will also have to be **judicious in choosing when to act and enforce the law.** Similar to post-9/11 times, the general public may now be more prepared to accept some justifiable limitations to privacy or incursions upon their freedom if their own safety or public health and welfare demand it. After all,

they have accepted severe limitations to the freedom of movement and association, so they may also be ready to accept justifiable and appropriate limitations to their data protection rights, providing the limitations are accompanied by accountability measures and controls. Similarly, the average individual may not be bothered by an organisation's technical breach of data privacy rules, or an unsolicited marketing email, or even incomplete cookie notices and their use to serve ads. The public may be more concerned, and would expect a DPA to act, if their health data are used in ways that result in unintended consequences or result in discrimination due to their health record or status. Indeed, some DPAs, such as the UK ICO, have already announced certain priority adjustments reflecting this mind set for the duration of the COVID-19 crisis to enable responsible data sharing for the public good. The need to adjust is also reflected in the European Data Protection Supervisor's (EDPS) recent decision to amend the EDPS's five-year strategy in response to the COVID-19 crisis, which he called a "game changer" in data protection.

Moving forward – and not just during the pandemic – all DPAs should consider such readjustment of priorities and also focus on further **exploring the real meaning of a risk-based approach to privacy and of implementing and demonstrating compliance with data protection laws through organisational accountability.** It is important that DPAs become more pragmatic and outcomes-based in a way that enables the flexibility necessary for technological innovation while promoting responsible data use.

Finally, it may be interesting for DPAs to have focus groups with individuals (similar to the past "citizens jury" exercise by the UK ICO or a privacy perception index) to test some of these hypotheses, shifts in perceptions and public acceptance of trade-offs between privacy and other rights and interest.

7. **Coordinating with other DPAs, regulators and international bodies**

A pandemic demands cross-jurisdictional and international coordination to fight it. However, while some DPAs have taken a pragmatic stance in enabling the use of personal data for good, other DPAs have not. For instance, some DPAs have taken conservative views on the use of employee personal data in the context of COVID-19. Some DPAs have even expressed doubt that anonymous data can ever be used and shared, as it always presents a risk of re-identification. Such inconsistent approaches between global DPAs cause tension, in particular for organisations that operate across multiple jurisdictions and countries and create uncertainties as to how data privacy laws apply to certain scenarios, such as contact tracing in cases involving multiple jurisdictions and the use of health data without explicit consent.

DPAs play a key role in providing pragmatic guidance that enables the use of personal data in a crisis while also protecting people and their data. As noted above, they should coordinate among themselves and with other sectoral regulators around the world (such as health, telecom and financial regulators), international bodies (such as the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation forum (APEC) and the WHO) and the GPA to ensure a coherent environment. Only such global coherence can truly enable all stakeholders, including private organisations, to seek common solutions to major problems such as the pandemic by leveraging the lessons learned from the COVID-19 experience. DPAs should also work together to take flexible and pragmatic approaches to regulation and enforcement and seek convergence in their approaches across different jurisdictions and countries. Indeed, there are positive examples of such global and multi-jurisdictional collaboration and coordination. The GPA has established a COVID-19

task force to advise its members (global DPAs) on best practices, provide insight and drive practical responses to the privacy issues associated with the COVID-19 pandemic. In Canada, DPAs have issued a Joint Statement by Federal, Provincial and Territorial Privacy Commissioners, setting forth common principles for the use of contact tracing and similar apps to complement and fill gaps in existing laws.

IV. OTHER CONSIDERATIONS FOR WIDER SOCIETAL IMPACTS OF COVID-19

1. Changes in individual perceptions of balancing fundamental rights

The COVID-19 crisis has made the societal value of data and personal data more evident and clearer to many people. Some individuals are starting to reconsider the weight that privacy and data protection should have compared to other human and fundamental rights. Some consider that the rights to life, freedom of movement, work and having a family life justify a reconfiguring of the balance between privacy and other rights. Others fear that, in the long term, any downgrading of privacy will remain after the crisis is over – often citing the 9/11 example. Finally, some individuals have "donated" and are sharing their personal data for the public good, either proactively or at the request of governments or academic and research institutions (although some have larger concerns about sharing data with governments than with the private sector).

The potential trade-offs between such competing rights and interests demonstrate that data protection cannot take place in a vacuum but must be considered in light of other important objectives such as maintaining or promoting social, political and economic wellbeing. However, regardless of where one draws the line, it is important and possible for individual privacy rights to be protected appropriately, even in crisis contexts, through accountable and responsible practices by private and public organisations, including public authorities and governments.

2. Social suspicion and surveillance by the community

COVID-19 has reinvigorated the sense of community and civic duty. People in general, and local communities especially, are now using communications technology – including social media, special apps and messaging services – to support each other and provide timely assistance. This has resulted in increased sharing of potentially sensitive data, which is likely to continue post COVID-19.

The other side of this coin is increased reporting (and even public shaming) by members of the community on their peers' alleged misbehaviours. Such reporting will often be made to, and may be encouraged by, government authorities, police and employers. As a result, these bodies will increasingly be processing personal data relating to COVID-19 and may seek DPAs' guidance, including on how to respond to society and to process personal data in this new scenario. The associated risks and potential challenges might be pre-empted, or their likelihood reduced, by education campaigns to the public as well as to public authorities and private organisations on data privacy risks and best practices.

3. Digital immunity cards and consequences

There is a possibility that, in many countries, individuals will be required to hold digital immunity cards to be able to re-engage in society. As mentioned above, a wide array of public and private sector organisations may be using and mandating some kind of immunity passport to allow physical access to premises, transport, services and other people. It is conceivable that this could even be expanded to other health conditions. Individuals may increasingly be granted or denied access to public

transportation, public or private places and even across borders on the basis of automated decisions. While this carries significant nefarious potential, well-designed accountability frameworks, with appropriate monitoring and oversight, may provide part of the answer and help enable the use of such tools for limited purposes and without negative impact to the legitimate countervailing rights of individuals.

4. **Data privacy safety net**

Many of the technologies developed and used in the context of COVID-19 are necessary and should be encouraged, provided that they are built and implemented with accountability and privacy by design. However, over time these tools lend themselves to misuse for inappropriate surveillance and other purposes. Therefore, there has to be a framework for ongoing review and oversight to ensure that these tools are being used for the appropriate purposes and that they are retired or adapted when no longer necessary. The DPOs of public and private organisations should be specifically tasked with such review and oversight. In some instances, internal or external data review boards will also have a role to play. Finally, DPAs must also have a central role in initiating public debate and review of such oversight frameworks, as well as enforcing applicable rules where appropriate. Where existing rules do not enable the creation or enforcement of such frameworks, stakeholders, including DPAs, should seek the appropriate legislative solutions.

If you would like to discuss any of the comments in this paper, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; and Nathalie Laneret, nlaneret@huntonAK.com.