

Hogan
Lovells

Privacy 2040

COVID-19 Exit Strategy A Global Privacy and Cybersecurity Guide

May 2020







Contents

Embed privacy. Apply cybersecurity. Save lives	5
Regulatory privacy guidance for a pandemic – The story so far	6
Legal bases for processing COVID-19 data	9
Employers' transparency requirements when collecting COVID-19 data	13
Temperature screening privacy implications	17
Using immunity certificates and data protection	21
Making COVID-19 contact tracing apps privacy compliant	25
Vendors and contractual implications of a COVID-19 exit strategy	29
The role of Data Protection Officers (“DPOs”) and Data Protection Impact Assessments (“DPIAs”) in the context of COVID-19 measures	33
Cybersecurity precautions for an agile workforce	37
Getting cloud projects right in times of COVID-19	41
Direct marketing communications in times of coronavirus	45
Mitigating investigation and litigation risks	49
Key privacy considerations for COVID-19 clinical trials	53
Privacy lessons from Asia	57
About us	61
Our global team	62
COVID-19 resources	64



Embed privacy. Apply cybersecurity. Save lives

Eduardo Ustaran

The world is on a mission: beating the coronavirus and making normal life safe again. This is a scientific and medical challenge like no other, but our collective hope is that a viable solution will be found. In parallel, organizations and governments throughout the world are also facing a leadership and management challenge: finding a way to function as a society without putting lives at risk. In response to this, a variety of measures such as COVID-19 testing, temperature screening, immunity certificates, and contact tracing apps have become crucial elements of a fast-moving strategy proving once again that data is today's most valuable asset.

The deployment of these measures highlights a potential trade-off between public health and privacy. Should we be prepared to sacrifice some of our privacy for the sake of saving lives, possibly including our own? Or is this a zero-sum choice that gets in the way of finding a reliable way forward? Public health and privacy are not in conflict. They are on the same side. Collecting and using data responsibly has never been more important. A workable strategy to ease off the world's lockdown and keep the coronavirus under control demands respect for people's rights and their trust. So by embedding data protection practices in the very measures that may threaten our privacy, we can contribute to ensure that those measures are truly effective.

This guide is aimed at serving that purpose. Our objective is to help and show how privacy and cybersecurity can be part of the solution to this crisis. Our approach is robust but pragmatic. Our analysis is based on our global understanding of the law and its operation in the real world. With that in mind, this guide is the result of the enthusiasm and constructive thinking of our global practice and, above all, a real team effort.

Privacy and cybersecurity need not be victims of COVID-19. Like the precious data on which we all rely to succeed, they should be strong allies to overcome one of the greatest challenges of our time.

Regulatory privacy guidance for a pandemic – The story so far

Julian Flamant

The COVID-19 health crisis has created operational and legal challenges for public and private organizations everywhere. It has become clear that personal data will play a significant role in containing the spread of the novel coronavirus. As the pandemic has unfolded, it has been questioned whether Europe's data protection rules, considered among the world's most restrictive, would impede remediation measures. But as European data protection authorities (DPAs) have released guidance outlining lawful approaches for data processing to fight the COVID-19 health crisis, it has become apparent that data protection in this context is not an impediment to resolving the crisis as long as it is correctly understood and applied.

Many other countries with national data protection regimes have taken similar pragmatic approaches. In the United States, which lacks a generally-applicable national privacy law, organizations have had to take measures to protect their workplaces while still balancing privacy interests that arise under an array of local, state and federal employment and sectoral laws.

Given the concern of multinational organizations about the impact of data protection law in Europe, to help track DPA approaches to processing data in the fight against the COVID-19 health crisis, the Hogan Lovells Privacy and Cybersecurity team has compiled summaries of the guidelines released by regulators in Europe. The compilation contains summaries of the approaches adopted by over 30 regulators.

DPA approaches to processing have continued to develop as the crisis has deepened and the need to find solutions for lawful processing of personal data – including more sensitive data concerning health – has intensified. Unsurprisingly, early guidelines published by DPAs focused on collection and dissemination of personal data by employers to help identify infected individuals and protect others in the workplace. These early approaches have been among the most restrictive in applying the GDPR framework for data processing.

Early on, the DPAs in Belgium, France, Italy, Luxemburg and the Netherlands adopted the most restrictive approaches to processing personal data to fight the COVID-19 health crisis. Each of these regulators outlined lawful bases for processing employee data but articulated strict limits on the contours of those lawful bases (e.g. prohibiting compulsory use of questionnaires related to employee health or travel).

These early efforts to outline permissible data processing approaches also highlighted how governments may still be willing to accept solutions that allow for more data processing in the context of the crisis. In Italy, guidelines released by the DPA instructing employers not to collect information about COVID-19 symptoms or employee location were quickly superseded by a joint protocol negotiated between the Italian Government, trade unions, and Italian company representatives. The Protocol was explicitly aimed at reducing the spread of coronavirus at the workplace and it allows the collection and processing of employee and visitor personal data (including temperature screening).

Other European regulators have adopted a neutral approach or permissive approach to data processing activities. A neutral approach, such as the one adopted in Austria, Finland, Germany, Greece and Switzerland, is one that may allow processing of health data pursuant to various lawful bases for processing but places strict parameters around these justifications and may still require that processing is based on the data subject's consent. A more permissive approach, such as the one adopted in Ireland, Russia, Spain and the United Kingdom, is more encouraging of health data processing in this context and allows for more flexible methodologies to satisfy GDPR processing requirements.



Under all approaches, the DPAs have consistently highlighted that fundamental GDPR principles related to processing personal data remain a top consideration.

Ultimately, a pragmatic but coherent stance has taken shape across Europe and most of the world. This pragmatic approach is best illustrated by the positions of the Global Privacy Assembly, the European Data Protection Board (EDPB), and European Data Protection Supervisor. The message is simple: data protection does not stand in the way of using personal data to fight the COVID-19 health crisis, but fundamental data protection principles also cannot be ignored. Under this approach, organizations in Europe can find bases for processing personal data, including health data, without the need to obtain consent from the data subject. The EDPB has even explicitly outlined the means for processing health data regarding public interest particularly in the area of public health, scientific research, or statistical purposes.

Organizations in the United States generally do not need a “legal basis” to process personal data as part of a COVID-19 response strategy. However, adhering to employment and sectoral requirements where applicable, and abiding by generally recognized fair information practice principles (FIPPs) including notice,

data minimization, purpose limitation and in some cases choice, are prudent strategies to minimize legal liability both from government and private plaintiff actions.

The new frontier of personal data processing in the context of the COVID-19 health crisis is the use of contact tracing technologies to help contain further spread of the virus. Contact tracing offers a particular challenge because it requires large-scale processing of personal data related to individuals’ locations to be effective. In Europe, however, the EDPB has noted that though adoption of contract tracing technologies requires voluntary adoption by users, the processing in this context need not be based on consent. Instead, the EDPB has advocated implementing core GDPR data processing principles, such as purpose limitation, data minimization and storage limitation as the most effective measures to help reduce privacy risks. In the United States, some employers are using contact tracing technologies not based on location and designed to minimize privacy concerns. This is another area where whatever technologies are utilized, following the FIPPs is a prudent strategy.

Elizabeth Champion, a Knowledge Paralegal in our London office, and Brittney Griffin, a Paralegal in our Washington, D.C. office, contributed to this chapter.

A person wearing a white protective suit, a white hairnet, a white face mask, and glasses is holding a green spiky ball. The background is blurred, showing what appears to be a laboratory or industrial setting with blue and yellow elements.

Quick read

The response to COVID-19 will involve the collection and use of personal data, including data concerning health and location.

Under the GDPR, controllers must have one or more legal bases for processing personal data. The GDPR imposes additional, stricter conditions on the collection and processing of “special category” personal data.

Employers may be able to rely on either the legal basis which permits processing where necessary for compliance with a legal obligation or where the processing is necessary in the public interest.

For the processing of special categories of personal data in response to COVID-19, employers may be able to rely on either the condition which permits processing where necessary for compliance with an obligation under employment law or the condition allowing processing where there is a substantial public interest.

Legal bases for processing COVID-19 data

Hannah Jackson, Olga Kurochkina and Roshni Patel

Under some complex legal frameworks such as the GDPR and many regimes around the world influenced by the European approach to privacy, each data processing operation requires a legal basis. The GDPR provides six legal bases: consent, contractual necessity, legal obligation, vital interests, public interest and legitimate interests. In processing personal data to respond to COVID-19, many organizations will have to re-evaluate their legal bases for processing to accommodate a range of new activities, including and in particular an increase in the processing of data relating to individuals' health. Notably, in some countries, including the United States, there generally is not the need to have to choose from among a number of legal bases to process personal data in the first instance, though other conditions on the processing of personal data may apply.

Health data is one of the types of “special category” personal data under the GDPR which imposes additional, stricter conditions on its collection and use, which is the case in a number of jurisdictions globally. Under the GDPR, these conditions must be met in addition to one of the six legal bases for processing set out above; moreover, the processing frequently must be authorized by specific European Union or Member State law in addition to the GDPR.

What personal data is processed in response to COVID-19?

When considering the processing of ‘COVID-19 data’, many will think of information relating to individuals' health: temperature screening readings, or records of symptoms and diagnoses obtained from health questionnaires or testing. This is undoubtedly a significant element of the ‘COVID-19 data’ processed by organizations in both the public and private sectors.

In the context of new technologies to manage the current pandemic, ‘COVID-19 data’ may also include telecoms data, such as location and access data, processed by applications designed to track infection and monitor population movement. In Europe and other similar regimes, in addition to identifying a legal basis for the processing of this personal data, controllers must also comply with any applicable e-privacy requirements.

In particular, where information is obtained from or stored on a user's internet connected device, that user's consent will be required (regardless of the legal basis for processing identified under the GDPR) unless exemptions are introduced in national legislation.

Processing of COVID-19 data by employers

Many employers used to processing only ‘standard’ human resources data are now considering collecting significantly increased types and volumes of information relating to employees' health in an effort to manage the return to pre-pandemic operations. In Europe and under similar regimes, identifying an appropriate legal basis for this processing and ensuring appropriate safeguards are in place to maintain compliance with that basis will be the first step in implementing these plans.

Consent?

This comes as no surprise: just as for other types of employee data processing, employers should avoid relying on consent (or explicit consent where special category personal data is processed) when processing ‘COVID-19 data’ relating to employees, as employee consent will normally not be considered “freely given”. Note that the concept of inequitable bargaining position precluding employees from being able to freely give consent is not ingrained in the United States and various other countries.

Legal obligation and public interest

In the employment context in Europe, the processing of ‘COVID-19 data’ which does not constitute special category personal data may be necessary for compliance with a legal obligation (under European or Member State law) to which the employer is subject, such as obligations relating to health and safety in the workplace.

An alternative legal basis for the collection and use of this type of personal data may be found where the processing is necessary for the performance of a task carried out in the public interest, in particular for the control and monitoring of the epidemic. The basis for this processing must be set out in European or Member State law, however. Employers may also be able to demonstrate that the collection and use of personal data to transition back to normality is within their ‘legitimate interests’, having established safeguards which enable those interests to be balanced against the rights of the individuals whose personal data is processed.

Where employers in Europe plan to process “special category” personal data as part of their response to COVID-19, additional conditions must be satisfied. These types of personal data, including information about individuals’ health, may be processed where necessary for an employer to comply with its obligations under European or Member State employment, social security or social protection legislation (as above, to comply with work place health and safety requirements, for example), or where the processing is necessary for the performance of a task carried out in the substantial public interest, again where the processing is permitted or required by European or Member State law other than the GDPR.

With this in mind, not all employers will be able to rely on this ‘substantial public interest’ legal basis. The evaluation of health risks and collection of information on COVID-19 symptoms may lie within the exclusive competence of public health authorities, for example, or there may be no applicable law which supports the collection and use of this information.

Special attention to the further processing of COVID-19 data

Also in Europe if an employer processes ‘COVID-19 data’ for purposes which are different from and incompatible with those for which the information was originally collected, this further processing will require its own legal basis. For example, an employer collecting employees’ temperatures to facilitate a return to corporate premises will require a new legal basis should it subsequently wish to use this information for the purposes of assessing performance.

Processing of ‘COVID-19 data’ by public authorities

The GDPR allows for the processing of personal data by competent public health authorities, in particular, in the context of pandemics. As such, “monitoring epidemics and their spread” is expressly cited as a type of processing that may serve both important grounds of public interest and the vital interests of the data subject. Indeed, in some jurisdictions the assessment and collection of information on COVID-19 symptoms and information on recent movements of certain persons may be the exclusive responsibility of public health authorities.

Under such circumstances, public authorities in Europe have no need to rely on the consent of individuals: a mix between vital interests and public interest will be a sufficient and lawful legal basis for processing of COVID-19 data.




What to do now

Prior to collecting and using personal data to respond to COVID-19, controllers should identify an appropriate legal basis for processing – ideally by undertaking a data protection impact assessment.

Organizations should carefully document their processing of 'COVID-19 data' in their processing records and amend their privacy notices and data protection policies accordingly taking into account the applicable legal bases.

Organizations should keep their own assessments of the applicable legal bases under review to ensure that they continue to be valid as the situation evolves.





Quick read

Employers may need to collect and process additional personal data of employees in order to continue to operate safely and efficiently during the COVID-19 pandemic.

Complying with the principle of transparency will be vital to ensuring that the processing of employee personal data is lawful in a number of jurisdictions.

Transparency information provided to employees on the processing of COVID-19 related personal data should be easily accessible, written in clear and plain language and allow the employee to genuinely understand what personal data is being processed and for what purposes.

Employers should consider specific guidance and recommendations issued by relevant authorities in the countries where they employ staff.

Employers' transparency requirements when collecting COVID-19 data

Emma Hughes, Ana Rumualdo, Patricia Suarez and Weronika Wotosiuk

In the face of the global COVID-19 pandemic, employers across the globe have needed to take exceptional measures in order to continue to operate safely and mitigate the impact of COVID-19. Many measures adopted by employers require the collection and processing of employee personal data in ways that the employer has not previously been required to do.

A top priority for employers during the COVID-19 pandemic will be the protection of employees by ensuring safe and hygienic working conditions. Many countries have introduced COVID-19 related regulations which impose on employers additional healthcare obligations in order to mitigate and prevent the spread of COVID-19, and, even when not required by law, other employers have sought strategies to continue operations while providing a safe workplace. The performance of these obligations may compel employers to introduce certain preventive measures in the workplace or procedures in the case of confirmed COVID-19 cases. These preventative measures may require the collection of sensitive information or disclosure of personal data to public authorities or to other employees. For example, when an employee is suspected or diagnosed with COVID-19, the employer may need to inform other employees without disclosing the identity of infected or possibly infected employee.

In addition, given the restrictions of movement and gathering, a large number of employees will be working remotely throughout the COVID-19 pandemic. The result is that employers will be using various tools such as frequent video calls in order to communicate with employees. In order to continue to operate effectively, some employers may also monitor the remote working performance of employees using activity monitoring software. Such measures will result in employers collecting and processing additional personal data of employees.

Information to be provided by employers

In order to comply with the transparency requirements under a number of data protection laws, information and communications relating to the processing of employee personal data must be easily accessible (e.g. available on the employee intranet) and easy to understand, using clear and plain language. Where required, employers should adapt such information so that employees can genuinely understand the extent of the processing of their personal data. Employees should be in a position where they understand what personal data is being collected and for what purpose.

Before carrying out any COVID-19 related data processing, employers must review existing employee privacy notices and other documents (e.g. internal policies or guidelines) to ensure all relevant information regarding the processing of COVID-19 related personal data is provided to employees.

Where employers intend to carry out any processing of COVID-19 related personal data that is not covered by existing employee privacy notices, when required by applicable data protection laws employers must provide additional information to ensure that the processing is both fair and transparent. Such additional information must include:

- The COVID-19 related personal data that will be collected and processed (e.g. health data or personal data related to remote working activities).
- The recipients of personal data (e.g. those employees who were in close contact with colleagues who have tested positive for COVID-19 or exhibiting symptoms – without disclosing his/her identity except as allowed by national law), including where applicable transfers of personal data to third countries and implemented safeguards.
- The specific purposes and applicable legal bases of the processing (taking into account the guidance and recommendations issued by the relevant national supervisory or other regulatory authority).
- The period for which COVID-19 related personal data will be stored (e.g. will personal data be deleted immediately after the pandemic is over).

In the majority of cases, it is likely that the processing of COVID-19 related personal data will not be fully covered by existing privacy notices and policies. Accordingly, where required, employers should implement appropriate mechanisms to provide updated or additional information to employees, visitors and clients prior to such processing. This presents an opportunity for employers to engage with employees and explain in simple terms why they are processing personal data and for what purposes.





What to do now

Review existing employee privacy notices and policies to ensure they appropriately cover the processing of COVID-19 related personal data.

Ensure that the information provided allows employees to genuinely understand why COVID-19 related personal data is being collected and for what purposes.

Enable appropriate channels so that employees, visitors and clients can easily receive and access information regarding the processing of COVID-19 related personal data.

Consider specific guidance and recommendations issued by supervisory or regulatory authorities in relevant countries where staff are employed.

A close-up photograph of a person's arm being scanned by a white, handheld non-invasive temperature scanner. The scanner has a small digital display and a blue button. The background is a blurred green wall with a large, faint stopwatch icon.

Quick read

Temperature screenings will be an important part of the back-to-business plan for many organizations.

However, the laws and regulations regarding temperature screenings vary broadly across jurisdictions. Some jurisdictions are broadly permissive of temperature screenings, while other jurisdictions continue to prohibit or strictly regulate temperature screenings even when conducted to help protect the health of the workforce, customers, and visitors.

Organizations must, therefore, assess temperature screening deployments based on the relevant jurisdictions and the specific nature of the screening programs.

Temperature screening privacy implications

James Denvil, Alex Ford-Cox, Anja Gremmelmaier and Theresa Mengler

One of the common symptoms of those infected with COVID-19 is a high fever. There are a number of technologies available to conduct temperature screenings swiftly and with little or no physical intrusion. As a result, many organizations are using or considering temperature screenings as a way of identifying who should be permitted entry to facilities and establishments.

Temperature screening deployments must be assessed based on the populations to be screened (e.g. worksite screenings vs. screenings for entry to retail stores or public transit). Organizations must take into account the nature of the technologies used for temperature screening, particularly if facial detection systems (or other biometric identification technologies) are deployed. Further complexity arises from the fact that the legal privacy compliance obligations will vary across jurisdictions, ranging from limited obligations under broadly permissive regimes to prohibitions under restrictive regimes.

EU and UK overview

Although many privacy compliance requirements in the European Union have been harmonized under the General Data Protection Regulation (“GDPR”), privacy compliance under GDPR with respect to temperature screenings is complex. EU Member States and local authorities have not adopted a uniform framework for regulating temperature screenings.

One reason for the lack of consensus is that temperature data derived from screenings is considered a special category personal data under the GDPR. The processing of such data under the GDPR requires a lawful basis under both Article 6 (required for processing any form of personal data) and a separate basis under Article 9 (which specifically addresses processing of special category personal data). In some jurisdictions, compliance with local law (such as workplace health and safety legislation in the UK) may provide a lawful basis under both Articles 6 and 9. However, in some jurisdictions, such as Belgium and France, employers may not lawfully conduct systematic temperature screenings of employees.

In addition to following published laws and regulations, organizations should take heed of regulatory guidance issued by relevant authorities. Some EU regulators have published useful, practical resources addressing frequent queries, such as whether and under what conditions an employer is allowed to take temperature readings from the employees.

In reality, organizations that operate across different EU countries should be wary of adopting a one-size-fits-all approach. The feasibility of temperature screening will depend on the specifics of the implementation. In practical terms, organizations intending to conduct temperature screening in the EU should consider:

1. Identifying the relevant jurisdictions in which such screenings are to be conducted.
2. Identifying the population to be screened and specifying the purposes for screening them.
3. Assessing whether relevant laws permit the contemplated screening practices.
4. Addressing broader GDPR compliance principles including: transparency, purpose limitation and record keeping (including whether to conduct a Data Protection Impact Assessment (“DPIA”).
5. Involving the Data Protection Officer.
6. Addressing relevant employment law and practical considerations, including for example, consulting with works councils and other groups, and translating privacy disclosures into local languages.

U.S. compliance

Screening employees' temperatures generally is considered a regulated medical examination under US employment laws. However, the US Centers for Disease Control and Prevention as well as state and local health authorities have recognized that temperature screenings are a useful way to mitigate community spread of COVID-19. In light of the potential benefits, employment authorities have stated that employers may conduct temperature screenings so long as certain precautions are in place such as:

1. Storing temperature records separate from personnel files.
2. Limiting access to screening results to those who need such information.

US-based organizations should consider privacy compliance at a state level. The California Consumer Privacy Act ("CCPA") requires certain businesses to provide California residents with information about how their personal information will be collected, used, and shared, along with information about consumer privacy rights. Businesses subject to the CCPA should assess whether their temperature screening programs will be subject to the CCPA and confirm that appropriate compliance mechanisms are in place should the CCPA apply.

The states of Illinois, Texas, and Washington have enacted laws restricting the collection and use of biometric information. Illinois' law allows individuals to recover up to the greater of \$5,000 or actual damages if biometrics are collected without consent. Businesses that intend to use facial detection technologies when conducting temperature screenings should assess whether biometric privacy laws will impact the screening process and consider whether express consents need to be obtained from screening subjects.

Asia-Pacific considerations

There is no uniform regulation that applies across the Asia-Pacific region with regard to the processing of personal data in the context of the coronavirus pandemic. Some jurisdictions may require consent to the collection of identifiable temperature screenings (e.g. Vietnam), while in other countries businesses may be broadly permitted to collect data from employees and visitors without consent for the purpose of coronavirus mitigation (e.g. China). In summary, while adopting a consistent approach to data collection and privacy practices across jurisdictions worldwide is always desirable, in the context of temperature screening, it is also important to understand and take into account where key jurisdictional rules stand.

What to do now

Identify the populations that will be subject to temperature screenings, the technologies that will be used for such screenings, the details of how screening information will be stored and shared (if at all), and the relevant jurisdictions.

Assess the legal requirements for conducting such screenings and confirm that broadly applicable privacy and data protection considerations are addressed (including transparency, lawful bases, data accuracy and retention periods, and data security).

Prepare materials to support required consultations with works councils or other stakeholders and communications to inform screened subjects about the nature and purpose of the screenings in line with applicable local requirements.



A close-up photograph of a person's hand holding a smartphone. The hand is positioned on the left side of the frame, with the thumb resting on the screen. The background is heavily blurred, showing indistinct shapes and colors, suggesting an indoor setting with other people or objects. The lighting is soft and natural, highlighting the texture of the skin and the metallic ring on the finger. The overall composition is clean and modern, typical of a professional report or presentation.

Quick read

Immunity certificates are intended to prove immunity to secondary infections of the virus and many countries see these certificates as the golden ticket to normality.

Given the current scientific uncertainty around COVID-19, there is a risk that any personal data processed in relation to immunity certificates would not be accurate and up to date.

Other privacy concerns arising from the use of immunity certificates relate to legal bases for processing personal data regarding immunity status, purpose limitation, automated-decision making, data security and storage limitation.

Using immunity certificates and data protection

Ina Bruns, Paula Garcia and Juan Ramon Robles

Notion of immunity certificates

The so-called “immunity certificates” or “immunity passports” are certificates that prove the presence of antibodies to SARS-CoV-2 and, theoretically, the individual’s immunity to secondary infections. Many countries see these certificates as the golden ticket to normality or, in other words, the way to allow the progressive and safe lift of lockdown measures without exposing the population to new waves of the virus. On that basis, many governments and companies around the world are planning to allow the holders of immunity certificates to be the first in line to return to work, travel and “normal life”.

The biggest scientific challenge at present is that many tests that detect antibodies are still inaccurate and not reliable. On top of that, we still do not have conclusive evidence that people who have recovered from the virus and have antibodies are indeed protected from future infection. In fact, the World Health Organization (WHO) has warned that the use of these certificates could even increase the risks of continued transmission.

Main privacy challenges in the use of immunity certificates

Despite the uncertainty, the use of immunity certificates may become commonplace and the privacy concerns arising from their use should be tackled from the outset.

Legal basis

Leaving aside employment-related considerations, entities that issue and use immunity certificates need to ensure that the processing of COVID-19 data is fair and lawful. Bearing in mind that an immunity certificate itself is likely to be regarded as health data of the certificate holder, companies must respect the specific and more stringent rules on the use of special category data. Legal bases may vary depending on national law and specific circumstances of use.

Accuracy

It goes without saying that accuracy in this context is critical from both a scientific and a privacy perspective. Therefore, in light of the current scientific uncertainty around COVID-19, there is a risk that providers and requestors of immunity certificates may be processing data which is not accurate or up to date. In reality, it is yet unclear whether immunity certificates are able to prove immunity at all. As a result, a company could be keeping inaccurate records if it labelled a certificate holder as “immune” and that individual was re-infected afterwards, with the added problem that it is unlikely for certificate holders to proactively request the change of their status from “immune” to “not immune”.

Purpose limitation

Under data protection law, any purpose for which personal data are processed must be explicit, specific and legitimate. In Europe, this is known as “purpose limitation” and, although it can be named differently in other jurisdictions around the world, the essence of the principle remains the same. This principle is of utmost importance in this context as the use of immunity certificates may lead to discrimination based on coronavirus immunity, especially in the context of employment and sectors like tourism, insurance and leisure. The principle of purpose limitation can help overcome this form of bias, for example, by ensuring that immunity certificates are only used for the ultimate purpose of avoiding the spreading of the virus, and not for other purposes which may not be legitimate or can be achieved by less intrusive means. A data protection impact assessment will certainly help (and even be necessary to) identify and address the risks resulting from the use of immunity certificates.

Automated decision-making

Due to the massive widespread of the virus, it cannot be ruled out the possibility that immunity certificates (or their absence) will be used to take automated decisions which significantly affect individuals, such as being accepted or denied entry into a country or place of work. Organizations subject to the GDPR or other similar frameworks around the world need to bear in mind that decisions based solely on automated processing of personal data are subject to more stringent rules and restrictions.

Data security

The urgency of the current situation should not prevent companies from implementing appropriate security measures to ensure that both hard and electronic copies of the certificates are kept safe and secure, especially given the sensitiveness of the data revealed by immunity certificates themselves.

Storage limitation

As with any other type of data, the general rule is that immunity certificates should not be kept indefinitely. Only time will tell us what the retention period for immunity certificates (or the criteria to determine the same) should be, and whether there may be other reasons (e.g. scientific or statistical purposes) which may justify longer retention periods.





What to do now

Keep an eye on scientific developments around immunity certificates and any guidance by data protection authorities on the topic.

Carry out a data protection impact assessment before deploying immunity certificates as this will help ensure that the purposes for the use of these certificates are clear and legitimate and there is no discrimination based on coronavirus immunity.

Ensure that there is a clear policy in place regarding data protection and the use of immunity certificates.

Keep in mind employment-related considerations around the use of immunity certificates.





Quick read

Contact tracing apps are key tools to deploy as part of the response to COVID-19.

It is essential that contact tracing apps embed privacy considerations into the development phase by undertaking a comprehensive privacy review, such as a DPIA, at the outset.

Transparency, purpose limitation and data minimization are key principles to focus on.

Other practical aspects to take into account include data storage and retention, security, accuracy, access and interoperability.

Making COVID-19 contact tracing apps privacy compliant

Giulia Mariuz, Alex Rutherford and Julie Schwartz

Contact tracing apps have emerged as a key tool to tackle the COVID-19 pandemic. Governments, national health services and organizations of all sizes are developing and implementing them as part of their strategies to manage the return to normality. There is no question that COVID-19 contact tracing apps are here to stay. The key question is how to ensure these apps are privacy and data protection compliant.

Key areas of focus for privacy compliance

As a starting point, it is essential that contact tracing apps embed privacy considerations into the development phase and comply with data protection by design and default. In practice, this means documenting the steps taken, conducting a rigorous privacy review that considers privacy risks and the ways to address them, and keeping it under review. In Europe, according to the European Data Protection Board (“EDPB”), formal Data Protection Impact Assessments (“DPIAs”) are mandatory for contact tracing apps.

Transparency will be crucial. Users should understand what data will be gathered, the uses of that data, and any recipients of data gathered through the COVID-19 app. In Europe and some other jurisdictions, entities must also identify the controller of the data, an appropriate legal basis for processing, and the existence of rights available to individuals. All of this information should be provided to the data subjects at the outset before they use the app, ideally by way of a suitable privacy notice which is clear and comprehensive.

COVID-19 contact tracing apps must respect the principle of purpose limitation, as the data collected must be used for clear, specific and justifiable purposes. By way of guidance on how to apply this principle in this context, the European Commission has indicated that the prevention of further COVID-19 infections is not specific enough and that multiple purposes should not be bundled together.

Contact tracing apps should process only data truly necessary for the stated purpose. This entails aggregating or anonymizing the data where

possible. If contact tracing involves alerting those who have been in close proximity with an infected person, this should be done anonymously.

There is also a preference to use proximity data (e.g. data generated by the exchange of Bluetooth signal) rather than location data. According to the EDPB, location data is not necessary and would increase privacy and security risks. Overall, unrelated data (e.g. messages, call logs, and identifiers) should not be captured or processed by COVID-19 apps.

App developers and users must also consider data storage and retention. Data should be destroyed once it is no longer necessary for the relevant purposes – maximum one month after an individual was tested negative, according to the European Commission. The Commission does suggest that health authorities may retain proximity data for longer for surveillance or research, but this data must be anonymized.

Security

Contact tracing apps must also be as secure and safe as possible. Industry standard cryptographic methods should be deployed to securely store and transmit data between apps and remote servers. Other security safeguards to implement include user authentication methods, logging controls and adopting security by design. The apps need to be tested as much as possible, including functional aspects (e.g. ensuring sufficient bandwidth to prevent the app/system crashing) and security elements (e.g. source code scanning and vulnerability scanning to consider threats to security infrastructure).

Accuracy, access and interoperability

The accuracy of the data is critical not only to ensure privacy compliance, but also for app effectiveness and to generate trust. Organizations need to identify potential sources of inaccuracy and mitigate those risks, especially in relation to false positives. For example, there are certain issues with obtaining accurate measurements from Bluetooth signals depending on where the user is located, and how many people are in close proximity. There is also a risk of users submitting false information either intentionally or unintentionally.

Contact tracing apps will only be effective if there are significant adoption rates. The overall access of the app also depends on its interoperability with different systems and devices. Ultimately, it is essential that users trust COVID-19 apps. Building a robust privacy framework is a key step to enhancing trust and making COVID-19 contact tracing apps truly effective to achieve their purpose.

Sophie Baum, a Law Clerk in our Washington, D.C. office, contributed to this chapter.



What to do now

Ensure that privacy and data protection professionals are directly involved in the development and implementation of COVID-19 contact tracing apps.

Carry out a DPIA of any proposed COVID-19 apps at the outset.

Focus on key privacy principles such as transparency, purpose limitation and data minimization as part of the building blocks of the app.

Embed data security by default.

Document all privacy and data protection measures adopted and keep them under review.





Quick read

While a business may be able to more easily institute return-to-work protocols for its employees, vendor contracts may contain provisions that facilitate or impair the business's ability to impose the same types of obligations on contractors.

Businesses will need to identify their rights as well as any contractual hurdles to collecting, using, and sharing health status information, denying contractors access to their premises, or requiring contractors to adhere to new safety protocol such as contact tracing.

Shelter-in-place may not be a one-time occurrence, and businesses and vendors may be able to proactively communicate about contractual ambiguities or conflicts to facilitate continuity of services in the event of another major workplace disruption.

With the benefit of hindsight, parties should consider revising certain template terms that are often overlooked and under-negotiated, such as business continuity and disaster recovery, force majeure, frustration, and arbitration clauses.

Vendors and contractual implications of a COVID-19 exit strategy

Morgan Perna and Nathan Salminen

As the world jumped into shelter-in-place, new working restrictions created extraordinary business disruptions that forced parties to examine their right to walk away from a contract under the governing force majeure provision. As we transition out of this shelter-in-place, businesses must consider how new and existing vendor contracts will be impacted, and even leveraged, to support a return to work.

Data regarding service provider personnel

In order to safeguard the workplace, businesses may wish to collect, use or disclose additional information regarding service provider personnel that may work on site at the business's location or otherwise interact with the business's personnel.

For example, some businesses may rely on contact tracing to track workplace interactions, travel history and travel plans of not only employees but also on-site contractors. Companies may trace by communicating directly with infected or at-risk workers, or may rely on device-based tracing technologies, such as tracking applications that alert workers who are encroaching on another worker's safety radius or that workers have come near individuals who have reported a positive COVID-19 status. Likewise, Businesses may wish to collect health status information regarding service providers' personnel, such as temperature checks, symptoms, or physicians' orders. Contracts with service providers may not include any type of mechanism that would allow the business to require service providers to, or to require their personnel to, provide this type of information or to submit to these types of surveillance.

Likewise, contracts with service providers may actually prohibit the collection, use or disclosure of these types of information. For example, a contract may have a broad definition for "confidential information" that would reach these types of information. If so, businesses may need to carefully review any restrictions on the use or disclosure of confidential information to determine whether the sorts of uses and disclosures they expect to make in connection with these sorts of measures complies with those restrictions. For example, contracts often include all information provided by a party's personnel, or "information that would reasonably be seen

as confidential" in the definition of "confidential information" and contracts often restrict the use of confidential information to only those uses that are necessary to exercise a party's rights under the contract. In those cases, with relatively standard confidentiality terms, these types of uses and disclosures of health data may be (perhaps inadvertently) prohibited by the contract.

In some jurisdictions, the collection, use and disclosure of these types of data may also require notice of the personnel or collecting consent from the personnel. In some cases, a business may need to rely on its service providers to facilitate those processes, but contracts may be unlikely to have contemplated that structure.

Data otherwise acquired from counterparties

In addition to data about the personnel of service providers, businesses may collect various types of data from contractual counterparties that are now relevant for purposes that were not considered when the contract was drafted. For example, a business may receive information regarding the locations of the devices of its employees when those employees use ride sharing apps funded by the business. A business might receive information regarding health insurance claims made by employees. A business might receive demographic information from resellers about customers who purchased a ticket to an event. If a business wishes to use any data that it receives under an existing contractual relationship for new purposes in connection with the transition out of shelter-in-place policies, that business should review those contracts to determine whether those uses are permitted.

Costs arising from workplace protections

As businesses implement new workplace safety protocols, workers may be required to wear personal protective equipment in certain workplace settings or adhere to other safety measures. Some types of businesses may need to reorganize how they operate entirely. These sorts of costs may fall on either the business or its service providers in the first instance, and in either case, those cost may need to be reallocated between the parties. In cases where a business is imposing new, and potentially expensive, requirements on a service provider, that service provider may resist absorbing that cost, and the contract with that service provider may or may not address that issue.

For example, a contract may require a service provider to comply with the reasonable workplace policies of the business, and it could be argued that a requirement to keep work spaces spread out a certain distance is a reasonable requirement that could be placed in a workplace policy, and hence the service provider would be required to implement those sorts of changes. On the other hand, a contract may be written in a “time and materials” model where the costs would all flow back to the business. Even if the service provider would technically be required to absorb significant costs, the service provider may simply not be willing to continue performing the services with those higher costs.

Shelter-in-place round 2?

Companies should identify provisions in vendor contracts that could be implicated if there is a subsequent shelter-in-place mandate. If the parties are able to anticipate events that would significantly affect their relationship, then the parties may be able to save time and money and preserve their relationship by planning accordingly. Such planning may include notifying the other party of any changes to cost or deadlines, revising the scope of products or services, or amending security or safety protocols that contractors are required to honor. The parties should identify any ambiguities in the contract, any conflicting interpretations of terms or expectations, or any cost-shifting issues. Parties may avoid relying on force majeure clauses or years of litigation by aligning expectations or amending obligations ahead of the next work disruption.

Businesses may consider submitting short questionnaires to vendors to learn more about their business continuity and disaster readiness, including how to maintain services when supply chains are (again) disrupted.

Revising template terms

This crisis put center-stage some less-negotiated commercial terms. Drawing upon lessons learned this time around, businesses might revisit certain template provisions to future-proof their rights and obligations in event of a similarly halting event:

- **Business continuity and disaster preparedness.** Major IT contracts often obligate the supplier to implement business continuity and disaster recovery plans. With the benefit of hindsight, businesses may consider expanding their template business continuity and disaster recovery requirements to more specifically address pandemics and similar disasters.
- **Force majeure.** Consider whether a pandemic or crisis of similar magnitude would trigger the force majeure provision for a particular vendor. A party’s position as vendor or business as well as the specific product or service being offered will guide whether the party will benefit from expressly including or excluding pandemics from template force majeure provisions.
- **Frustration.** In certain relationships, and where permitted by law, it may be appropriate to include a frustration clause. Frustration clauses are generally triggered upon events of lesser magnitude than forces majeure, where performance becomes so costly or requires so much more time or resources that a party’s performance of the contract is frustrated. Businesses may wish to consider whether or not such a clause may be appropriate to address a possible return to shelter-in-place policies.



What to do now

Assess the rights of the business to require vendors to disclose or permit the collection of additional information, whether the business will require assistance in collecting that information from the vendor, or whether the business expects to use or disclose information it receives differently, and consider amending the applicable contracts to address that collection, use and disclosure of data.

Determine whether the business or the vendor will bear costs relating to COVID-19 safety protocols.

Anticipate any vendor relationships that may be particularly stressed by another shelter-in-place order and communicate proactively with that vendor to prepare and minimize conflict.

Review template vendor contract terms for weaknesses that were exposed during the COVID-19 response.

Revise terms to build in better protections and enhanced rights to account for extraordinary disasters in the future.





Quick read

Engaging DPOs or other privacy officers and undertaking DPIAs will help organizations manage data protection compliance in the challenging COVID-19 context.

DPOs should form part of the COVID-19 crisis management team and encouraged to see themselves as part of the solution to this challenge, so they can contribute their knowledge in a practical and constructive way.

A DPIA or other privacy review is a hugely useful tool to help organizations put in place an effective COVID-19 exit strategy. It provides a roadmap for how to ensure data protection compliance and demonstrate that you have done so.

The role of Data Protection Officers (“DPOs”) and Data Protection Impact Assessments (“DPIAs”) in the context of COVID-19 measures

David Bamberg, Valerio Natale, Sabrina Salhi and Louisa Williams

Since the GDPR became enforceable in May 2018, organizations have been coming to grips with the roles of DPOs and DPIAs, attempting to integrate them into normal business practices efficiently and effectively. The two roles share a number of qualities: both are important mechanisms for enhancing data protection compliance and accountability introduced by the GDPR.

In these times of COVID-19, innovation is, of course, key, with new self-reporting apps and contact tracing technologies likely to become increasingly commonplace. As organizations begin to explore these more intrusive forms of data processing in an effort to protect workforces and prevent the spread of COVID-19 more generally, appreciation of the role of DPOs and DPIAs will be crucial to ensure and demonstrate that any such processing is fully risk-assessed and undertaken with data protection compliance firmly in mind.

In times of crisis, your DPO is your friend

Put simply, the role of a DPO or other officer responsible for advising on privacy compliance is to help an organization meet their obligations under data protection law, particularly when any high risk processing involving sensitive data, such as health data, is anticipated. In the context of managing the COVID-19 crisis, it is clear that organizations will need to adopt a range of data-reliant measures in order to protect the health and safety of their staff. This will typically include the deployment of intense data processing operations involving sensitive information. With that in mind, it is essential that business leaders and managers understand that a DPO should be at the forefront of the deployment of effective and compliant data activities. When engaged fully from an early stage, a DPO will be able to help organizations reinforce their ability to use data in this way.

In practical terms, this means a number of things:

- DPOs should form part of the COVID-19 crisis management team, particularly in relation to any strategic and practical steps involving the use of sensitive personal data.
- Any plans to develop or implement technological solutions that rely on the processing of personal data should have the input of the DPO.
- This input should be actively sought by senior decision-makers as part of the planning process.
- DPOs should be encouraged to see themselves as part of the solution to this challenge so they can contribute their knowledge in a practical and constructive way.

DPIAs – your cure for COVID-19 compliance

Under the GDPR, DPIAs are mandatory for any high risk data processing, and data protection authorities across Europe have published non-exhaustive lists with examples of the types of processing that are likely to trigger this requirement. In the context of COVID-19 measures, self-reporting, contact tracing technologies and certain medical checks (such as temperature screening) will be processing health and location data in a way that most people would probably find intrusive and unwelcome in normal times. With that in mind, and supported by EDPB guidance, the implementation of most COVID-19 measures in Europe will require a DPIA.

Undertaking a DPIA or other privacy assessment proactively and from an early stage is not only a legal obligation, but a good business practice, particularly in a crisis. Given the potentially sensitive nature of the data, this is especially true in relation to COVID-19 measures. A DPIA will help organizations consider, identify, address and record explicitly all the key data protection issues related to a particular COVID-19 measure. In other words, a DPIA will be a hugely useful tool to help organizations put in place an effective COVID-19 exit strategy – a roadmap for how to ensure data protection compliance and demonstrate that you have done so. Involving the DPO in the DPIA process – which in Europe is required under the GDPR – will also help to find solutions to data protection issues and challenges which arise from the risk assessment.

The key message

With sensitive data collection and innovation playing an increasingly crucial role in preventing and managing the spread of COVID-19, the role of DPOs and DPIAs is critical. By ensuring that DPOs are engaged and DPIAs are undertaken, organizations will be better placed to justify their use of any COVID-19 measures, while simultaneously ensuring and demonstrating that any such measures have been implemented in compliance with data protection legislation.





What to do now

Consider what new types of processing activities are likely to arise for your organization in the context of the COVID-19 Exit Strategy.

Consult with your DPO before undertaking any new processing, particularly where it is high risk.

Undertake a DPIA prior to implementing any COVID-19 measures and keep a comprehensive record of all new processing activities.





Quick read

The COVID-19 pandemic has changed the way all organizations operate by forcing a shift towards homeworking. This new way of working entails an increased risk of cyber-attacks and personal data breaches.

Being accountable, recording all actions and measures taken, and keeping a pre-litigation strategy in mind when designing data processing arrangements is key.

Essential precautions to take when employees are working remotely include ensuring that policies, protocols and procedures governing remote working arrangements are up to date, providing security-related training, adopting key technical measures such as the use of VPNs and strong access controls, and keeping employees on high alert and increase their cyber-awareness generally.



Cybersecurity precautions for an agile workforce

Laur Badin, Wout Olieslagers and Noor Hogerzeil

As part of the global COVID-19 containment strategy, governments imposed strict measures (lockdowns) to control and prevent the spread of the virus. These measures forced many organizations to migrate towards new work-from-home practices, or scale up existing arrangements.

With remote working more widely available and the transformation of the working environment exceeding its initial lifespan, companies' exposure to cybersecurity threats is now growing exponentially. In this rapidly evolving context, it is vital to address the cybersecurity challenges to ensure business continuity and safeguard critical information. In light of the COVID-19 response and its undeniable global repercussions, some organizations may take the view that remote working is here to stay. Cyber threats increase the risk of suffering a security breach, and this may lead to costly regulatory investigations and even class action litigation. Therefore, companies must be able to prove that their data processing and security standards are in line with the applicable laws. Being accountable, recording all actions and measures taken, and keeping a pre-litigation strategy in mind when designing cybersecurity safeguards and data processing arrangements is key.

What precautions should businesses take when employees are working remotely?

Policies: Ensure that policies, protocols and procedures governing remote working arrangements, use and monitoring of company resources and devices, BYOD, business continuity and disaster recovery, and incident management and response – including the collection and subsequent processing of personal data in those contexts – are reviewed, updated and effectively communicated to staff.

Resources: Consider allocating specific resources such as user-friendly guides and accessible contact points (e.g. hotlines). These can help employees to better understand and react to their new working environment.

Devices: Company-issued devices must be encrypted, to help safeguard the information stored on such devices whilst at rest. Remote device management tools must also be implemented in order to ensure that lost or stolen devices can be locked, erased or recovered as necessary. Personal devices must pass a prior security vetting process to ensure that they have been updated and patched. Otherwise, they should not be used to store or transfer company information.

Training: Ensure that all employees refresh security-related knowledge by making available training modules covering topics such as: (i) remote working “hygiene” by locking, protecting and safeguarding devices and removable media or paper documents, and (ii) detection, management and reporting of security incidents and personal data breaches.

Connection: Before enabling access to corporate applications and resources it is essential to set up an encrypted network connection (e.g. via VPN), which authenticates incoming connection requests. The VPN should be able to accommodate a much larger than usual number of simultaneous connections, and must be updated with the latest security patches.

Credentials: Staff must only use unique and complex passwords and, where available, multi-factor authentication (e.g. verification codes or tokens). Users' access credentials must only be stored if encrypted. Other advisable access control measures include: (i) establishing account timeouts for privileged users, (ii) disabling default administrator accounts, (iii) limiting remote access connections, and (iv) disabling access to OS administrative tools, shortcuts or help menus.

Services: Businesses may need to acquire new services or add user licenses to existing platforms so that employees can collaborate, share documents and stay in touch with other stakeholders as they did in the office. Most of these activities are performed through online tools and services that must be evaluated through an exhaustive due-diligence process to ensure that all vendors are held to high security standards.

Videoconferencing: When relying on online communication tools, organizations should choose a platform that (i) supports centralized management, (ii) provides end-to-end encryption, (iii) supports strong authentication (e.g. MFA), and (iv) integrates with existing business tools and Single Sign-on (SSO). Businesses should also instruct employees to (i) refrain from using these tools from personal devices, (ii) password protect all meetings and avoid public sharing of connection details, (iii) apply privacy-by-default settings, and (iv) only enable chat and screen sharing when absolutely necessary in order to avoid inadvertent disclosure of business sensitive information or personal data.

Email: Keep employees on high alert and increase their awareness when receiving and sending emails. Clearly instruct employees to: (i) be suspicious of emails that ask to connect to links or open files, create a sense of urgency or severe consequences, or may contain unusual requests, even if these come from an apparently legitimate source, (ii) refrain from replying or opening suspicious links and attachments, (iii) reach out to the security officer immediately, and (v) always check the integrity of links before providing login credentials. Evaluate additional measures that may enhance overall email security, such as flagging external emails and deploying additional anti-phishing tools.

What to do now

Design and implement a 5-Step Action Plan: (1) identify critical processes, (2) assess the impact on such processes from WFH arrangements, (3) make an inventory of WFH risks relevant to critical processes, (4) implement adequate measures to mitigate such risks, and (5) keep records of all actions and measures taken.

Ensure that the policies, protocols and procedures governing WFH (and the processing of personal data in such context) are updated accordingly and effectively communicated to affected staff.

Increase employees' awareness and preparedness levels by providing adequate training so that they understand the risks posed by working remotely and ensure the timely detection, management and reporting of any incident.

Closely monitor whether implemented measures appropriately address the cyber threats in practice.





Quick read

Cloud services have been essential to weathering the impacts of COVID-19 as organizations accelerate digitization projects. Cloud projects will likely also be a crucial component of any exit strategy.

To reduce legal, operational, and reputational risks, cloud solutions should be managed thoughtfully in the context of a broader IT strategy, with realistic expectations and timelines, thorough testing, and a clear understanding of legal obligations.

Organizations should identify legal requirements that may limit where and how cloud services can be used. Entering into data processing agreements is often a crucial element to support compliance.

As part of vendor due diligence, organizations should pay close attention to whether a cloud provider offers tools or sufficient safeguards to comply with security obligations, data localization requirements, and cross-border data transfer restrictions.

Getting cloud projects right in times of COVID-19

Henrik Hanssen, Shee Shee Jin and Filippo A. Raso

Cloud computing has proven to be a key technology for business continuity during lockdowns and quarantines. Organizations have leaned on Software-, Platform- and Infrastructure-as-a-Service (SaaS, PaaS, and IaaS) cloud solutions to market and distribute products and services, maintain capacity, and ensure workers can connect from afar, and COVID-19 has propelled many organizations to modernize operations and implement IT wish lists. While cloud computing has played a crucial role in keeping business open, organizations might also find cloud computing a central component of their COVID-19 exit plans.

What's the challenge?

Like other IT projects, the deployment, maintenance, and management of cloud solutions requires careful planning, thorough testing, and assessment of legal risks and compliance requirements. Despite the current circumstances, a diligent approach to cloud projects, including realistic expectations and timelines, is crucial to reducing legal, operational, and reputational risks. Wherever a company is in its cloud strategy, there are key considerations to keep in mind.

Build off existing plans and structures

Decisions made for the cloud can have significant impacts on an organization's IT and broader business strategy. While organizations have moved quickly to respond to COVID-19, working in the cloud without a strategy and coordination across teams risks wasted resources and undesirable consequences down the road, such as interoperability issues, compromised data security, or privacy concerns. Take stock of existing implementation and migration plans and consider how a new cloud project fits in your governance program, including compliance, security, data privacy, incident response, and vendor management.

Understand applicable legal requirements

Organizations must account for legal requirements when moving their operations and data to the cloud, including complex data privacy frameworks like the European General Data Protection Regulation ("GDPR") or the California Consumer Privacy Act ("CCPA"). Be mindful of specific requirements on outsourcing projects, particularly if you or your customers operate in highly-regulated industries, such as the financial, health, or public sectors.

Execute compliant data processing agreements

It is good practice – and often required by laws – to execute written agreements with cloud providers specifying how data are processed. For example, the GDPR requires data processing agreements that contain specific provisions, such as on subcontracting or data security. Many cloud providers offer standard data processing agreements that align with key legal requirements: make sure that these agreements satisfy your particular obligations.

Key data considerations for the cloud

Consider the following issues when adopting cloud services:

- **Data location and cross-border data transfers:** Cloud providers might store data on servers physically located in different countries, and sub-processors might be able to access data for limited purposes, such as hosting or support, even if operating in another country. Organizations subject to data localization obligations or cross-border data transfer or offshoring restrictions, including prohibitions from contract or professional obligations, should evaluate whether they can configure the cloud service to comply with those requirements or whether additional safeguards are needed. For example, European data controllers can consider whether a provider offers Binding Corporate Rules, EU Standard Contractual Clauses, or is certified under the EU-U.S. Privacy Shield.
- **Sensitive data:** Consider what types of data will be migrated to the cloud. Contractual terms detailing processing and safeguards may apply to customer data, and additional requirements often apply to the processing of sensitive data, such as health data. If the cloud provider might process sensitive data, pay extra attention to applicable data security requirements and evaluate whether the provider's practices align with those requirements. In the US, for example, government customers require specific security standards and controls.
- **Data security:** Security controls are a crucial element of each cloud project. Organizations should review the provider's documentation on data security, including aspects like intrusion detection, incident management, disaster recovery, access controls, and security audits (e.g., Service Organization Control ("SOC") reports or ISO/IEC 27000-series certifications). Shared resources are a key benefit of the cloud, and security controls are vital for implementing segmentation between environments. The dynamism of the cloud means that the environment may be constantly shifting, with the speed at which a new workload can be spun up. And companies often rely on vendors for critical components such as data migration and backup restoration. Assess how centralized tools, automation, and managed services will combine to implement and maintain security controls.
- **Risk, security, and impact assessments:** Organizations may be required by corporate policy or legal requirements to conduct and document risk, security, or impact assessments prior to using a cloud service and to periodically update such assessments. Cloud providers may have materials available to assist, including documentation on data processing activities and security safeguards.
- **Accountability:** Organizations may need to be capable of demonstrating compliance with legal requirements, such as by maintaining proper documentation regarding data protection compliance or audits. In the cloud context, such documentation may include audit reports that cloud providers regularly publish.
- **Termination and transition:** Consider the consequences of terminating a cloud service. Organizations should establish the parties' contractual obligations relating to the exit process, which usually require the provider to return and/or securely delete all customer data, including from backups.



What to do now

Integrate cloud projects into your COVID-19 exit strategy and consider how a cloud service fits within your organization's broader business strategy and governance program, including data governance and vendor management.

Identify and review compliance with legal requirements, including data localization requirements or cross-border data transfer or offshoring restrictions.

Conduct vendor due diligence and, if necessary, carry out a formal risk, security, or impact assessment of the cloud service.

Execute a data processing agreement that complies with legal requirements and establishes important processes, such as post-termination transition obligations.

Make sure cloud data are protected by appropriate and documented security controls.





Quick read

With all of the practical arrangements in place as a result of the pandemic and the need to keep in touch with customers and contacts, understanding the distinction between transactional and promotional communications is essential.

A transactional communication becomes direct marketing when it comprises any advertising or marketing that is directed to particular individuals.

Direct marketing is strictly regulated and the general rule in most jurisdictions is that businesses can only send marketing emails or texts with prior consent, unless an exception applies.

Businesses should always consider and respect the limits of what is permissible under the laws of the jurisdictions in which they operate when trying to get in touch with consumers.

Direct marketing communications in times of coronavirus

Chantal van Dam, Julia Gurieva, Katie McMullan and Sian Rudgard

What's the issue?

Across the world, large retail stores and small businesses alike are looking for ways to remain open for business. Mass gatherings and sporting events, conferences and concerts (and everything in between) are being creatively rearranged. With all of the cancellations, postponements and alternative arrangements that are required as a result of this global crisis, plus the special desire of all consumer-facing businesses to stay in touch with their customers and contacts, many organizations face the critical challenge of getting to grips with the legal rules that apply to those unsolicited communications and interactions. Below we explore the key issues to consider when sending such communications and provide practical guidance to approach this challenge without breaching any of the applicable rules.

What counts as direct marketing?

It would seem logical to assume that even if someone has unsubscribed from email marketing or opted-out of sales calls that it would be reasonable to contact them to tell them that the concert for which they have booked tickets, or the hairdresser appointment they have scheduled, has now been rearranged, or is now able to be rebooked. Similarly, when a business – such as bank, a supermarket, or retailer – plans to return to operate under special trading conditions and hours, it will naturally want to let its customers know. But what if that email or telephone call to a consumer also includes an advertisement for its online offering, upcoming events, or a new product/service on offer which goes beyond what the consumer would typically expect from the organization in question? Does that communication then qualify as ‘transactional’ (and hence outside the direct marketing rules) or ‘promotional’?

Many countries have different views on what counts as direct marketing but the common theme is that it comprises any advertising or marketing that is directed to particular individuals.

It includes not only communications that offer goods and services for sale, but also promotional emails (e.g. explaining the aims or philosophy behind a business’s approach to, or exit plan from the pandemic). Contrast this with communications that are likely to be considered ‘transactional’ or service-related (and therefore outside of the rules that apply to marketing communications), such as when the communication directly relates to a particular product or service that a customer receives or has ordered. Transactional communications are typically functional and provide information that a customer needs about a current contract or past purchase (e.g. purchase confirmation messages, delivery updates or other routine customer service messages). Even transactional communications, however, depending on the mode of delivery (e.g. if sent by text with autodialer equipment), the relationship with the sender and how the sender obtained the recipient’s contact information may be subject to various restrictions.

As a general rule, any communication that is sent to a customer or prospect wholly or partly in order to market products or services to that individual is likely to be considered direct marketing. Understanding when a transactional communication becomes direct marketing has therefore become an urgent necessity to ensure that a well-intended attempt to reassure customers when dealing with COVID-19 special arrangements does not breach a law relating to the use of their personal data.

Practical steps to get it right

While the legal framework is different in every jurisdiction, the general rule in most jurisdictions is that businesses can only send marketing emails or texts with prior consent, unless an exception applies. A notable exception is the approach to marketing emails in the United States where they can be sent by default without consent provided there is an opportunity for the recipient to opt-out. However, even in the United States, certain types of communications require advance consent in a very specific format. But, as a general matter in many jurisdictions and in particular in Europe, for consent to be sufficient it follows a particular format. In particular in Europe, to be valid, consent must be knowingly and freely given, informed, clear and specific. Individuals should be informed of and consent to:

- The organization sending direct marketing communications.
- The specific types of communications they would like to receive (e.g. call, automated call, email, and text).
- The specific brand, products or services about which they would like to receive communications.

This means that an organization must be satisfied that the individual fully understands that they are giving consent and the scope of that consent, and that they have clearly indicated their wishes by a clear affirmative action. In practice, the clearest way to obtain such consent is to ask the customer to tick an opt-in box confirming they agree.

An organization should keep clear records of what a person has consented to, and when and how it got this consent, so that it can demonstrate compliance in the event of a complaint. An opt-out or 'do not contact' list must also be maintained and consulted, so that opt out requests are respected.

Prior consent may not be required in all cases. In countries where the organization has an existing relationship with an existing or potential customer, there may be an exception to the opt-in consent rule for sending direct marketing communications. The concept of "existing business relationship" is defined differently in different countries and even as to different forms or marketing. This exemption, the so-called

"soft opt-in exception", allows an organization to send direct marketing communications without consent if certain conditions are met. As a general rule, and noting that there are some differences on a per country basis, the soft opt-in rules allow an organization to send marketing communications without prior consent where it:

- has obtained the email address directly from a prospect or customer in the course of sale (or negotiations for a sale) of a product or service to that prospect or customer;
- is only marketing its own similar products and services (so no third party marketing and no marketing of unrelated products); and
- has provided the opportunity to opt out of receiving the marketing, both when first collecting the contact details from the individuals concerned and in every message after that (e.g. by including an opt-out hyperlink in marketing emails).

What's the risk?

Penalizing businesses for getting this wrong may not be at the top of regulators' lists during these unprecedented and uncertain times. However, in some countries, such as the United States for texting and telemarketing activities depending on how they are performed, the potential for major liability under private plaintiff class action litigation is significant. To retain consumer confidence and reduce the legal risk from both from a customer, regulatory and litigation risk standpoint, it is crucial to remember that compliance with relevant laws remains very important and that in many countries individuals have the right to control how their contact details are used by others. Therefore, even in times of coronavirus, it is essential that businesses consider and respect the limits of what is permissible under the laws of the jurisdictions in which they operate when trying to get in touch with consumers and that they are not seen or perceived as taking advantage of customers in these unprecedented times. Social distancing has made customer communications more important than ever, but getting those communications right today will likely be remembered once this nightmare is finally over.



What to do now


Consider whether your customer communications are purely transactional or whether they also contain promotional content.

If the communication contains promotional content, check whether you can rely on an exemption, such as soft opt-in to send the communication on an opt-out basis.

If you cannot rely on the soft opt-in exception, check whether you have obtained valid consent from the relevant individuals to receive direct marketing communications.

Before sending the communications, check your 'do not contact' list to ensure promotional content is not sent to the individuals who have exercised their right to opt-out.

Look at your own communications through the lens of your customers and assess how those customers are likely to perceive them.





Quick read

It's almost business-as-usual for some data protection authorities who continue their investigation and enforcement activities into breaches, whether related or not to the COVID-19 crisis.

When it comes to measures implemented in the wake of the crisis, data protection rights are not "in quarantine". Wary data subjects will be keen to ensure this remains the case, while regulators will be watchful that any new collection and processing of personal data remains lawful.

Companies would be wise to revisit existing data compliance policies – and map out supplemental policies targeted to the crisis – as soon as possible.

Cybersecurity risks are on the rise with the move to remote working – mitigating the potential for future regulatory investigations or data class actions related to data leaks is vital.

Mitigating investigation and litigation risks

Christelle Coslin, Victor Fabre and Adeela Khan

1. Will COVID-19 impact the investigation of data breaches unrelated to the crisis?

By all accounts, it is almost “business-as-usual” for some data protection regulators when dealing with breaches that predate the crisis. At the same time, authorities have acknowledged that added flexibility may be required and introduced temporary derogations to current investigations or to the usual investigation framework, notably in terms of deadlines. To take a couple of examples:

- In France, we have seen the CNIL initiate new investigations for alleged breaches unrelated to the COVID-19 situation. Moreover, the CNIL continues existing investigations, in particular through online inspections - but with extended time limits for organizations to reply to requests from the authority, and additional time to comply with formal notices. On the flipside, in a statement dated 17 March 2020, CNIL has also made it clear that shorter deadlines may instead be stipulated in case of serious violations of GDPR.
- The UK ICO’s Regulatory Action Policy requires it to take into account economic impact and affordability of any measures levied; as noted by the authority in its statement dated 15 April 2020, in the current circumstances this may mean that “the level of fines is reduced”. In this light, it is noteworthy that as at April 2020 the ICO has delayed imposition of several proposed GDPR-related fines of a large magnitude.

Despite this, and as set out below, it is clear the crisis will not be accepted by authorities as a blanket excuse for disregarding either existing or future data protection issues. Organizations subject to on-going investigations should continue dialogue with authorities, while keeping an eye out for any potential derogations or extensions of time-limits issued by local regulators.

2. Enforcement in connection with the pandemic

a) Data protection rights are not “in quarantine”

Data protection authorities have been clear that individuals’ concerns of privacy and protection of their rights remain paramount. Recent debates over a need to put privacy rights “in quarantine” to effectively fight the virus are likely to heighten data subjects’ concerns over potential infringements.

An increase in data subject access requests is not unlikely particularly with the development of COVID-19 related apps or employer health-screening measures. Care should be taken to accede to such requests within the timeframes normally expected, to avoid complaints being filed with local authorities.

b) Closely monitor and comply with quickly evolving guidance and regulation

In response to the pandemic, governments and data protection authorities have introduced a spate of new measures: specifying new “best practice” for on-going privacy compliance when adjusting to these difficult times. It is important that organizations endeavor to comply with these recommendations, which could potentially form the basis for future investigations.

Primarily, this means that organizations should regularly monitor any new guidance or regulation, whether mandatory or not, to ensure they stay up-to-date of the latest expectations expressed by their data protection authorities. It is key to check that one's data collection and processing remains compliant as the notion of compliance quickly changes.

c) Anticipate potential investigation measures

No organization is safe from an investigation and appropriate preparations are always a worthwhile investment. Keeping a clear record of processing activities is paramount to ensure compliance with the principles of accountability enshrined in the GDPR. Organizations would be wise to revisit and adapt existing policies and privacy impact assessments, to reflect any newly implemented COVID-19 related measures. This will effectively act as a pre-litigation and pre-inspection strategy, anticipating questions as to the organizational and technical measures taken.

d) Be mindful of increased cybersecurity risks

The increase in remote-working across organizations brings a concomitant increase in cybersecurity risks. Recognizing that the use of personal computers enhances vulnerabilities, organizations planning COVID-19 response and exit strategies should implement clear policies, procedures and training to employees on addressing risks of hacking, phishing and other malicious activities.

Personal data breaches should continue to be reported to authorities within the stipulated timeframes to mitigate the costs of any cybersecurity attack which may occur. Quick action should be taken to restore, anonymize and remove from the public domain any personal data which may be inadvertently leaked.

Failure to do so could result not only in (potentially very substantial) administrative fines, but also data class actions brought on behalf of affected data subjects, who may seek damages even in the absence of any financial losses suffered as a result of the breach. In these times of major and global distress, non-material damages which may be compensated in some jurisdictions – like the UK or France – could reach new levels.




What to do now

Privacy and cybersecurity compliance should not come last: Even if it doesn't seem like your immediate priority, data protection compliance should not be forgotten. Regulators remain attentive and have been clear that their activities will not stop as a result of the crisis.

Don't forget your basics and revisit your data collection and processing policies and procedures to ensure they are up-to-date and properly documented: While the focus for many employers implementing COVID-19 exit strategies may be on local or national laws, it is imperative not to neglect considering and carefully documenting data protection compliance in this arena. Existing organizational policies may need to be updated to include the collection and processing of new categories of personal data. These records will form key evidence in any subsequent investigation or litigation.

Keep apprised of the latest guidance and regulation issued by your local data protection authority and other global bodies: New guidelines and recommendations have been published on a frequent basis since March 2020 – review and consideration of these will help ensure your organization is acting in accordance with current “best practice” in the industry and mitigate risks arising in the future.

Beware of the consequences of a cyber-security attack: Ensure employees are aware of how to report perceived cybersecurity threats, and remain compliant with your responsibilities to react to any breaches of personal data.





Quick read

While competent authorities encourage and support the conduct of COVID-19 clinical trials, data protection rules must still be complied with.

Some flexibility has been granted given the health emergency. Recent EDPB's guidelines help create a more unified approach across the EU. However, Member States' approach may still differ from Member State to Member State.

Emphasis must be placed on the transparency principle and information duties towards the data subjects.

Key privacy considerations for COVID-19 clinical trials

Lilly Taranto, Santiago de Ampuero, Patrice Navarro and Alexander Wenzel

What's the deal?

Due to the rapid spread of the COVID-19 pandemic, the search for an effective vaccine or medicinal products to combat the virus has become a top priority. Consequently, many clinical trials (“CTs”) and studies have been rapidly initiated and organized to fight the disease.

In this maelstrom of political decisions and new CTs initiated on a weekly basis, there is a risk of patients’ and trial subjects’ privacy being disregarded even with heavily regulated CT procedures.

This fast-paced context explains why the EDPB issued the Guidelines on the processing of health data for research purposes in the COVID-19 context.

These Guidelines follow the European Commission’s, the European Medicines Agency’s and the European Heads of Medicines Agencies’ Guidance to sponsors on the management of CTs in this scenario.

What should you take away from the EU Guidance?

Core idea

Data protection rules should not hinder measures taken to fight COVID-19. However, this is no *carte blanche* for not complying with data protection principles and requirements. Sponsors must respect data protection principles and adequately document the risk assessment regarding CTs.

Bases and exceptions for the processing of health data

The EDPB has a very strict approach on consent-based CT processing operations, and its Guidelines provide that sponsors may only rely on consent to process personal data – including health data – if all conditions for a valid consent are fulfilled.

Legitimate interest and public interest may be lawful bases to process trial subjects’ data for COVID-19 trials, if EU Member State legislation provides for derogations to process health

data as per Articles 9.2 (i) and (j) of the GDPR (i.e. respectively, the public interest and where processing is necessary for scientific research purposes). Sponsors need to assess national laws as such derogations must be based on Member State law, and approach may vary between Member States.

Importance of transparency and information duties

Emphasis must be placed on the transparency principle and information duties towards the data subjects, including when data is not directly collected from them. Different actors intervene in CTs and individuals must be duly informed about the processing of their data. The COVID-19 crisis fosters a higher degree of data sharing, but should not hinder the provision of the appropriate information to data subjects.

Other principles to consider

Regarding the purpose limitation principle, there is a “compatibility presumption” on further or secondary processing activities for scientific research purposes which may prove particularly useful in the context of COVID-19 CTs.

Related to data minimization and storage limitation principles, true anonymization becomes relevant for further use of the scientific results.

Dealing with health data – even where pseudonymized – entails implementing reinforced security measures.

Moving data outside the EU

Given the extraordinary and “temporal” circumstances, more flexibility is granted to international data transfers. The Guidance acknowledges the possibility of relying on GDPR derogations to transfer personal data to “non-adequate” countries. For the duration of this crisis, organizations may rely on the following derogations: (i) transfer necessary for important reasons of public interest, and (ii) data subjects’ explicit consent.

Examples of measures taken by affected countries

Germany

The German authority for medicinal products (BfArM) has published guidance concerning the management of CTs during the pandemic. It provides recommendations to sponsors on how to manage CTs during COVID-19, including the use of remote monitoring and telemedicine for CTs, in compliance with data protection requirements.

France

The French Data Protection Authority (CNIL) has also issued guidance in this respect. Under French law, research on health data, including in the context of CTs, may be subject to an authorization from the CNIL, in case the CT does not meet the requirements of a so-called “reference methodology”. The CNIL announced giving priority to the review of COVID-19 research authorizations in case they do not conform to one of the reference methodologies.

UK

The ICO has set up the coronavirus information hub to help navigate data protection. The ICO states that its approach is pragmatic and proportionate, and that enforcement action will take into account the pandemic and challenges faced by organizations.

The Health Research Authority (HRA) issued guidance on how to use patients’ data in the context of the pandemic. It has reiterated that consent is not required to process patients’ data, and follows the EU Guidance’s approach.

Fast track approval processes for COVID-19-related CTs reduces approval times to a couple of days and new mCTAs are in place.





What to do now

Despite the emergency, sponsors should be careful when designing the study protocol and setting up their data processing operations. A country by country assessment is recommended to consider local health and data protection regulations.

Sponsors should consider the appropriate legal basis for processing patients' data in each EU Member State and assess the risk to participants in clinical trials during COVID-19 (for instance, upon their data sharing, remote monitoring activities, or telemedicine).





Quick read

Medical institutions, disease control and prevention centers, and enterprises in China collecting and processing personal data in relation to COVID-19 are required to follow *the Cyber Security Law of the People's Republic of China, the PRC Law of Prevention and Treatment of Infectious Diseases, the Provisions on Responses to the Public Health Emergencies, the Personal Information Security Specification, and the Notice of Effectively Protecting Personal Information and Using Big Data to Support Joint Prevention and Control* issued by the Office of the Central Cyberspace Affairs Commission.

In China, express consent from data subjects is not required for medical institutions and disease control and prevention centers authorized by the National Health Commission under the *PRC Law of Prevention and Treatment of Infectious Diseases and the Provisions on Responses to the Public Health Emergencies* to collect personal data in order to contain COVID-19.

Express consent from data subjects is still required for collecting and processing of personal data related to COVID-19 by other enterprises.

In Japan, regulatory authorities have issued guidance on how businesses might implement countermeasures to COVID-19 without violating Japan's privacy laws.



Privacy lessons from Asia

Mizue Kakiuchi, Kyle Reykalin, Jessie Xie and Lan Xu

I. China

As the novel coronavirus disease spreads across the world, creating new epicenters, perhaps is now an opportune moment to look back at the lessons learnt from China in relation to privacy protection and its practice. During the COVID-19 outbreak, medical institutions, disease control and prevention centers, and enterprises in China collected and processed the personal information of their employees, customers, patients, and persons who were suspected or confirmed to have COVID-19, including such as name, mobile number, temperature, whereabouts, personal health information, residential address, and family relations (“**COVID-19 Data**”). This COVID-19 Data is deemed to be the sensitive personal information in China.

Although consent has been the fundamental legal basis for the handling of personal data in most scenarios, consent from the data subjects is not required by medical institutions or the disease control and prevention centers which are expressly authorized by Chinese laws and regulations to collect the COVID-19 Data. However, such exemption does not apply to other entities.

When enterprises collect and process COVID-19 Data, they are required to:

- a) Inform the data subjects of (a) the purposes of data collecting and processing, (b) scope and method of data processing, (c) the recipients to whom the data may be disclosed, and (d) period for which the information will be stored.
- b) Seek express consent from the data subjects before collection and processing.
- c) Adopt strict management and technical protection measures to prevent theft and unauthorized access to data. For example, enterprises should provide training to the relevant personnel and require them to sign a commitment to respect confidentiality and apply necessary techniques, such as data de-identification and encryption to secure the data.
- d) Keep and maintain accurate records of sharing of personal information, including the date, scope and purpose of such sharing, as well as basic information about the data recipients. (e.g. in the case of sharing to vendors and contractual parties).
- e) Follow the principle of data minimization and avoid collecting excessive data.
- f) Not disclose the COVID-19 Data to the public without prior express consent of the data subjects, unless: (i) otherwise authorized by the authorities to be made public for containment of COVID-19; and (ii) data masking techniques have been applied.

II. Japan

Japan has not introduced any legislation specific to COVID-19 privacy concerns. However, elements of Japanese privacy law are still relevant to COVID-19 issues.

The Act on the Protection of Personal Information (“**APPI**”) generally divides personal information into two categories: (1) personal information and (2) special care-required personal information (“**SPI**”). SPI, which includes most health-related information, has certain additional protections, including that the data handler must, in general, obtain consent of the data subject prior to obtaining, as well as transferring, SPI.

SPI may include, for example, an employee’s medical history. Generally, if an employee voluntarily provides this information, further express consent would not be necessary, as consent is implied. Consent would not be deemed as implied if the information will be handled in a way beyond the scope of what the employee would reasonably expect. If an employee will not consent, certain exceptions may apply. Exceptions specific to COVID-19 issues may include cases:

- g) Existing laws and regulations.
- h) Where there is a need to protect a human life, body or fortune, and it is difficult to obtain consent.
- i) Where there is a special need to enhance public hygiene or promote fostering healthy children and it is difficult to obtain consent.
- j) Where there is a need to cooperate in regard to a government organization, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining consent would interfere with the performance of government duties.

On 2 April, the data protection authority issued its guidance entitled *Handling of personal data for preventing the spread of Novel-Coronavirus (COVID-19) disease*. The guidance makes it clear that companies may generally announce that an employee has been infected or may have contacted a person who is infected with COVID-19, including by providing the employee’s name, both internally and externally to customers or other third-parties who might be at risk even if it exceeds the scope of the purpose originally specified. Consent is not required if it is necessary to disclose the information in order to prevent secondary infection, to continue business activities, or to enhance public hygiene.

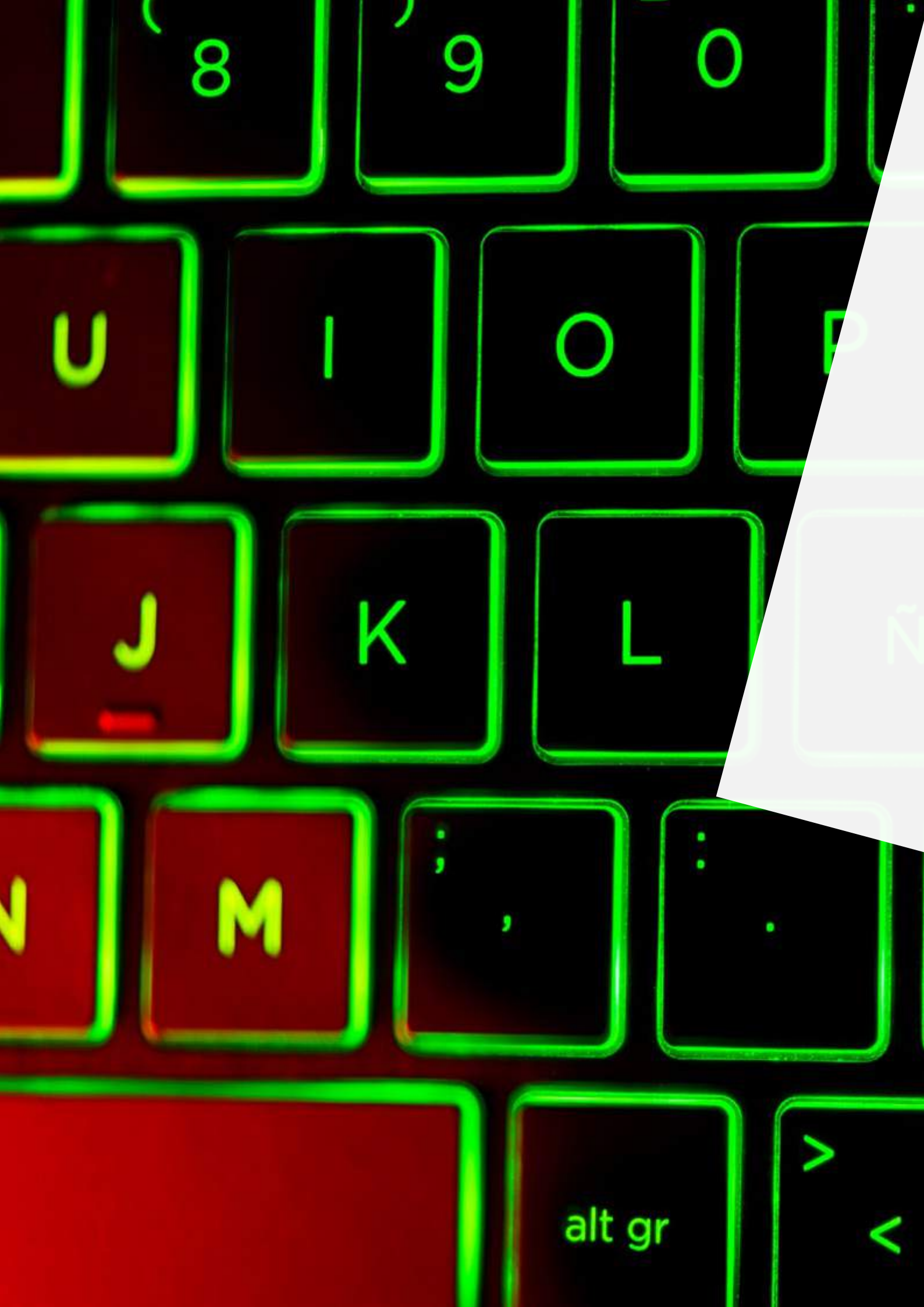


What to do now

Closely monitor the fast-evolving guidelines and policies at both national and local level to assess all data privacy requirements in the context of COVID-19, and adapt any necessary corporate policies to ensure compliance.

Ensure any policy aimed at stopping the spread of COVID-19 involving employee data falls within one of the grounds identified by the law or the regulators.





8

9

0

U

I

O

P

J

K

L

N

N

M

;

:

Shift

alt gr

>
<

About us

We have had a team specializing in privacy and cybersecurity for over 25 years. Today, Hogan Lovells has one of the largest and most experienced privacy and cybersecurity practices in the world, spanning the United States, Europe, and Asia.

We offer:

- A true specialist practice focused on privacy, cybersecurity, data protection, and information management.
- Thought leadership and close involvement in the development and interpretation of the law.
- Seamless global coverage through our well established and continuously developing team.
- Advice which goes beyond achieving compliance and adds value to the information held by organizations.
- A one stop shop for all of your privacy and cybersecurity needs around the globe.

Key contacts



Eduardo Ustaran
Co-head, Global Privacy and Cybersecurity Practice, London
T +44 20 7296 2000
eduardo.ustaran@hoganlovells.com



Marcy Wilder
Co-head, Global Privacy and Cybersecurity Practice, Washington, D.C.
T +1 202 637 5600
marcy.wilder@hoganlovells.com



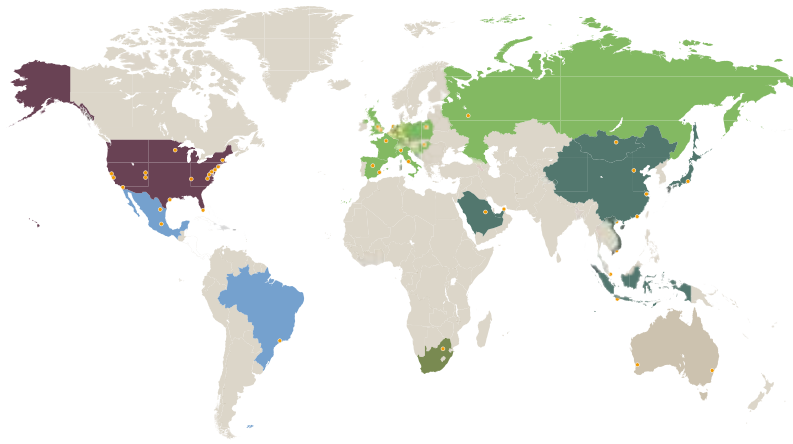
[@HLPrivacy](https://twitter.com/HLPrivacy)



pausa

No matter where, we're there.

Our global Privacy and Cybersecurity team



Asia



S. Gong
Beijing

J. Wei
Beijing

R. Zou
Beijing



E. Low
Hong Kong

M. Parsons
Hong Kong

S. Keen
Singapore



P. Cheng
Shanghai

H. Imai
Tokyo

Europe



B. Blok
Amsterdam

J. Bodewits
Amsterdam

J. Janssen
Amsterdam

W. Olieslagers
Amsterdam

C. Van Dam
Amsterdam

R. Zagers
Amsterdam

H. Boland
Brussels

F. Roy
Brussels

E. Wright
Brussels



L. Bresler
Dusseldorf

S. Kreutzmann
Dusseldorf

T. Mengler
Dusseldorf

C. Bosch Rivero
Dusseldorf

M. Schreiberbauer
Dusseldorf

M. Thiesen
Dusseldorf

C. Kesting
Frankfurt

I. Bruns
Hamburg

H. Hanssen
Hamburg



C. Tinnefeld
Hamburg

M. Anthofer
London

A. Ford-Cox
London

N. Fulford
London

P. Garcia
London

E. Hughes
London

E. Hughes
London

H. Jackson
London

K. McMullan
London



S. Rudgard
London

A. Rutherford
London

S. Salhi
London

L. Taranto
London

E. Ustaran
London

D. Whitehead
London

L. Williams
London

L. Badin
Madrid

S. Castellanos
Madrid



G. Gállego
Madrid

C. Lazaro
Madrid

V. López
Madrid

C. Regalado
Madrid

J. Robles
Madrid

P. Suarez
Madrid

N. Gulyaeva
Moscow

D. Bamberg
Munich

A. Gremmelmaier
Munich



A. Hess
Munich

D. Huber
Munich

M. Pflueger
Munich

S. Schuppert
Munich

J. Beaufour
Paris

E. Drouard
Paris

M. Goudiaby
Paris

O. Kurochkina
Paris

A. Ligot
Paris



G. Le Cordier
Paris



C. Le Roux
Paris



P. Navarro
Paris



J. Schwartz
Paris



D. Taylor
Paris



F. Zannotti
Paris



M. Berliri
Rome



M. Colonna
Rome



G. Mariuz
Rome



M. Masnada
Rome



E. Kacperek
Warsaw



W. Wolosiuk
Warsaw

Latin America



I. Carvalho
Brazil



F. Hernández
Arroyo
Mexico City



F. de Noriega
Olea
Mexico City



A. Rumualdo
Mexico City



M. Yáñez V.
Monterrey



A. Brown
Denver



C. James
Denver



A. Lillie
Denver



J. Black Livingston
Denver



V. Iliadis
Los Angeles



M. Maddigan
Los Angeles



S. Yonerkura
Los Angeles



A. Awad-Farid
New York



P. Marta
New York



J. McGovern
New York



D. Merck
New York



M. Larner
Northern Virginia



J. Talotta
Northern Virginia



C. Cox
Silicon Valley



M. Amer
Washington, D.C.



M. Bianchi
Washington, D.C.



M. Brennan
Washington, D.C.



B. Cohen
Washington, D.C.



A. Cooke
Washington, D.C.



J. Denvil
Washington, D.C.



D. DePass
Washington, D.C.



C. Essig
Washington, D.C.



J. Flamant
Washington, D.C.



M. Gitomer
Washington, D.C.



A. Golay
Washington, D.C.



B. Hall
Washington, D.C.



L. Hardy
Washington, D.C.



J. Hirsch
Washington, D.C.



D. Hogan
Washington, D.C.



S. Jin
Washington, D.C.



D. Kaplan
Washington, D.C.



M. Kisloff
Washington, D.C.



M. Levine
Washington, D.C.



S. Loughlin
Washington, D.C.



M. Mason
Washington, D.C.



P. Otto
Washington, D.C.



R. Patel
Washington, D.C.



H. Pearson
Washington, D.C.



M. Perna
Washington, D.C.



E. Ramirez
Washington, D.C.



F. Raso
Washington, D.C.



A. Holt Ryan
Washington, D.C.



N. Salminen
Washington, D.C.



M. Scheimer
Washington, D.C.



M. Sneed
Washington, D.C.



A. Sura
Washington, D.C.



T. Tobin
Washington, D.C.



M. Wilder
Washington, D.C.



C. Wolf
Washington, D.C.



R. Woo
Washington, D.C.

North America

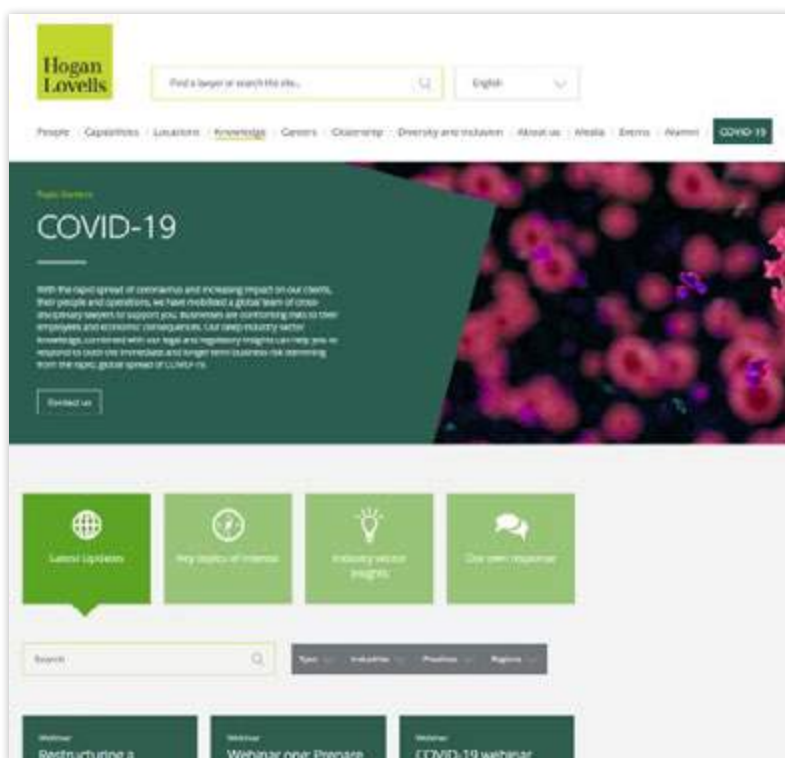


COVID-19 resources

With the rapid spread of coronavirus and increasing impact on our clients, their people and operations, we have mobilized a global team of cross-disciplinary lawyers to support you. Businesses are confronting risks to their employees and economic consequences. Our deep industry sector knowledge, combined with our legal and regulatory insights can help you to respond to both the immediate and longer term business risk stemming from the rapid, global spread of COVID-19.

Last month, we launched a COVID-19 Global Guide to help Hogan Lovells clients navigate the rapidly changing government, legal and regulatory landscape of COVID-19. The guide covers 17 topics ranging from privacy and cybersecurity, to the impact on litigation, across 20 countries. You can access the COVID-19 Global Guide [here](#) and this [short video](#) will help you navigate the content available.

To stay up to date with our latest updates, visit our COVID-19 Topic Centre: www.hoganlovells.com/en/knowledge/topic-centers/covid-19





EUROPE

SPAIN

MOROCCO

ALGERIA

LIBYA

EGYPT

NIGER REP.

MAURITANIA REP.

MALI REP.

GUINEA

UNITED KINGDOM

IRELAND

NORWAY

FRANCE

GERMANY

ITALY

SPAIN

TUNISIA

LIBYA

EGYPT

NIGER REP.

MALI REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

AUSTRIA

SWITZERLAND

GREECE

TURKEY

ALGERIA

LIBYA

EGYPT

NIGER REP.

NETHERLANDS

LUXEMBURG

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
Sao Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices

Legal Services Centre: Berlin

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2020. All rights reserved. 1207800_0520