DIFC

FORCE MAJEURE PRIVACY: INSIGHTS INTO THE IMPERATIVE FOR DATA PROTECTION LEGISLATION (AND FAQS)

Commissioner of Data Protection

With contributions from members of the

UAE / GCC Data Protection & Security Working Group

CONTENTS

Introduction

The Dubai International Financial Centre and/or its affiliates and entities (collectively "DIFC", "DIFCA") values individuals' security and privacy. DIFC has its own Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law"), and may for certain types of Personal Data processing also apply the laws from other jurisdictions.

The defined terms used herein have the same meaning as the defined terms in the DP Law.

If you require further information or clarification about anything provided in this guidance document or any other guidance referenced herein, please contact the DIFC Commissioner of Data Protection (the **Commissioner**) either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office. Also, you may wish to refer to the DIFC Online Data Protection Policy.

Scope

Due to DIFC's historical reliance on UK and EU data protection and privacy principles and the interpretation thereof by the UK authorities, from a common law perspective, this guidance should be read in conjunction with those existing UK and EU laws and guidance on the same topic, with which the DP Law is also aligned.

Please note that ***this guidance expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice****. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm.*

Purpose

During the first pandemic in over two generations, the work has been turned upside-down. Rights of all kinds have been tested as all kinds of decisions have to be made by governments, employees / employers, educators, retailers, and yes, families at a breakneck pace to keep up with the increasing pandemic numbers we as a global community face regarding coronavirus. There are certain rights and decisions that underpin all of these areas of concern, but specifically none more so than those regarding personal data and security.

International data protection standards and principles have perhaps never been under more stress-testing than in coping with COVID-19. Government-shared *personal data*, Employee / employer *personal data*, educational *personal data*, retail *personal data* and yes, individual / family *personal data* are at the crux of each aspect of this new world order. Bear in mind, above all, ***health*** related personal data is special category data by any measure in data privacy laws.

Jurisdictions with data protection laws and the regulators administering them are up against the proverbial wall even with the most sound data privacy law to enforce.

Standard data sharing, data transfers, notification and any other processing and compliance practices should in theory remain in place even where such practices are conducted at a feverish pace (no pun intended). Especially because times now are challenging and quick judgements often need to be made, regulators should take a moment to review any sharing or transfer requests they are making to ensure they are compliant with the very principles their national (or jurisdictional) data protection laws mandate. More on the data sharing point to come.

Likewise data controllers or processors should take a moment to review requests made to them or within their own business or practice, and for the sake of transparency must be sure to document what actions are taken, and assess the risk – heightened risk perhaps - as the current environment dictates. Accountability – rather than panic processing - is absolutely critical to protect both individuals and the regulators protecting them.

Senior management, crisis response teams, IT / Security teams, customers / clients or colleagues must assess whether what appears to be a non-DP matter to ensure they are engaging in the data protection part of the conversation, even if to rule it out.

Flexibility and sensible, risk-based evaluations are key at this time, in every single decision being made about data collection and exchange. The regulators in jurisdictions with data protection laws (i.e., the DIFC and ADGM here in the UAE) should take this same approach when reviewing issues of possible non-compliance.

However, only a portion of the world's governments, and therefore the people subject to their governance, have data protection regimes. Some major geographic jurisdictions and their economies, where sheer numbers of individuals – as well as controllers or processors – reside have no national privacy laws at all. The absence of data protection laws should not however mean that governments, ministries, and organisations in these jurisdictions simply do not take

privacy measures into account when dealing with COVID-19. More than ever, data controllers and processors in these extraordinary times must ensure the protection of personal data of individuals, regardless of the existence of a local data protection law or not.

As such, the present paper seeks to guide and lay down some best practices for relevant stakeholders like the senior management/ executive leadership, crisis response teams, in-house counsels, IT / Security teams, customers / clients or colleagues.

Pandemic without Privacy

It is easy to list the benefits of promulgating a national data protection law. Transparency and accountability to the data subjects governed by a government is but one. Transparency and accountability necessitates analysis and documentation. The clear payoff of such regimes go both ways – data subjects are protected almost as considerably as the government itself, which will be able to demonstrate decision making, consideration of risks and a well-reasoned conclusion on which to base such critical decisions. Imagine if a highly security-based, punitive data protection law was in place. The government itself and those who administer the law on its behalf would be at risk of violating the law and therefore facing criminal penalties in doing so. A principles-based law driven by risk-tolerance changes the game and is much more reasonable an approach to sharing such highly contentious data as is required to be shared now.

That being said, it is also a time to reflect on what a legislative and administrative landscape looks like without a privacy law in place at all. For starters, individuals' rights are at risk and the soundness of the government mandate to protect people diminishes considerably. As set out earlier, protection of personal data that must be shared exists in every scenario we face at this time - to order groceries, or login for online learning, or provide information to employers about exposure to a highly contagious disease, or to obtain (or share) information about a loved one sick and dying in hospital. Without a solid, industry-agnostic privacy law cutting across industry-specific laws that support each facet of life as we now know it, the very substance of transparency and honesty, integral for a fully functioning society, is at risk. One risk is simply exchanged for another.

For example if information gets out from an employer that does not have solid privacy policies in place and it appears that an individual has coronavirus, others around this person may act differently towards them, even discriminatorily or aggressively, without justification and worse, without recourse – judicial or otherwise. This is but one scenario where the lack of a data protection law and the accountability such laws require ends in harm to the individual.

Another example, which several governments are considering, or have in fact implemented is the use of mobile applications that allow limited movement tracking and analyse whether a user has been in close proximity to another person who has been tested, or will be within a certain timeframe after contact, test positive for COVID-19. It is clear that the buy-in of the population to use the application can be expected to be higher where the individuals feel that the relevant app is set-up in a way that protects rights to own data. Only where individuals feel in control of what

data is collected, when is it collected, who can get access to it, or how will be used there is a possibility for such application to be a successful measure in helping regulators combat the pandemic. Best case scenario, there is a privacy law in place and individuals have some say in the matter of their personal data management to govern such new found uses.

Where there is not a privacy law, however, even a trustworthy, decisive government is not enough. For instance, where no agreed data protection laws and regulations exist yet for rapidly emerging technology like AI – especially where it is used for Covid surveillance - ethics and integrity are time-honored values but they are also subjective and potentially not on everyone's agenda. People, especially the most vulnerable in such situations, need to be able to have at least some form of redress provided for in a basic law, especially where "choice" about collecting or using such data is less of an option. The less choice people have with how their data is used during a crisis, the more redress and controls should be required. What governments without a privacy law may consider is that with or without a law, the app is just as effective and even necessary, people still benefit from it, public interests are served – but one piece is missing, and that is protection in the form of liability protection should anything go wrong. A well-formed privacy law and policy is again key to supporting such efforts.

This raises the further question of sharing that personal data collected in whatever format, whether through employer / employee relationship as the workforce slowly goes back to the office, or through contract tracing apps. Regulators will often agree to share with each other data that aids in the fight against something – terrorism, bribery and fraud, and now, even deadly diseases[1]. The data that is most valuable, and at times the only data shared, is personal data. Looking ahead to when airline travel resumes to a more usual condition, or when ex-pats seek to live in a new country where medical exams are required, or other personal data is needed for any number of other legitimate reasons, cross-border personal data sharing will be – using that word again – critical to supporting such vast and varied public interests, both social and economic.

Let us remind ourselves that a data protection law written with built in flexibility by way of accountability principles and risk-based self-assessment does not hamper the very necessary sharing of critical data that supports the public interest, be it health-related or otherwise. It will indeed ***allow*** governments to make the decisions they need to make in the interests of its citizens and residents while at the same time providing individuals with adequate protection against privacy threats of all kinds.

To reconcile public safety, on the one hand, and the right to privacy and data protection, on the other hand, it is important that governments embed necessity and proportionality in their decisions and the measures they take. Such situations where two fundamental rights are in direct conflict are not new or uncommon but handling them appropriately is crucial for preserving individuals' legitimate expectations.

European law provides a well-established method of dealing with such conflicts by applying the so-called proportionality and necessity test. Using this method can provide jurisdictions with less

[1] Imagine a PNR-type directive for Covid-19 data sharing, or for sharing health data for pioneering health research, or even for terrorism (biological) prevention. This is however a paper for another time.

developed practice and jurisprudence in the area with a sensible approach to appropriately handle, decide and justify possible limitations to privacy.

The right to privacy is generally not an absolute right and in exceptional cases such as the current pandemic, limitations can apply provided that those are justified. To assess to what extent potential limitations to privacy can be justified, legislators should consider conducting a proportionality and necessity test beforehand. This implies a step-by-step assessment of the measures likely to limit the right to privacy and data protection. What first needs to be established is whether the measure is strictly necessary for achieving the specific objective of general interest. If the measure is deemed to be necessary, then it needs to be assessed in terms of its proportionality which would involve evaluating what safeguards should accompany the measure to limit the risk to the right to privacy. The assessment is usually conducted "fact-based" and on a case-by-case basis. The end goal of this test is to balance the intensity of the interference against the importance of the objective pursued. Hence, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes to the right to privacy.

More than ever, governments without a national privacy law that incorporates common international standards, such as the US, many countries in the Middle East and Africa, and certain outliers in Asia, should, even in a time of crisis, in fact speed up the promulgation of privacy laws and indeed bring it forward to the front of the legislative queue.

These are extraordinary times. There is of course an argument for pausing the implementation of data protection laws and regulations to help businesses already under significant compliance-related strain. The flip side is that it is imperative to think about the impact on the data subjects themselves, and to consider customers or businesses and economy, and with those things in mind, consider also the work and jobs that would make the UAE an even more attractive place to be. Take for example the National Plan for UAE Smart Government Goals, UAE Vision 2021 and even the goals of Expo 2020. Socio-economic development of the UAE, world-class healthcare, education, a sustainable environment and infrastructure, competitive knowledge economy will all be driven by data exchange, but importantly, digital trust and transparency. For the UAE to develop as a digital hub, the tourism, continued investment in property, even a notion of healthcare tourism, where the aim is to attract foreign investment by multinational companies, will require the creation of an environment where people feel their privacy is respected, founded on transparency, accountability, and so on. Make the UAE/GCC attractive to investors and differentiate it against competition through privacy and security forward thinking.

Bear in mind as well that businesses need in this day and age to earn and preserve trust. They need help with a framework to develop programs for compliance that make it relatively easy to achieve, and such a law would assist in this regard. Consistency with existing international laws levels the playing field, otherwise businesses will find it difficult to compete not only locally but globally as well. Note: It only takes one or two major breach incidents which are then poorly handled (not prepared, no notification, lack of transparency) to massively impact the reputation of the UAE, and the businesses in this jurisdiction. With the unplanned move to remote working the risk of cyberattacks of any kind has never been higher. Now is the time to help businesses prepare for such an event. Big companies in the UAE are ready, arguably. Global entities are subject to certain international data protection laws, but there is a significant missing link even for them where no such law exists locally. Especially during Covid-19 or other emergencies (and

there will be more), having that assurance of a framework, instructions, a guidebook for supporting a businesses, employees and yes, the government, through key data sharing considerations for all the reasons listed about is of vital importance.

The cost of compliance should be outweighed by the benefits of a well-founded national privacy law that indeed enables it.

COVID-19 has affected every inch of the globe and with that brought up many privacy issues to the forefront of our minds. Set out below are issues to think about and how they should be addressed.

FAQs About Privacy and COVID-19

Can Healthcare institutions and providers send communications to individuals?

Data protection and electronic communication laws both across the Middle East and globally, do not generally prohibit government agencies or healthcare institutions and providers from sending public health announcements to individuals. These may be sent via phone, text or email and do not constitute direct marketing as long as they do not include any promotion or marketing for products and services.

Public bodies can also require the additional collection and sharing of personal data to protect against serious threats to public health.

Telling staff about COVID cases/ Can an Employer inform employees that a member of their team has contracted COVID-19?

Organisations have an obligation to ensure the health and safety of employees and should therefore inform staff about COVID-19 cases and take the relevant protective measures. However, organisations should not provide staff with any more information than is necessary. This is in line with the core data protection principles of proportionality and data minimisation.

In the case of suspected or confirmed cases of COVID-19 within the organisation, the individuals in question should not be named and organisations should only provide the information that is strictly necessary. For example, disclosing the fact that somebody within the organisation has, or is likely to have, the virus, but go no further than this.

Consider taking steps now to notify staff of how their personal information will be handled in responding to any potential or confirmed case of COVID-19 in the workplace.

Can we ask about any symptoms of an employee's household?

In principle yes, but DPA's (across the globe) have stressed the importance of data minimisation when requesting additional health data from their employee.[2] In addition, once the data is collected, employers still have to ensure that it is treated with the appropriate safeguards, as

[2] The Global Privacy Assembly has collated the guidance of several its members (privacy regulators worldwide). The ICO in the UK has also provided guidance, which the DIFC DP Commissioner's Office endorses.

specified under any applicable data protection regulations (if such exist). Personal information should be used or disclosed on a 'need-to-know' basis.

As an employer, am I allowed to perform medical check-ups on employees or require employees to get checked?

This would primarily be dependent on existing laws relating to employment or health and safety. However, it is advised that employers should only access and process health data if their own legal obligations require so.

As part of COVID-19 prevention efforts, am I allowed to request from my commercial partners to share personal data relating to their employees' health?

Asking to receive personal data on contractors and vendors' employees may pose additional privacy risks. Organisations should consider having the adequate controls in place to protect the exchange of sensitive data with third parties, including contractual and cross-border transfer measures, while respecting key privacy principles such as proportionality and data minimisation.

Can I collect health data in relation to COVID-19 about employees or from visitors to my organisation? What about health information ahead of a conference, or an event?

The core data protection principles of proportionality and data minimisation, both of which are found in many data protection laws, are of particular importance here. Only the minimum amount of personal information reasonably necessary to prevent or manage COVID-19 should be collected, used or disclosed.

Employers have a duty to ensure employees' health and safety, but they should not gather unnecessary information about their employees. For example, it may be reasonable in the current circumstances to ask an employee or a visitor if they have visited a particular country or are experiencing any COVID-19 symptoms. On the other hand, it would be unreasonable to ask an employee or visitor if they or any of their family members have ever been diagnosed with any other contagious disease.

If additional health data is required, employers must ensure that they do not collect any more Personal Data or Sensitive Personal Data than is necessary (note: Sensitive Personal Data includes health information). In addition, employers must ensure that any Personal Data or Sensitive Personal Data that is collected is treated with appropriate safeguards, as specified in the relevant data protection law or regulation.

It would be appropriate to ask people who may be coming for a meeting or conference that if they are currently experiencing any of the COVID-19 symptoms that they should not attend in this instance.

Organisations should review existing privacy notices to ensure that these provide the necessary information regarding the data being collected and the purposes of processing.

Can I share employees' health information to authorities for public health purposes?

An employer is unlikely to have to share an individual's health information with the Health Authorities. However, if this does happen, data privacy regulations generally do not prevent employers from sharing such information, provided there is a legal basis for the processing of the Personal or Sensitive Personal Data and appropriate safeguards have been met. In first instance organisations should however try and share this information in an anonymized and aggregated way, thus removing any concerns around data privacy.

Working from home

As a result of the pandemic, many governments and organisations are now asking employees to work from home. For some, this may have already been the norm, but others may not be as prepared. The sudden shift to remote working has left organizations acting quickly, and in this rush, safeguards and controls may be overlooked or missed, presenting unexpected challenges particularly in relation to data privacy and security.

In an office environment, networks and devices are thoroughly protected and monitored. However, the configurations and set-up at home may not be in line with the organisation's standards, therefore presenting a higher risk.

For some this may be the norm, but for others this will be the first time and may present some unexpected challenges, particularly in relation to data protection.

We have outlined some of the most important data privacy and security considerations practices for organisations and employees to consider when working from home below.

Key considerations for organisations:

1. Establishing an effective foundation:
    - Establish remote working guidelines and include privacy and security into crisis management procedures. The remote working guidelines should clearly define what employees needs to do and what you expect of them when working remotely including access security practices, approved messaging applications, and other essential guidelines.
    - Perform critical analysis of business continuity plans for weaknesses and unidentified impacts specific to COVID-19 (supply chain, staff availability, customer demand etc.). This could include simulation of various contingency scenarios to 'stress test' continuity plans and assess impact on associated data privacy processes and controls.
    - Have a proper disaster recovery plan outlining the process to backup all valuable company data, and make sure the process is tested to be ready to recover from any potential attack.
      For incident monitoring and response, ensure that ongoing governance arrangements remain in place with appropriate investigation and action performed as issues are identified.

2. Protecting devices:
    - Communicate access and security guidelines to all employees. Access to company-sensitive data must be adequately restricted on a need to know basis only.

- Restrict the access to company-issued devices only, or alternatively establish guidelines for securely accessing the company's network through personal devices.
- To reduce the potential impact of unauthorized attacks, consider having your remote workforce use a virtual private network (VPN) and implementing multi-factor authentication on critical systems.
- Ensure that data is adequately backed up and capable of recovery and reconstitution, particularly essential data.
- Apply the necessary patches and system updates regularly and perform security monitoring to identify any suspicious patterns.
  Ensure that vendors and contractors are contractually obligated to follow the same security standards as full-time employees.

3. Security attacks and awareness:
   There has been an increase in phishing attacks in light of the coronavirus pandemic, as employees are not on the organization's network and the organization is not fully in control of their devices. Therefore:
   - Employees should be reminded and tested on phishing attacks, and receive regular reminders on what to look out for and who to contact in the event of a suspected attack.
   - Internet-facing and remote access systems of an organisation should have the latest critical patches applied and the configurations secured. They should constantly assess and monitor the critical systems landscapes for any vulnerabilities or misconfigurations by frequently conducting vulnerability scans and penetration testing.
   - Consistently communicate with your employees through various channels and keep them informed on the latest privacy and security threats and how to reduce their risk to their personal or company confidential information.
   - Log identified malicious attempts and follow your security monitoring and reporting mechanisms.

Key considerations for employees:

1. Securing access:
   - Only use company-issued devices to connect to the organisation's network remotely. If your organization allows use of personal devices for work, make sure your follow the remote working guidelines to apply the necessary updates and configurations.
   - Make sure devices are stored in a safe location when not in use and always lock your workstations if working in a shared environment.
   - Use work email accounts not personal accounts for all work-related emails that contain personal information.
   - Be careful when sharing data and only use company-approved application for file sharing and storage.
   - Restrict using your home or other secure networks only – public networks in restaurants and café are not as secure.
   - Change your router's default login and password, as these are widely known and used by attackers to gain access.
     If you are working from home without cloud or network access, ensure any locally stored data is adequately and periodically backed up in a secure manner.

2. Securing physical files:
   Data protection and information security laws also apply to data that is in the form of hard copies, such as paper records. Physical files should be:
   - Securely put away when not in use, for example in a locked filing cabinet or drawer.
   - Disposed of securely when no longer required, for example by shredding them.
     Care should be taken to ensure hard copies are not left somewhere where they could be misplaced or stolen.

3. Be aware of security attacks:
   Security attacks and breaches are on the rise. You should be vigilant when responding or opening emails and documents online. The EU Agency for Cybersecurity recommends being especially suspicious of the following:
   - Emails from people you don't know- especially if they ask to connect to links or open files.
   - Emails that create an image of urgency or severe consequences. These are key candidates for phishing and in these cases you should always verify via an external channel before complying.
   - Emails sent from people you know, but asking for unusual things.

   If you suspect that you've received a phishing email, directly report it to the IT security team.

Video Conferencing

The coronavirus crisis has hugely increased the amount and frequency of organisations and individuals using video conferencing services to connect with colleagues and clients remotely. It is important that people are aware of the data privacy considerations of using such services, both from a personal and organisational point of view.

- When not in use, keep your mic and webcam turned off.
- When participating in a video conference, if you have windows open containing information that you do not plan to share, make sure they are all properly closed before you begin conferencing.
- Do not record video conferences without obtaining the other attendees' consent, be it as best practice or to comply with local requirements on call recordings.
- Make sure you are using company approved tools.

Third party

- Re-evaluate third party service line agreements to include or amend new ways of conducting business through digital channels and existing contingencies to cover data privacy requirements.
- Assess data privacy risks associated with outsourced arrangements and the robustness of third-party controls. Where organisations are significantly dependent on third parties to process large amounts of personal and sensitive data, consider a 'fit-for-purpose'

assurance program over key risks and controls associated with the delivery of services by a third party.

Role of the authorities/ data protection regulators during and post the pandemic

Data protection law is never a barrier to sharing data where it's necessary and proportionate. While data controllers and processors are being put in hot waters during the COVID-19 situation, the authorities at the helm of affairs and wherever present, the data protection regulators (DIFC and ADGM) are also faced with the task of handing out real-time guidance and advice. It is expected that the approach of the relevant authorities / regulators will remain a pragmatic and proportionate one – but the key is that this is the case with or without a pandemic, and with or without a privacy law. In the UAE for example, the TRA, Central Bank, relevant municipality leadership teams and so on, despite having no national privacy law, have all had to be flexible and agile, considering people's rights through all of this (but without the protection that a law based on accountability will provide). Accordingly, all authorities, whether data protection regulators or not, must lead the way and-

- continue to recognise the rights and protections granted to people by the law, both around their personal information and their right to freedom of information.
- focus their efforts on the most serious challenges and greatest threats to the public.
- assist frontline organisations in providing advice and guidance on handling personal data.
- take firm action against those looking to exploit the public health emergency through nuisance calls or by misusing personal information.
- be flexible in their approach, taking into account the impact of the potential economic or resource burden our actions could place on organisations.
- be ready to provide maximum support for business and public authorities as they recover from the public health emergency.

Preparing for post pandemic normalcy

To provide a definitive perspective to the situational recommendations discussed in the preceding paragraphs, it is imperative that the key actors- data controllers and processors – align themselves with the following data privacy principles, whether required by law or not, in the current times to prepare for when the pandemic subsides:

<u>Lawful Processing</u>

In order to ascertain whether you / your company should be handling personal data, think about whether it falls into one of the legitimate processing categories, most relevant likely to be:

- Would the person expect me to use their information in this way (*legitimate interests*)?
- Have they given me their clear and unambiguous consent to use their personal information (*consent*)?

- Is there a clear legal obligation requiring that personal data is shared for the purposes of health security, public interest and similar reasons. (*legal obligations*)
- Is the person's health or safety at risk if I don't use their personal data (*vital interests*)?

If the answer is yes to any of these questions, then you can handle and share personal data.

Adherence to core principles relating while processing personal data

- *Transparency and accountability*- In addition, individuals should receive transparent information on the processing activities that are being carried out and their main features, including the retention period for collected data and the purposes of the processing. The information provided should be easily accessible and provided in clear and plain language.
- *Data minimization and purpose limitation*- Only such personal data that is necessary to attain the objectives pursued should be processed or kept for specified and explicit purposes. When the emergency is over and normalcy is restored, make sure to securely delete or destroy any personal information that is no longer need.
- *Proportionality*-The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved and the solutions must be in proportion to the purpose.

Ensure appropriate safeguards are in place

It is important to adopt adequate security measures and confidentiality policies ensuring that personal data is not disclosed to unauthorised parties. However, in such extraordinary times, it is understood that security measures need not be so onerous as to prevent you carrying out your work.

Keep a record of what you've done

As a company, either in the capacity of a data controller or a data processor, you should keep a record of any decisions you make that involve the use of personal information. Measures implemented to manage the current emergency and the underlying decision-making process should be appropriately documented. Ideally, this should be done even prior to collection of information. Although it is understandable that it might not be possible during the pandemic, it will however be helpful if you keep notes of what you've done and why and subsequently make more detailed records as soon as possible.

While in certain jurisdictions there may be no national or applicable law that posits data protection principles, provisions or measures, it is upon ourselves to observe the basic tenets regardless and ensure continued provision of basic minimum rights which must be ensured to all individuals at all times.

Conclusions and Parting Thoughts:

The emergency situation created by COVID-19 has necessitated the implementation of exceptional measures such as contact tracing to protect the public interest and safety. We exposed why such measures can raise significant risks for individuals and their right to privacy.

As elaborated in the sections above, failing to attribute to privacy and data protection the necessary weight, even in emergencies such as COVID -19, could raise important societal, political and economic risks such as *discrimination, defamation,* and a *lack of confidence in the government.*

Consequently, it is of utmost importance that governments and organisations ensure that they strike the right balance between protecting the public interest and avoiding unjustified restrictions to the right to privacy.

The key privacy challenges that COVID-19 raises are:

- **Sharing sensitive data** (e.g., COVID-19 infected) within and outside organisations
- **Using applications which track the COVID-19** spread
- Handling the **increased risk of fraud and data breaches** (e.g., phishing attacks)
- **Transferring internationally health data for clinical trials**

Taking stock of jurisdictions with an established privacy culture and an advanced regulatory framework in data protection such as the EU and the UK, we note that applying a **risk-based approach** is key in handling such challenges.

Considering the privacy-related guidance on COVID-19 released by the ICO (UK Information Commissioner Officer), EDPB (European Data Protection Board) and the EU Commission, below is a summary of the main recommendations on how to address the current challenges:

- **Enabling responsible data sharing**: ensuring that data shared in the fight of COVID-19 is shared in a responsible manner and genuinely for the public interest. This means providing for precise purposes for processing and legal basis. It should be no doubt on why and what data is necessary for the desired objective.

- **Monitoring the use of privacy-intrusive and disruptive technology**: using technology and digital innovation to fight COVID-19 is key but it has to be done in a way which avoids unjustified and disproportionate surveillance. Given the sensitivity of the data collected through such apps, to convince individuals to use them, it would be necessary to establish trust, by ensuring that individuals **remain in control of their data**.

- **Enabling a high degree of Transparency**: keeping the confidence of citizens in a state of emergency is of utmost importance and can be achieved only through a high level of transparency. Therefore, informing the citizens on why certain measures such as contact tracing are taken, how they can affect their rights, as well as the risks arising from a failure to implement those should be a top priority for public institutions and organisations.
- **Ensure appropriate international transfers safeguards**: developing an effective vaccine requires the processing of health data for scientific research and clinical trials. Given the global aspect of COVID-19, developing such a vaccine would probably necessitate international cooperation and hence, transferring sensitive data cross-border. Considering the sensitivity of such data, it is key that the organisations sharing the data (data exporter) ensure that appropriate data protection safeguards are put in place.

Whether governments, public institutions or private organisations, the most important concept to keep in mind while taking decisions in the context of COVID-19 that might affect privacy is to apply a **risk-based and proportionality approach** with a view to strike a **fair balance** between all interests concerned.