Volume 2, Issue 3
May 2020
dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

Brazil
Impact of the postponement of the LGPD on organisations
6

Interview with
Professor Joe Cannataci, UN Special Rapporteur on the Right to Privacy
10

Compliance guidance
Petruta Pirvan discusses the need for a global privacy program for international organisations
24

IS COVID-19 THE NEW GDPR?

Eduardo Ustaran discusses the impact of COVID-19 on the data protection compliance of organisations and governments 4

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTRIBUTORS TO THIS ISSUE

Eduardo Ustaran, Hogan Lovells
Eduardo Ustaran is Global co-head of the Hogan Lovells Privacy and Cybersecurity practice and is widely recognised as one of the world's leading privacy and data protection lawyers and thought leaders. With over two decades of experience, Eduardo advises multinationals and governments around the world on the adoption of privacy and cybersecurity strategies and policies.
Based in London, Eduardo leads a highly dedicated team advising on all aspects of data protection law – from strategic issues related to the latest technological developments such as artificial intelligence and connected devices to the implementation of global privacy compliance programs and mechanisms to legitimise international data flows.

Ruth Boardman, Bird & Bird LLP
Ruth is a Partner and co-head of Bird & Bird's International Privacy and Data Protection Group
Ruth has extensive experience advising a broad range of organisations on data privacy matters and advises on the data protection aspects of new products or services and on commercial arrangements involving personal data. Ruth also helps when there has been a personal data breach, and advises clients on their dealings with data protection authorities, with the European Data Protection Board, and with those involved in passing new data protection legislation. Ruth works with clients in many sectors - including online providers and ad-tech, new technology and electronics, life sciences, financial services including payments, creative industries (such as music and film), automotive and sports.

Felipe Palhares, Palhares Advogados
Felipe is a partner at a Brazilian law firm specialized in privacy and data protection. Felipe advises multinational corporations in doing business in Brazil and complying with Brazil's data protection laws either by structuring privacy programs from scratch or adapting GDPR compliance programs to Brazil's privacy framework. Felipe is the first Brazilian national to have been recognized as a Fellow of Information Privacy and the only Brazilian national to have earned all privacy and data protection certifications from the IAPP. Felipe holds an LL.M. degree in corporate law from New York University and a Data Protection Officer Professional Certificate from Maastricht University. Felipe is admitted to practice law in Brazil and in New York. He also has extensive experience with litigation and M&A transactions.

Stuart Beraha, Latham & Watkins
Stuart Beraha advises leading Japanese and international companies on sophisticated cross-border technology and intellectual property transactions. Mr. Beraha helps clients developing, acquiring and exploiting technology, content, brands and other intellectual property. He advises on a full spectrum of licensing and partnering transactions, including technology, software, and content licenses and assignments, and e-commerce, search, and other Internet-related transactions. Mr. Beraha draws on more than two decades of experience in the Japanese market, and possesses a nuanced understanding of the interplay between practices of domestic and global companies. Prior to joining Latham, he was a partner at a leading international law firm in Tokyo.

Takaki Sato, Latham & Watkins
Takaki Sato is an associate in Latham & Watkins' Tokyo office and a member of the firm's Corporate Department. He advises multinational companies on the adoption of privacy strategies and policies. He regularly advises US tech companies on data privacy issues arising from transactions relating to ad tech and platform businesses. He also represents Japanese and non-Japanese companies in regulatory filings arising from data breaches.

Professor Joe Cannataci, United Nations
Prof. Joe Cannataci was appointed UN Special Rapporteur on the right to privacy in July 2015.
He is the Head of the Department of Information Policy & Governance at the Faculty of Media & Knowledge Sciences of the University of Malta. He also holds the Chair of European Information Policy & Technology Law within the Faculty of Law at the University of Groningen where he co-founded the STeP Research Group. A UK Chartered Information Technology Professional & Fellow of the British Computer Society, he also continues to act as Expert Consultant to a number of international organisations.

Petruta Privan, A.P. Moller-Maersk
Petruta is the Global Data Privacy Compliance Manager at A.P. Moller-Maersk. Petruta joined Moller-Maersk in October 2018 and has managed the data privacy compliance efforts in the company since then. Previously, Petruta was part of the Global Data Privacy team in Accenture where she specialised in cross-border data transfers and mobile applications, among others.

Image production credits
Cover / page 4 image: XXX
Page 6 image: Photoman / Essentials collection / istockphoto.com
Page 12-13 image: wsfurian / Signature collection / istockphoto.com
Page 20-21 image: Raylipscombe / Signature collection / istockphoto.com
Page 26-27 image: dem10 / Signature collection / istockphoto.com
Page 28-29 image: CJ_Romas / Essentials collection / istockphoto.com
Page 30-31 image: BrianAJackson / Essentials collection / istockphoto.com
Page 32-33 image: shulz / Signature collection / istockphoto.com

Data Protection Leader is published bi-monthly by OneTrust Technology Limited, Dixon House, 1 Lloyd's Avenue, London EC3N 3DS

Website **www.dataguidance.com**

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Editor **Eduardo Ustaran**
eduardo.ustaran@hoganlovells.com

Managing Editor **Alexis Kateifides**
akateifides@onetrust.com

Editorial **Victoria Ashcroft**
vashcroft@onetrust.com

OneTrust DataGuidance™ Content Team
Mona Benaissa, Souzana Georgopoulou, Alexander Fetani

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

4 Editorial: Is COVID-19 the new GDPR?
By Eduardo Ustaran, Partner at Hogan Lovells

6 USA: Coronavirus implications for privacy and security
By Sonia S. Siddiqui, from Grant Thornton LLP, and Hamza Jilani, from W.L. Gore & Associates

10 Privacy Talks with Ruth Boardman, Partner at Bird & Bird

12 Brazil: Impact of possible postponement of LGPD
By Felipe Palhares, Partner at Palhares Advogados

15 Key takeaways: COVID-19 European and U.S. cybersecurity issues

16 Regulator Spotlight with Professor Joe Cannataci, UN Special Rapporteur on the Right to Privacy

20 International: Transferring data between Japanese companies and the UK post-Brexit
By Stuart Beraha and Takaki Sato, from Latham & Watkins

24 Thought Leaders in Privacy with Petruta Pirvan, Global Data Privacy Compliance Manager at A.P. Moller-Maersk

26 Turkey: Personal Data Protection Authority announces Binding Corporate Rules
By Burcu Tuzcu Ersin, LL.M. and Burcu Güray, from Moroglu Arseven

28 News in Brief: Macau, EU, and USA
Produced by the OneTrust DataGuidance Content Team

34 Key takeaways: A practical guide to breach notifications: Australia, EU, and California

EDITORIAL

Eduardo Ustaran Partner
eduardo.ustaran@hoganlovells.com
Hogan Lovells, London

Justifying the use of data, particularly when it involves health data, is an essential aspect of justifying the measure itself

Editorial: Is COVID-19 the new GDPR?

COVID-19 is a killer infectious disease and the world is looking for a solution. Our collective hope is that with the help of science, such a solution will arrive in the coming months. In the meantime, global leaders are putting their efforts into managing the devastating effects of the latest coronavirus roaming the world. This has led to the deployment of draconian (but justifiable) measures and the implementation of rigorous 'track, trace, and test' strategies. As our liberties and our lives as we knew them are put on hold, there is a troubling question that is becoming more pressing by the day: will privacy be one of COVID-19's victims? Fortunately, the evidence is robust: Unlikely.

The fight against COVID-19 is often positioned as a trade-off between public health and privacy. In other words, we are supposed to be prepared to sacrifice some of our privacy for the sake of saving lives, possibly including our own. But far from framing this as a binary zero-sum choice, the world is witnessing concerted efforts to ensure that privacy and cybersecurity are part of the solution. 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. To that effect, many organisations and governments are adopting the most advanced data protection practices and making compliance efforts not seen since the preparations for the coming into effect of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').

With that in mind and when engaging in measures such as temperature screening, COVID-19 testing, immunity passports, contact tracing apps, or anything along those lines, the right approach is to ensure that their deployment addresses the following key requirements:

- **Transparency** – No matter how sophisticated the intended data processing, explaining what this involves in a clear and comprehensive way, at the outset, and through the most appropriate interface is key.
- **Legal basis** – Justifying the use of data, particularly when it involves health data, is an essential aspect of justifying the measure itself.
- **Purpose limitation** – This is primarily about assertive governance aimed at identifying all possible uses of data and making sure they are legitimate and justifiable. While flexibility is needed, clarity of purposes is a must.
- **Data minimisation** – Only the data that is truly relevant and limited to deliver what is necessary in relation to the purposes of the measure must be collected and used.
- **Accuracy** – This is a critical requirement not only from a legal perspective, but to ensure the effectiveness of the measure and to generate trust among the population.
- **Storage limitation** – In order to avoid function creep and excessive use or oversharing of data, data must not be kept for longer than is necessary for the purposes for which the processing is required.
- **Data security** – The integrity and confidentiality of the data must be maintained through appropriate security measures, which in many cases will rely on encryption and solid access controls.
- **Rights of individuals** – Given that individuals should ultimately be in control of their own data, there must be appropriate mechanisms and procedures for individuals to have access to their own data and exercise their rights of deletion and portability.
- **Protection against unjustified government access globally** – The data must always be guarded against the risk of disproportionate and potentially indiscriminate access, particularly when it is stored globally and subject to the jurisdiction of different countries around the world.
- **Accountability** – There must be a system of privacy and cybersecurity governance that supports a 'Privacy by Design' approach and relies on the involvement of data protection officers and the use of Data Protection Impact Assessments.

None of this is as difficult as developing a COVID-19 vaccine or finding a cure, but considering these issues and getting them right is essential for the effectiveness of the actions being undertaken to stop the spread of the disease. Like with the GDPR, the motivation for getting this right should not be to avoid stratospheric fines, but to achieve the prosperity we all seek in a safe and responsible way.

USA: Coronavirus implications for privacy and security

The COVID-19 ('Coronavirus') pandemic has disrupted business operations on an unprecedented scale, forcing companies to adapt almost every facet of their organisation within a short timeframe. Sonia S. Siddiqui, from Grant Thornton LLP, and Hamza Jilani, from W.L. Gore & Associates, discuss the range of privacy and security issues which have been brought into focus as a result of this and how these might be best faced by employers.

The Coronavirus outbreak has forced companies across America to respond quickly to complex shifts in their operational capabilities - from health checks on site to ensuring the continuity of business via a shift to working from home for employees. With these challenges come added privacy complexities, as companies are grappling with challenges presented when providing access to sensitive personal information, as well as potentially sharing sensitive personal information, which may cause concerns relating to employee privacy.

Employee monitoring: keeping the workplace safe

As Americans face anxiety and uncertainty, essential businesses and their workers are in an even more precarious situation: how to keep the workplace safe. Given the current limited testing capabilities in the US and based on guidance from the Centers for Disease Control and Prevention ('CDC') to quarantine and isolate as much as possible, for many essential businesses the issue of workplace safety is intertwined with employee monitoring through health checks at work.

Evaluating workplace safety requires businesses and employees to not only monitor the cleanliness of workspaces but to also monitor employee health in a way that many have never had to before. From an employee's temperature to their health conditions, businesses are faced with collecting and evaluating health-related information without clear guidance. In the US employers dealing with the collection and use of health-related information should look to requirements from the U.S. Equal Employment Opportunity Commission[1], the Americans with Disabilities Act ('ADA')[2], the Family Medical Leave Act ('FMLA')[3], and the Genetic Information Nondiscrimination Act ('GINA')[4] which, amongst other things, all stress maintaining the confidentiality of employee health information.

As companies rush to continue to operate their businesses amid Coronavirus, employers often assess employees in an *ad-hoc* manner, and need to develop a process to not only share the information with those at risk but also protect such information. Without the appropriate infrastructure to manage health-related information, businesses are in a difficult situation trying to balance workplace safety with employee privacy. Employers dealing with these issues should define rules for why the health information is needed, what information minimally would will fulfil that need, and once that need is met how would the health information be disposed of.

Ultimately, companies must find ways to grapple with risks associated with this pandemic while balancing privacy. In doing so, companies should consider

their communications in the context of federal laws and workplace safety.

Company communications amid Coronavirus

Given current projections in the US, employers may have employees infected with Coronavirus. It is important to consider the channels through which an employer may become aware of a positive case and how other employees find out. Establishing these protocols is paramount to enable safe working environments while limiting unnecessary disclosures of personal information. Many organisations have crisis teams whose expertise should be leveraged to enable consistent and focused messaging.

There are a few key considerations that organisations should keep in mind during this time:

- companies should consider establishing a Coronavirus task force or project management team to centralise the effort and management of risks associated with the collection, handling and disclosure of personal information and disclosures of affected employees. Centralising decision making with a set group like a project management office will mitigate potential delays in responses and also allow for consistent messaging across the company;
- if collecting additional personal information at this time, particularly sensitive information such as health or medical data, companies should consider providing notice prior to collection. Companies should limit the use and storage of this data to health and work site safety, and de-identify the data if possible;
- companies should consider establishing communications plans to manage this situation. This may include situations where a company is made aware of the exposure directly from the affected employee, or indirectly. Prepared responses may provide including letting the the employee know that their exposure will be communicated to other employees but that their identity will not be shared. The CDC has also advised employers to inform fellow employees of their possible exposure while maintaining an individual's confidentiality;
- if collecting additional personal information at this time, particularly sensitive information such as health or medical data which may be necessary, companies should consider asking for authorisation prior to collection. Companies should limit the use and storage of this data to health and work site safety, and de-identify the data if possible; and
- companies should be aware of federal laws such as the ADA, GINA, and FMLA that have confidentiality requirements relating to medical and health data of employees. Companies should take steps to avoid involuntary disclosure of confidential information to supervisors and managers.

Privacy and security challenges with a remote workforce

In today's world of widespread connectivity and global travel, few anticipated that anything could bring the world to come to a near halt as Coronavirus has done. Within the span of a few months, Coronavirus has caused governments to seal their borders, restrict movement of citizens, and cancel group gatherings, entire professional sport seasons, and more. Companies have sought to adjust to these times by adopting policies to allow for employees to work from home in situations where they can.

With many employees working from home, they are no longer working under the security of their employer's protected networks. This leaves organisations vulnerable to cyber threats.

Privacy has become a major issue, with record numbers of businesses and individuals relying on videoconferencing platforms during the Coronavirus pandemic. Notably, Zoom has received criticism due to issues with security and privacy. The platform has been a target of multiple instances of organised harassment termed Zoombombing. Citing privacy and security issues, many companies, organisations, and schools have limited the use of Zoom. Such videoconferencing platforms may introduce unwanted vulnerabilities.

Companies have come to realise that while many of their employees may in theory be able to continue work from home, they are not prepared for the IT-realities of managing hundreds, thousands or even tens of thousands of remote workplaces. Even companies that felt prepared due to their business continuity planning are now discovering that such plans may not be adequate for these times. Issues such as virtual private network overload, limited licenses for conference lines, and capacity issues with such lines are thematic.

With many employees working from home, they are no longer working under the security of their employer's protected networks. This leaves organisations vulnerable to cyber threats. In the past two months alone, companies have reported phishing attacks with emails purporting to provide information on Coronavirus, or requests to pay invoices.

By establishing and reviewing preparedness plans and policies, companies can begin to think with their IT departments about security vulnerabilities that have come to light in the recent disruptions. Additionally, companies can use this moment as an opportunity to converse with their IT departments about network limitations and resources to support remote work.

Ultimately, companies and their employees are all adjusting to remote work. To ensure that employees are only using devices they are authorised to use for work purposes and storing and transferring files appropriately, companies should offer refresher training and send out reminders linking employees to privacy policies, acceptable use policies, and other relevant policies and procedures. This can be an opportunity to bring that level of awareness to employees.

The Coronavirus pandemic has wreaked havoc on the world and created a need to react and respond to complex privacy issues related to employee monitoring, internal and external communications, and working remotely. The privacy challenge here is to prevent the erosion of privacy rights in the face of these difficult issues. Employers should strive to limit the collection and disclosure of personal information as much as possible and clearly define rules for how that information can be used, protected, and for how long it should be retained.

Sonia S. Siddiqui Manager
www.linkedin.com/in/soniassiddiqui
Grant Thornton LLP
Hamza Jilani Global Privacy Director
hjilani@wlgore.com
W.L. Gore & Associates, Newark, DE

1. The US Equal Employment Opportunity Commission, Pandemic Preparedness in the Workplace and the Americans with Disabilities, available at https://www.eeoc.gov/facts/pandemic_flu.html.
2. Americans with Disabilities Act, Pub. L. No. 101-336 (relevant provisions codified at 42 U.S.C. § 12112(d)(3)(B); §12112(d)(4)(C)).
3. Family Medical Leave Act, Pub. L. No. 111-84, 123 Stat. 124 (codified 29 C.F.R. § 825.500 (g)).
4. Genetic Information Nondiscrimination Act, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 29 & 42 U.S.C.).

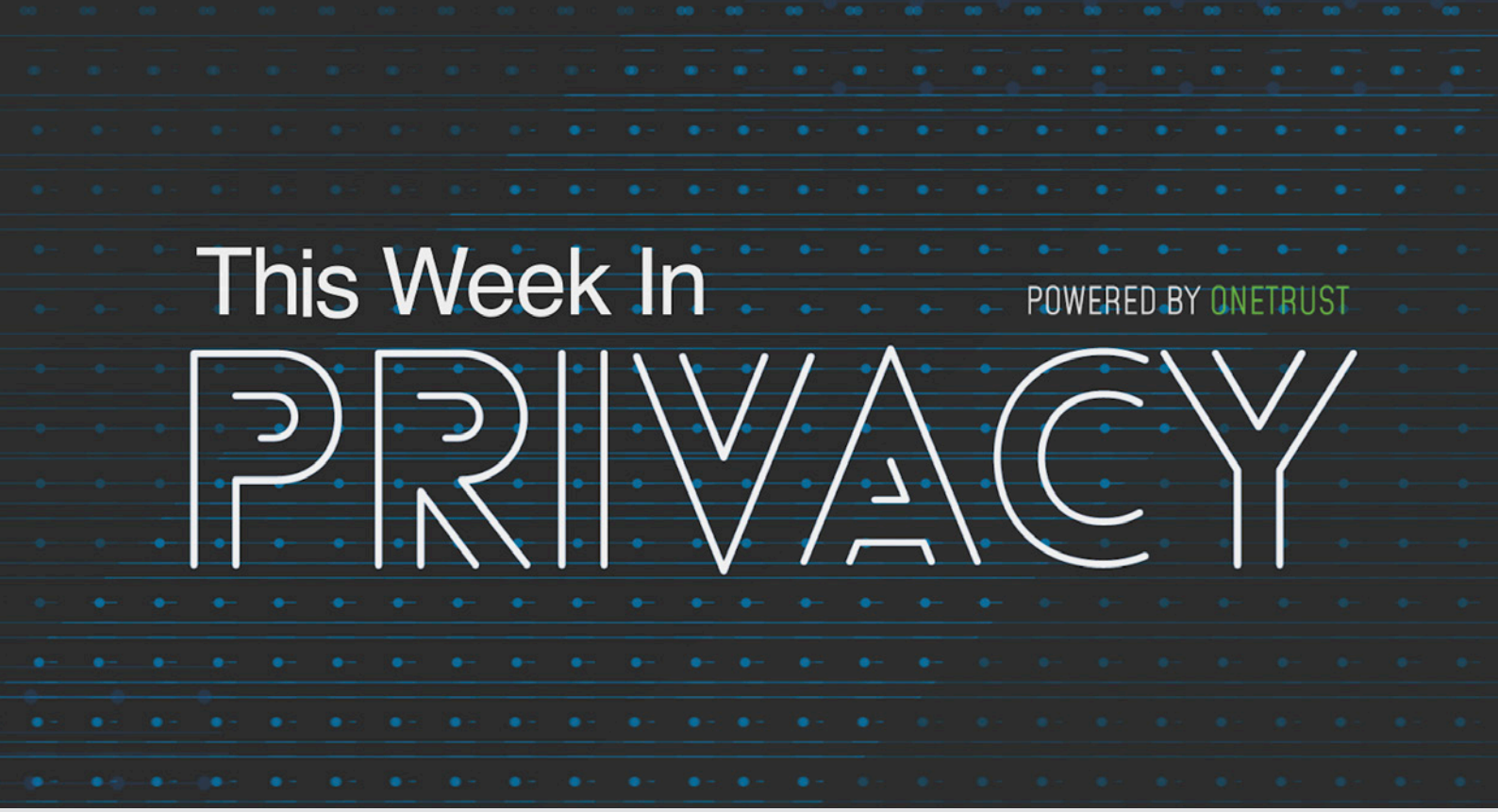
OneTrust Privacy

PRIVACY MANAGEMENT SOFTWARE

Get OneTrust Certified Online

Free for 60 Days | CPE Credits

SIGN UP



This Week In Privacy, powered by OneTrust, is a brand new video series available now. Each week, OneTrust DataGuidance's in-house privacy experts provide you with the top international privacy industry highlights to help you keep up-to-date with the changing regulatory landscape. Head over the OneTrust DataGuidance platform to access This Week In Privacy, and more.

Here are some of the highlights from April 2020.

EDPB guidelines

The European Data Protection Board has continued to release guidance in relation to the COVID-19 ('Coronavirus') pandemic. Following its 23rd plenary session, the EDPB announced that it had adopted new guidelines on the processing of health data for scientific research and guidelines on the use of location data and contact tracing tools.

TCF V2.0 delayed

IAB Europe announced, on 20 April, that the timelines for compliance with the Transparency & Consent Framework v2.0 have been extended in light of Coronavirus.

Hong Kong

In Hong Kong, the Legislative Council and the Office of the Privacy Commissioner for Personal Data published, on 20 April 2020, further discussions on the amendments considered for the Personal Data (Privacy) Ordinance 1997.

Coronavirus

Authorities have continued to publish guidance around privacy and cybersecurity matters related to Coronavirus. The European Data Protection Board recently adopted a letter to the European Commission on the Commission's draft guidance on apps to support the fight against Coronavirus.

New data protection bill in Pakistan

The Ministry of Information Technology and Telecommunications published a new Personal Data Protection Bill and launched a public consultation for its discussion. Comments can be submitted until 15 May 2020.

Privacy Talks

Ruth is a Partner at Bird & Bird and the co-head of Bird & Bird's International Privacy and Data Protection Group. She has extensive experience advising a broad range of organisations on data privacy matters.

OneTrust DataGuidance spoke to Ruth about the current challenges faced by companies due to Brexit, and how the transition period will impact organisations, including in relation to data transfers, lead supervisory authorities, and cross-bored processing.

Current challenges

There are two main areas where we are currently getting questions. One is in relation to data transfers, but the question which is more pressing for organisations at the moment is often to do with the one-stop-shop in the main establishment. What do I mean by that? Well, one-stop-shop is the name that's given to the process under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') whereby organisations can have a streamlined process for dealing with data protection authorities. If an organisation has cross-border processing, then potentially it could end up with investigations in multiple EU Member States. The one-stop-shop provides a streamlined way of dealing with that. So, organisations look to see where their main establishment is and, if they have a main establishment in the EU, then the data protection authority ('DPA') which is competent for that main establishment is the DPA that liaises with the organisation. So rather than having investigations in multiple Member States, as was the case under the Data Protection Directive (95/46/EC), you just deal with one authority and that authority is then responsible for liaising with other authorities if required. So, it's a much more streamlined process. It's also likely that you only get one enforcement action at the end of this from the lead authority. Now, in order to benefit from this one-stop-shop process, you have to have a main establishment, or an establishment at any rate, in an EU Member State. So, post-Brexit, the question is, will you have an establishment in the EU, and if you have more than one establishment, will it be a main establishment.

A couple of examples might make that clearer. Let's say that you are a retailer in the UK and let's say that you are selling to individuals in the EU. It's apparent that you intend to offer services to individuals in the EU, so you'll be subject to the GDPR on an extra-territorial basis, but if you don't have any EU establishment because you are just a business in the UK, you can't benefit from one-stop-shop because you have to

have an establishment in the EU to benefit from this. So, you will end up with potentially, in the event of an investigation, multiple investigations by data protection authorities.

Let's vary the facts a little bit. Let's say that this retailer has an office in Paris and let's say that there is an investigation into a cross-border processing. In that case, they do have an establishment in the EU so if something goes wrong, then it will obviously have to do with the UK's Information Commissioner's Office ('ICO'), and the French data protection authority ('CNIL') will then act as the lead supervisory authority, so far as the European investigation is concerned. Let's vary the facts a bit more. If the retailer is actually bigger than that and it has establishments in the UK and in Paris, but also in Madrid and Berlin, well in that case, if there is cross-border processing and if there's a need to run an investigation, because it's got multiple establishments you need to look and say, 'Is one of those establishments its main establishment?' and does one of those establishments actually take decisions about personal data processing and does it have the power to have those decisions implemented? If the answer is a 'yes,' and in this example Madrid is taking all of the decisions to do with its customer relationship management system, then Madrid could be the main establishment and the Spanish data protection authority ('AEPD') would be the lead authority. However, if none of those entities is able to take decisions and have them implemented, again, no lead authority.

So, as you have seen, there are quite a lot of complicated alternatives here depending on the way an organisation is structured, but there can be a real advantage to having one authority in the EU which leads on an investigation. Therefore, it's well worth looking into that and seeing if post-Brexit you will qualify for lead authority or if not, and maybe you want to actually give one of your EU establishments the authority to deal with data protection matters so that you can benefit from that.

Data transfers

As from the end of this year, the UK will become a third country so anyone who has presence in the EU where that presence and those organisations are transferring data to them in the UK, they will need to meet the restrictions on data transfer under the GDPR. Now, there is a commitment in the political declaration, assuming all the relevant conditions in the GDPR are met, to try and achieve an adequacy decision. In the same way that Switzerland or Argentina have adequacy decisions, there is a commitment to try and achieve one for the UK.

There is also a commitment the other way around, that the UK also commits that it will seek to facilitate data transfers to the EU. So, if that adequacy decision is adopted in time, then there'll be no disruption to data transfers. If the adequacy decision is not adopted in time, then the UK will be a third country like any other country and organisations who are transferring data, so sharing personal data with organisations in the UK will need alternative measures to ensure adequate protection for the personal data. For example, they might have Binding Corporate Rules in place or they may need Standard Contractual Clauses ('SCCs').

It's just worth bearing in mind that this works two ways, in that most people look at this from the perspective of data transfers from the EU to the UK. Post-Brexit, however, the UK will have its own version of the GDPR that will contain restrictions on transfers of data. The obvious question is, 'what are the rules going to be for those transfers?' If you are a UK organisation and you are transferring data to somewhere else, such as to China, and you're relying on SCCs, will they still be valid? What if you're transferring data to a Privacy Shield organisation or to a country which has been determined to be adequate by the EU, will those decisions all still apply to the UK?

> **Sharing personal data with organisations in the UK will need alternative measures to ensure adequate protection for the personal data**

This is one of the rare areas where data protection lawyers get some good news. The UK government has been committed to try and make this as free from disruption as possible for UK businesses. So, all the methods for data transfers which currently work for the EU, will work for the UK as from the end of 2020. EU adequacy decisions will be recognised in the UK. If you are currently relying on SCCs, even though those clauses refer to European law, they will still be valid in the UK even without amendment. So actually, that's the one bit of good news on data transfers.

Ruth's interview was part of the Privacy in Motion: Brexit series. Visit the OneTrust Dataguidance video for related interviews and more.

www.dataguidance.com/videohub

Brazil: Impact of possible postponement of LGPD

The effect of the COVID-19 ('Coronavirus') pandemic has been felt almost everywhere, not least by data protection and privacy professionals. Felipe Palhares, Partner at Palhares Advogados, discusses how this has led to the likely postponement of Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ('LGPD') in Brazil and how this will impact ongoing compliance preperations by organisations in the country.

The LGPD was to be one of the main legal topics of discussion throughout this year both in Brazil and abroad, due to its extra-territorial effect and the fact that it was expected to enter into force on 16 August 2020, however, in light of the COVID-19 ('Coronavirus') pandemic, the LGPD shall be adversely impacted.

Since its enactment, in August 2018, the LGPD always faced a lack of trust by private companies and public bodies. As Brazil does not have a prior privacy culture, the LGPD was viewed by many as an obstacle to the development of new businesses and technologies and as a barrier for innovation, with commentators saying that the LGPD would probably not be enforced as it was an extremely difficult law to implement.
The grace period between the enactment of the LGPD and the date of its enforcement was initially 18 months, but this was soon extended to 24 months upon the issuance of Executive Order n. 869/2018, signed by the former President Michel Temer, on 27 December 2018.

Over the last year, several companies, mainly international companies and large national companies, started structuring a privacy program to adapt their practices in order to comply with the LGPD and to be fully compliant with the law by its effective date. As a number of these companies already had to comply with international data protection laws, it was easier for them to understand the relevance of compliance with the LGPD and the challenges of the road towards compliance.
Small and mid-size companies, as well as most public bodies, did not follow the same path however. As has often been pointed out, the LGPD is a law that contains many gaps which are left for Brazil's data protection authority ('ANPD') to fill through regulations and guidance. In the lack of such regulation and guidance, the LGPD is even harder to implement, leaving companies and public bodies out in the open and struggling as to how to comply with some of its provisions.

As an example, take the provisions on international data transfers, almost all the scenarios where data can be transferred internationally rely on some action by the ANPD. The recognition of

adequate jurisdictions, as well as Standard Contractual Clauses ('SCC'), specific contractual clauses, Binding Corporate Rules ('BCRs'), seals, certificates, or codes of conduct must be approved by the ANPD. These are the most common safeguards adopted abroad by other countries to allow international data transfers, and in Brazil they cannot be implemented before the ANPD is fully functioning and approves such measures. In the current situation, transferring data abroad could only be performed under more burdensome legal bases, such as where the data subject has given their specific consent set apart from any other clauses or conditions and with prior information regarding the international nature of the processing.

As Brazil does not have a prior privacy culture, the LGPD was viewed by many as an obstacle to the development of new businesses and technologies and as a barrier for innovation

The absence of a fully functioning data protection authority ('DPA') has in fact compromised the initial plans of some companies that decided to wait until its structuring before starting the establishment of their data protection compliance programs. As the ANPD never came to be, the beginning of their road to compliance also never started. Over the second half of 2019, Government officials commented at public events and seminars that the Government was working diligently on enacting a decree structuring the ANPD and on the selection and appointment of the directors of the same, which should have been expected to happen by the end of that year.

At the same time, privacy professionals were expecting that, in the lack of a fully functioning DPA, the President would issue an Executive Order closer to August 2020 determining the postponement of the LGPD. In this instance, huge criticism was expected to arise in response to the presidential action as the Government had since December 2018 the task of creating and structuring the ANPD, and had failed in doing so.

With the spread of Coronavirus and its arrival in Brazil in March 2020, the landscape shifted completely. On 30 March 2020, Brazilian Senator Antonio Anastasia proposed the Bill no. 1179/2020 ('Bill 1179'), which would create a special and transitory legal regime in Brazil under which several laws would be amended in order for some of its provisions to be suspended or altered during the Coronavirus outbreak and until 30 October 2020. Although Bill 1179 mainly focused on changing laws already in force, its second to last provision set forth that the LGPD would be delayed for another 12 months, thus entering into force on 16 August 2021.

It is relevant to note that prior bills related to postponing the effective date of the LGPD had been presented before by other congressmen, but these all failed to move expeditiously through congress and were not expected to be voted by 16 August 2020, when the LGPD should enter into force. There are two reasons why Bill 1179 sets itself apart from the other bills related to delaying the LGPD. The first, and more obvious one, is that the surfacing of the Coronavirus in Brazil dramatically changed the economic scenario everywhere, thus making it harder for companies to invest in compliance with the LGPD when they are facing more severe challenges, such as not going bankrupt in the near future. Secondly, and probably more importantly, is that Bill 1179 is not intended to address only the effective date of the LGPD, on the contrary, it has the goal of bending several laws for a limited amount of time, giving companies and individuals an additional chance to survive the grave economic effects of the Coronavirus crisis. Including a provision related to the postponement of the enforcement of the LGPD in a bill like that is quite different than voting for a bill that only aims to delay the LGPD.

On 3 April 2020, the Senate voted on Bill 1179. After some agreements made between the senators, it was amended in several areas, including the provision relating to the postponement of the

LGPD. The amended language that passed the Senate set forth that most of the provisions of the LGPD will enter into force on 1 January 2021, while the provisions related to the administrative sanctions prescribed by the law will entry into force later, on 1 August 2021. Bill 1179 now has to pass the House and later be sanctioned by the President in order to be converted into law. Although there is no clear indication if the dates above will stand considering that the House may amend the text of Bill 1179 and change it drastically (even by eliminating the provision regarding the postponement of the LGPD), it seems that the LGPD will be delayed somehow. During the remote vote session in the Senate, the congressmen mentioned that an arrangement had been made by the political parties to approve Bill 1179, which should also apply to the House and should lead to the deferment of the law, even though the specific postponement time is uncertain. However, as anything could happen when it comes to politics, we are still far away from actually knowing if the LGPD will in fact be delayed or not.

While postponing the LGPD could be helpful for companies and public bodies that have not started their path towards compliance, it will surely be harmful for Brazil.

To stir the pot even more, on 29 April 2020 President Bolsonaro issued Executive Order no. 959 which delayed the effective date of the LGPD to 3 May 2021. This is a strange and unexpected twist considering that Bill 1179 is still pending and already set forth a possible postponement of the law, making it unnecessary for the President to issue an Executive Order like this at this point. If Bill 1179 does not pass, the President would be able to later issue an Executive Order postponing the LGPD if that was the case. Anticipating such move only creates more chaos as right now Congress will need to decide which of the extensions (if any) will be sustained. According to Brazil's legislative process an Executive Order must be approved by Congress within 120 days of its enactment by the President or it becomes void, thus this new possible deadline of 3 May 2021 is not definitive yet.

If the amended language of Bill 1179 or the language of Executive Order 959 stand, the extension granted to the companies and public bodies to comply with the LGPD will be quite curious and, in a large way, ineffective. One of the arguments for the postponement of the LGPD was that companies would not have the budget to start or continue the establishment of their privacy programs due to the Coronavirus pandemic. As the outbreak of Coronavirus is still ongoing and there is no certainty of when it is going to be resolved, it is hard to imagine that budgets will flourish between August 2020 and January 2021. Moreover, as the ANPD has not been structured yet, the companies that were standing still and waiting for its creation will have to move towards compliance with the LGPD if they want to be ready by this possible new deadline (and even more so if the effective date of the law is sustained as is). Both arguments (lack of budget and lack of a DPA) could be later invoked when we get closer to January, to once again plea for another extension of the enforcement date.

While postponing the LGPD could be helpful for companies and public bodies that have not started their path towards compliance, it will surely be harmful for Brazil. During these challenging times where tracking activities have been deployed by several governments to monitor people infected by Coronavirus, sometimes by completely ignoring privacy rights, it is fundamental to have a data protection law and a DPA in place.

A great example of this need is Executive Order no. 954/2020, issued by the President on 17 April 2020, which requires all telecommunications companies to provide the Brazilian Geography and Statistic Institute with a list of all the names, telephone numbers, and addresses of all their customers, which is being highly debated in Brazil and challenged before the Supreme Court. If the ANPD were already in place, it could be consulted by the Government before such actions were taken. Furthermore, not having a data protection law in force nor a DPA in place damages the reputation of Brazil abroad as a country that cares for privacy and data protection, precluding it from being recognised by the EU or the United Kingdom as an adequate jurisdiction, precluding it from joining the Organisation for Economic Co-operation and Development, as well as preventing domestic companies from contracting with international companies that require its local partners have data protection legislation in place in their respective countries and comply with it.

Regardless of being delayed or not, it is undisputed that the preparations of companies towards compliance with the LGPD have changed due to Coronavirus. Albeit the impact on the companies that are already far in their compliance path, such as those that are now structuring policies and procedures, is relatively low considering that these tasks can be performed quite well even at a distance if people are in constant connection with each other, the first steps of privacy programs are making companies struggle a little more. Performing readiness assessments and conducting data mapping activities remotely is harder, especially when people need to be interviewed for the completion of these tasks. While an in-person setting makes the interviewees feel more comfortable to relay large amounts of information on the data processing activities they perform, and the things they believe they may be doing wrong or inadequately, the same is usually not true for an interview conducted through videoconference applications.

Adapting these procedures in order to make them resemble more closely what used to be the normal standard will be crucial for the success of carrying on with preparations regarding compliance with the LGPD. Privacy and data protection are hot issues in Brazil right now, and companies that fail to uphold such values come under criticism from the media and consumers. Blaming the Coronavirus pandemic for its failure to comply with the LGPD will hardly be an acceptable excuse by data subjects and, when the LGPD comes into force, it will certainly lead to a high level of litigation.

As a privacy program usually takes time to implement, there is no time to lose even if the LGPD is eventually postponed. Understanding the requirements of the LGPD is a great first step in beginning the process of complying with the LGPD, especially because it gives a better idea of which tasks may be performed in-house and which tasks will require retaining outside counsel. For companies that are currently going through extreme situations, even small steps might be later deemed as acceptable towards compliance with the LGPD and viewed as good initiatives that are able to potentially minimise any sanctions to be applied under the law.

Therefore, even during these gruelling times it is important not to lose sight of the value of complying with the LGPD. Although there is doubt if the LGPD will come into force in 2020 or in 2021, there is no doubt about the fact that the LGPD is highly anticipated by the market and it should be highly enforced when it finally becomes effective.

Felipe Palhares Partner

felipe@palharesadvogados.com

Palhares Advogados, São Paulo

WEBINAR

Key Takeaways: COVID-19 European and U.S. cybersecurity issues

On 26 and 27 March 2020, OneTrust DataGuidance was joined by Tim Finan, Cyber Growth Leader at Willis Tower Watson, Bill Hardin, Vice President at Charles River Associates, and Vishnu Shankar and Clay Northouse, Senior Associate and Associate at Sidley Austin, to discuss the cybersecurity issues associated with the COVID-19 ('Coronavirus') global pandemic.

The Coronavirus global pandemic presents unique legal and practical challenges for companies across all industries, including with respect to cybersecurity risks and protections. This webinar highlights the dynamic and evolving cybersecurity threats companies may face and the global legal implications of a cyber breach in this new environment, as well as how companies can reduce these risks and effectively respond to a cyber incident. These key takeaways provide a summary of the webinar and the topics covered.

Key cyber risks in the Coronavirus era

Our speakers highlight that key risks can be put into six broad buckets: vulnerabilities from employee remote access, phishing attacks and scams, removal of data and physical devices from offices, use of unofficial or unsecure communications channels, dispersed incident response decision-makers and IT staff, and supply chain cybersecurity risks. Examples noted within these broad groups include accessing company networks from unsecure home WiFi networks, impersonation of employees to perform fraudulent wire/bank transfers or securities transfers, and increased challenges for an organisation to comply with its regulatory record-keeping obligations.

Security tips when working from home

Guidance issued by the UK's National Cyber Security Centre and the European Union Agency for Cybersecurity provide detailed information regarding issues such as setup of user accounts, remote access via virtual private networks, software usage, and device management. Organisations should seek to implement additional security measures such as multi-factor authentication, the testing and proper management configuration of firewalls, and protocols regarding lost or stolen devices.

Responding to a cyber incident under COVID conditions

Our speakers note that, should organisations suffer a cyber incident, there are three key issues to consider. Firstly, businesses should prepare and test their incident response plans against coronavirus conditions, which include dispersed decision makers. Secondly, it is important that legal privilege is preserved. This may be more challenging under current circumstances given that employees may be communicating on unofficial channels, which may then be discoverable. Thirdly, organisations need to continue to stay abreast of developments regarding breach notification obligations.

Cyber risk insurance coverage

Should any of the potential exposures highlighted in the webinar become reality, our speakers note that existing coverage will likely address these. For example, costs and payments to end a ransomware event would be covered under a policy, as well as those related to forensic investigation, legal counsel, and loss of business income. Having said this, our speakers note that there are potentially two scenarios where coverage may be a challenge: in relation to network access slowdown and where a systems shutdown leads to a business shutdown.

You can now find all our webinars, along with key takeaways, at www.dataguidance.com

Regulator Spotlight

OneTrust DataGuidance met Professor Joe Cannataci, United Nations Special Rapporteur on the Right to Privacy, in October 2019. Professor Cannataci discusses the key takeaways that the organisation have been working towards through the year, as well as sharing his thoughts on recent laws such as the California Consumer Privacy Act of 2018 ('CCPA') and Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ('LGPD'). Joe also discusses the progress his organisation has made in respect to gender and privacy as well as how priorities have shifted during his mandate.

What have been your key takeaways from your international work on privacy in 2019?

If I had to sum it up in two words, one would be diversity and the other is similarity. You can see that, in some countries, there has been great progress in various ways, whether we're talking about Argentina, or we're talking about South Korea, for example. I'm happy to be able to say that there has been progress and, at the same time, you also become very conscious of the impact of history and cultural diversity in the sense that it requires cultural change. Diversity is important too, because you notice that, while the core elements of privacy remain the same, some people have problems which other people don't. If I had to compare South Korea with some jurisdictions in Europe, for example, the in South Korea, they have put in a law where they have cameras in every kindergarten, which some parents are worried about. But actually, the safeguards they have are very good. Then, I compare that to some cities in Europe where, unless you have cameras in the kindergarten, which people can look through and see on their app or on their smartphone what their child is up to, you wouldn't even get customers in that private kindergarten. So, people's reflections on the right to privacy, which is so universal, and the way they react to it, tend to be quite different as you go from country to country.

You also have if have to look at diversity and similarity. The similarity of problems everywhere, in other words, every place I go to when they ask the data protection authority, 'do you have enough resources.?' The answer is, 'hell no.' 'Can you do with more resources?' 'Of course I can.' Another similar problem that people have is whether they can recruit techies with the wages that they can offer and a government department? No. It's extremely difficult to do so. Do you need techies? We can't do without them is the answer. So you see, there are the same similarities coming out when people are looking at the day-to-day problems. The good news, of course, is that privacy is talked about more than ever before. It is a very satisfying thing that there is more awareness, but there is more risk too. We don't have enough time to go individually into all the risks of all the countries, but you also notice those countries which are more sincere than others. Without mentioning the country necessarily, when a country sends me a complaint which I investigate, but then I say, 'OK, let me come along and speak to your officials,' and the country doesn't react in a positive way, I begin to wonder the extent to which they simply seek to instrumentalise the United Nations mandate of the Special Rapporteur on the Right to Privacy.

People's reflections on the right to privacy, which is so universal, and the way they react to it, tend to be quite different as you go from country to country

What are your thoughts on recent laws such as the CCPA and the LGPD?

I'm delighted, it helps me sleep well at night. It's good to see that more and more countries outside of Europe are taking privacy more seriously and taking the obligation to introduce rules which are more or less going in the same direction. They're not necessarily identical but they're going in the same direction. Europe was leading in some ways for some time, but in effect, you also see other countries taking an innovative approach in some regions while also meeting the same problems. That California, for example, has introduced a law delights me because California is around the fifth or sixth biggest country in the world in terms of gross domestic product. As a state, it's larger than the UK, and the UK is part of the G7 and California is not. The United States is part of the G7, but at this moment in time, the leadership of the United States doesn't seem, at the federal level at least, to be taking privacy with the same level of importance that the Californian assembly is. This is not to say that there are no privacy protections in the United States, far from it. The United States is one of the leading countries and I am pleased to see that over the past three years, the United States has made lots of progress even in appointing people who were in there before. And coming up with new initiatives.

Once again, the Italians have a saying which can be understood to mean that all the world is one small village or a country but really you have the same problems everywhere. So, if you were to ask the Brazilians, 'have you had the same problem as other countries?' In other words, in getting down and nominating your data protection commissioners, setting it up, seeing which ministries are going to share finances, or whatever the actual grind of setting up a data protection authority. I'm sure that the representatives would be honest and tell you, 'yes.'

How has your work with respect to gender and privacy progressed?

We've continued to take that forward in a structured and

REGULATOR SPOTLIGHT

Professor Joe Cannataci, UN Special Rapporteur on the Right to Privacy

systemic manner and last year we launched the first online consultation on gender. We had actually started that in 2018, but by this time last year we had already started receiving responses to our online consultation to the extent that in, March of 2019, I was able to publish an interim report on the subject which is to be found annexed my annual report to the Human Rights Council. As a result, we will then send that out for further feedback, and in fact now it's leading to an in-person consultation rather than an online consultation, and that would be organised at New York University. So it continues to be my plan that after these two very intensive days of panel after panel, speaker after speaker, and hopefully lots of audience engagement, we would be able to come up with a revised document which would include recommendations which I would then be presenting to the UN Human Rights Council in Geneva.

We obviously are very interested about the implications, impact, and safeguards which need to be introduced in the cyber area where children are concerned

How have your priorities changed over the course of your mandate?

When I took up my appointment as the first special rapporteur on privacy in 2015, I was lucky to have a clean slate as nobody had been working on the brief from a UN point of view before that, except for a report which had been published slightly previously, and so I had to draw up my list of priorities. My list of priorities consisted of five priorities at that moment in time that I was working on, including, understandably enough for a mandate which was born out of the Edward Snowden revelations, security and surveillance, and then health data, Big Data and open data, the personal use of personal data by corporations, and better understanding of privacy as a priority.

So, we've worked systematically on all of these and I published a report on Big Data and open data in 2018. Health data, I hope, will help people move forward in a coherent vision in that very important sector of sensitive personal data. The same applies to gender, to link it up with what we were saying before.

Children, I hope to be presenting to the Human Rights Council in March of 2021, which means that between now and 2021, we hope to continue our current research and our current background work. In terms of the background work, we've prepared the table of contents identifying issues, and we've started speaking to experts in the field, but also consulting with other people who are concerned. For example, the United Nations Convention on the Rights of the Child which was launched in 1989, its committee and the committee responsible for administering that multinational treaty has launched a consultation on what they call the general comment on basically updating the interpretation of the treaty to modern times. So, we've got involved with that consultation.

We obviously are very interested about the implications, impact, and safeguards which need to be introduced in the cyber area where children are concerned. I'm very concerned about that. I think that the area is extremely complicated to sort out because it's not only children, but you also have the guardians of children and the guardians of children expect to have a say until the children are 18, and the children are not exactly in agreement with that. If you simply had to ask how many kids allow their parents to befriend them on Facebook or any other social media and notice that the children's independence starts well before the age of majority 18 or 21, or whatever it may be in some countries. And, of course, inspired by the Convention on the Rights of the Child which attempts to give children a say in what's going on, it's quite tricky because even in those countries which have been innovative enough, like the United Kingdom, for example, introducing the concept of age appropriate behaviour and age appropriate content to be precise into the law and now in the publication of the code on age appropriate content by the Information Commissioner of the United Kingdom, which is a statutory obligation placed upon the Information Comissioner's Office, it's very interesting to see from my point of view how much of that is actually going to be effective, what are the new obligations being placed on companies, and would they be effective.

So, consulting with the companies about that, and how much of that is simply just pious intentions and how much of that, if it's effective, is a good idea, and can we borrow as a part of the way forward, not only for Europe but for the rest of the world.

Watch Joe's interview, along with other insight from regulators, at www.dataguidance.com

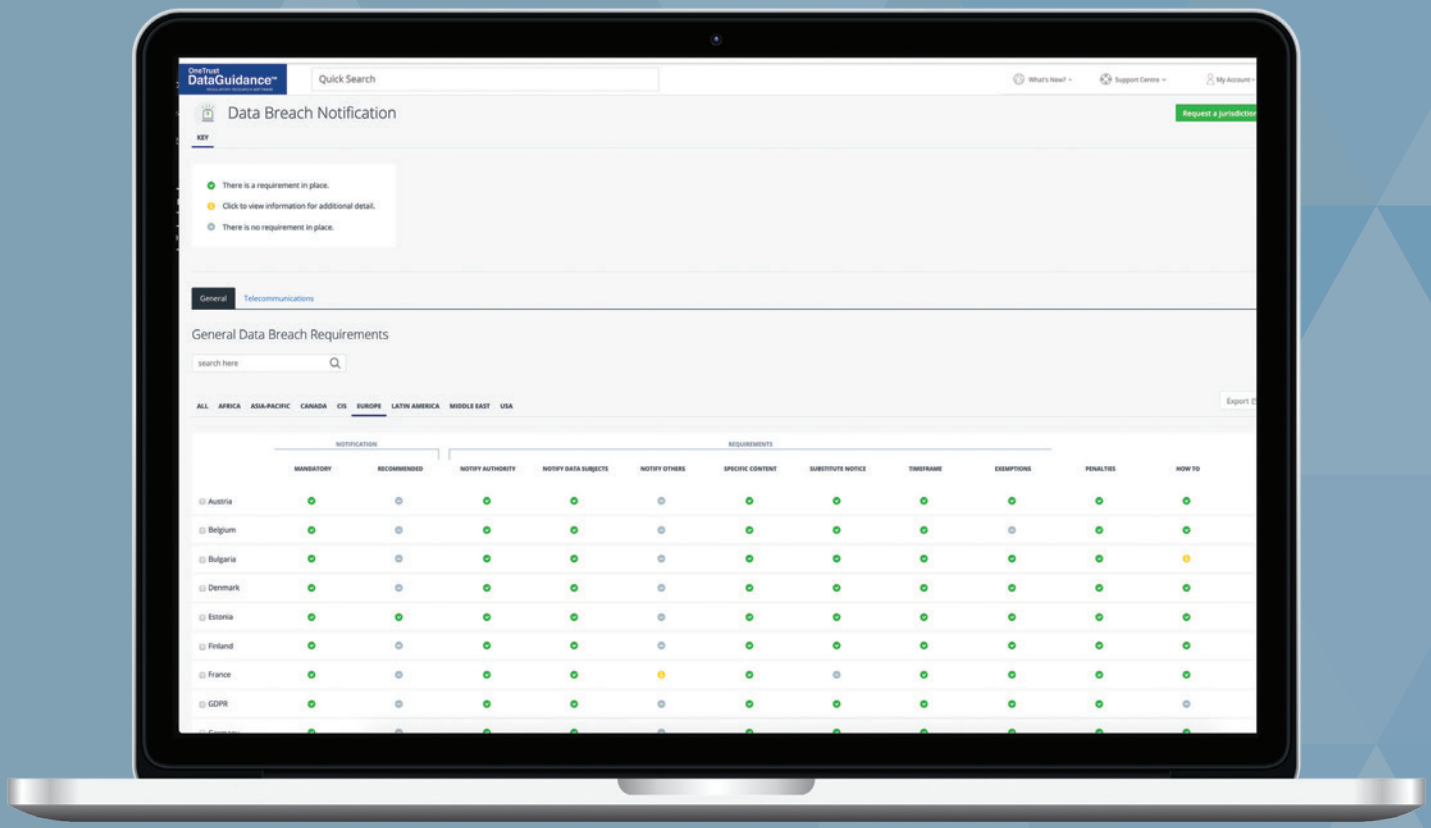
Global Regulatory Research Software

40 In-House Legal Researchers

500 Lawyers Across 300 Jurisdictions

With focused guidance around core topics, Comparison Charts, a daily customised news service and expert analysis, OneTrust DataGuidance provides a cost-effective and efficient solution to design and support your privacy program

- Legal Guidance & Opinion
- Law Comparison Tools
- Breach & Enforcement Tracker
- Ask-An-Analyst Service



SCAN TO ACCESS
FREE TRIAL
Use your camera or a QR code reader

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

International: Transferring data between Japanese companies and the UK post-Brexit

While Brexit is likely to cause uncertainty in many areas, the continuity of data transfers for countries such as Japan who have attained a positive adequacy decision from the EU is largely ensured. Stuart Beraha and Takaki Sato, Partner and Associate respectively at Latham & Watkins, discuss the legal framework governing personal data transferred from the UK to Japan and how the gaps between the two countries' data protection rules are made up for in this process.

Brexit

On 31 January 2020, the UK exited the EU. While there are many issues likely to be affected by Brexit, this article focuses on the effect of Brexit on the UK's data protection regime, particularly in relation to the requirements applicable to Japanese companies with respect to transfers of personal data between the UK and Japan. The Japanese data privacy regulatory authority, the Personal Information Protection Commission ('PPC'), is primarily concerned with whether Brexit is likely to result in changes to the existing Japan-EU regime with respect to cross-border transfers of personal data. In the lead up to Brexit, the Japanese regulators kept a close eye on the UK regulatory authority's policy with regard to such data transfers and determined how Japan would treat cross-border transfers of personal data between Japan and the UK in the post-Brexit world.

Framework governing data flow between the EU and Japan - to be imputed to Japan-UK data flow

In Japan, the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2016) ('APPI') includes regulations addressing cross-

border transfers of personal data from Japan to foreign countries. The data privacy regulation of the EU, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), similarly has regulations addressing cross-border transfers of personal data from the European Economic Area ('EEA') to non-EEA countries. A 'mutual adequacy agreement' has been adopted by Japan and the EU in order to allow smooth cross-border data flows between the two. Under this agreement, the EC allows personal data to be transferred from the EEA to Japan and, accordingly, EEA member states are included by the PPC on Japan's 'white list' of countries to which personal data transfers are permitted. In the post-Brexit era, the UK and Japan will each retain the mutual adequacy arrangement vis-à-vis the other. Below, we discuss how the UK-Japan mutual adequacy arrangement works and its implications for the transfer of personal data between the UK and Japan.

Personal Data to be transferred from the UK to Japan

The transfer of personal data by a UK company to a Japanese company is permitted under UK law due to the mutual adequacy arrangement. The Japanese recipient company is then obligated to handle such transferred personal data in compliance with the APPI. In addition to the generally applicable Japanese regulations, the PPC has established additional Japanese data privacy guidelines which address the handling of personal data transferred from the UK to Japan pursuant to the UK-Japan mutual adequacy arrangement ('the Adequacy Guidelines'). The Adequacy Guidelines, which simply apply the EU-Japan mutual adequacy arrangement to the UK, impose additional obligations on the Japanese recipient with respect to handling personal data transferred from the UK to Japan ('UK Personal Data') in order to fill certain gaps that would have existed under the generally applicable Japanese regulations in relation to the personal data protections that apply in the UK.

> **In the post-Brexit era, the UK and Japan will each retain the mutual adequacy arrangement vis-à-vis the other**

For purposes of this discussion, the GDPR currently constitutes the personal data protections applicable in the UK. In the post-Brexit era, the GDPR will continue to apply in the UK during a transition period lasting until the end of 2020. Although the GDPR will no longer apply to the UK upon expiration of this transition period, the UK government has nevertheless stated that it intends to incorporate the terms of the GDPR directly into UK data protection laws with little change. References made below to the GDPR refer collectively to both the GDPR itself (i.e. the EU regulation with applies in the UK until the end of 2020) and the version of the GDPR to be adopted by the UK. The additional obligations that apply to UK Personal Data are summarised below.

Additional special categories of personal data

The GDPR imposes a higher standard of protection to categories of personal data considered particularly sensitive. The APPI adopts a similar framework, under which sensitive data may not be collected without the consent of the relevant data subject. Although the GDPR and APPI structures are similar in this respect, the categories of sensitive personal data are narrower under the APPI than they are under the GDPR. Specifically, unlike the GDPR, the APPI does not recognise

data revealing a data subject's 'sex life,' 'sexual orientation,' or 'trade union membership' as falling within the special category of sensitive personal data.

The Adequacy Guidelines address this gap by recognising as sensitive UK Personal Data revealing a data subject's 'sex life,' 'sexual orientation,' or 'trade union membership'. A Japanese recipient of these types of UK Personal Data therefore must treat such UK Personal Data in compliance with the Japanese regulations applicable to the special category of sensitive personal data.

When a Japanese company transfers non-UK personal data to a foreign company, the Japanese company must enter into a contract with or ensure binding corporate group rules apply to the foreign data recipient

Eliminating exceptions to right to request deletion, correction, or non-use/disclosure of personal data

The APPI entitles data subjects to require a company processing his/her personal data to delete, correct, cease to use, and cease the disclosure of the data subject's personal data. However, this right does not apply to personal data that has been retained by the processing company for less than six months. The Adequacy Guidelines remove this six-month minimum retention period with respect to UK Personal Data. Accordingly, the data recipient is obliged to satisfy such requests from data subjects with respect to UK Personal Data, regardless of how long the UK Personal Data has been retained by the recipient.

Imputed restriction on purpose of use

The APPI does not explicitly state that a data recipient's use of personal data must be limited to the purpose of use specified by the data provider.

To obtain consistency with the GDPR, the Adequacy Guidelines obligate a Japanese recipient of UK Personal Data to use the UK Personal Data only for the purposes permitted by the data provider transferring the UK Personal Data to the Japanese recipient.

Higher standard of protection for anonymised data

The APPI includes regulations addressing the creation and handling of 'anonymised data.' For the process of anonymising personal data, a particular technological processing method is required, which includes the removal of certain items/records/cells, generalisation, and micro-aggregation. Anonymisation also requires the removal from personal data of descriptions and identifiers by which a specific individual can be identified. Under the APPI, the party creating anonymised data is permitted to retain data that could allow the anonymisation process to be reversed, as well as the removed personal data, if the creating party takes security measures to prevent data breaches with respect thereto.

Under the GDPR, however, this retention will not be permissible. To obtain consistency with the GDPR as to anonymised data, the Adequacy Guidelines therefore require the creating party to completely delete such forms of data.

Additional requirements for onward transfers of received UK Personal Data

The APPI's regulations regarding cross-border transfers of personal data from Japan to foreign countries require the party transferring the data to obligate by contract or, in the case of a foreign recipient that is an affiliate of the transferring Japanese company, by binding group corporate rules. Due to the similarity of these requirements to the Standard Contractual Clauses ('SCC') and Binding Corporate Rules ('BCRs') adopted under the GDPR, the foreign recipient would process transferred personal data in compliance with substantially the same obligations as would apply to a Japanese company under the APPI.

In the case of onward transfer of UK Personal Data from a Japanese data transferor to a foreign data recipient, the additional requirements explained in the above must be included in the applicable Japanese SCC/BCRs.

Personal data to be transferred from Japan to the UK

As discussed above, when a Japanese company transfers non-UK personal data to a foreign company, the Japanese company must enter into a contract with or ensure binding corporate group rules apply to the foreign data recipient. The mutual adequacy arrangement removed this requirement with respect to cross-border transfers to UK companies. As a result, Japanese companies are able to transfer personal data to UK companies as if such a personal data transfer takes place entirely within Japan. As a general matter, under the APPI, domestic personal data transfers are subject to the following restrictions:

- in principle, the data provider must obtain the data subject's prior consent;
- in practice, data providers rely on statutory exemptions from the 'consent collection' regime, with statutory exemptions applying where:
  - personal data is transferred in the course of consignment of handling of such personal data (e.g. providing customer lists to a marketing company for the purpose of a direct mailing campaign, or providing employee profile data to a payroll company for the purpose of enabling salary payment services);
  - personal data is transferred in the course of a corporate merger or certain other business transfer transactions; or
  - personal data is shared pursuant to a 'Joint Utilisation' structure meeting certain procedural requirements; and
- in theory, a data provider may satisfy the consent requirement via an opt-out structure. This approach is however comparatively uncommon in practice (only 186 enterprises across the entire country as of the end of March 2019), partly because the associated procedural requirements are onerous. This is in particular due to the fact that the procedure includes a requirement to file with the PPC, which appears unattractive to data providers.

Stuart Beraha Partner
stuart.beraha@lw.com
Takaki Sato Associate
takaki.sato@lw.com
Latham & Watkins, Tokyo

OneTrust DataGuidance™

REGULATORY RESEARCH SOFTWARE

GLOBAL REGULATORY RESEARCH SOFTWARE TO HELP YOU BUILD AND MAINTAIN YOUR COMPLIANCE PROGRAM

Same day support with a global contributor network of over 500 lawyers and 40 in-house legal researchers, covering 300 jurisdictions.

REGULATORY RESEARCH

Track and interpret requirements for implementation of the GDPR, CCPA, LGPD and hundreds of other privacy laws globally

MATURITY & PLANNING

Assess and demonstrate your organizational readiness against global governance frameworks

PROGRAM BENCHMARKING

Benchmark your organizational preparedness against companies of similar size, industry and region

AWARENESS TRAINING

Meet regulatory requirements and instill a privacy first culture with 30+ role-based training modules

Get started today with a **FREE Trial**

INTERVIEW WITH:

Petruta Pirvan Global Data Privacy Compliance Manager at Moller-Maersk

THOUGHT LEADERS IN PRIVACY

OneTrust DataGuidance spoke with Petruta Pirvan, Global Data Privacy Compliance Manager at Moller-Maersk in February 2020. Moller-Maersk is a Danish business conglomerate with activities in the transport, logistics and energy sectors and has been the largest container ship and supply vessel operator in the world since 1996. Petruta shares her opinions on upcoming trends and technologies that are likely to have an impact on the data privacy landscape, as well as her recommendations for others trying to comply with a range of emerging global privacy laws.

What emerging global privacy laws are you tracking and why?

As we are a global business and I am the data protection officer ('DPO') for the entire organisation, of course we are focusing a lot on the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and everything that is coming on top of the GDPR in terms of guidelines from authorities and decisions of the courts of the EU, for example. Of course, we cannot ignore the emerging legislation coming out from countries outside of the EU, specifically because the type of business which we are doing, which is global business. We keep a sharp eye on what's happening in California, with the California Consumer Privacy Act of 2018 ('CCPA') and in the rest of the US. We are obliged to know and acknowledge the new legislation emerging out of India, we are obliged to keep an eye on whatever happens in China or in Africa, and other areas if we have localisation requirements in certain jurisdictions and certain countries. We have to know everything, and we have to keep an eye on each development. This is why it's so important to have a legislative software program to help us.

How do you manage and adapt your global privacy program to the continued regulation and legislation which is emerging?

It is important for companies that are conducting global businesses like us, and this is what we are currently doing, to have a program that is structured around the type of legislation that mostly apply to the business. For example, if your operations are centred into the EU then maybe it's a good idea to have a GDPR-centric approach for your compliance program. So, that is how we are managing. We have a backbone program based on the GDPR privacy principles and we are trying to apply the same principles to non-EU countries observing similar data protection standards and adequacy status, and trying to give the same rights to data subjects from non-EU countries as we do for the data subjects inside of the EU.

What recommendations do you have for others that also have to comply with the myriad of data protection laws around the world?

First of all, I think it's very important to know the business that you operate in. That's hugely important and is the first step. If you know exactly the business that you operate in and the way your company conducts business, what type of data is relevant for that type of business, what type of data subject, what type of data flows, and so on, so this would be the first step. Then, go to the next step and have a program in place, define a program. Of course, if you are headquartered in the EU then you can pick the regulation that you want to apply to your business. Then it is very important also to observe if certain specific legal requirements apply to your business because you might want to base your type of processing on those legal requirements and that would be your legal basis for the majority of your processing. It is very important that you know that. Once you acquire that type of knowledge and you feel confident that you know exactly what applies to your business, and what type of legal requirements and regulations you need to adhere to, then you can define your program and you can choose how it operates. The best part is that the principles which are laid down in Article 5 of the GDPR are basically the foundation of the majority of the privacy legislations that are emerging right now worldwide, so that makes it easier for global companies.

> **What we can do is to make sure that we mitigate risks, we identify risk, we communicate within the company, and we find ways and resources to minimise these risks**

Another thing that makes it easier for these type of businesses is if you have a centralised operation because if you have a centralised operation, then you can have a centralised compliance program when it comes to compliance with data privacy and you can, for example, implement an automated type of data mapping for your personal data, and you can identify the sources where you have personal data and then acquire a tool that would automatically do the mapping process for you. You can go a step further and you can integrate your Data Protection Impact Assessment processing with the records of processing activity with a mapping exercise. Again, if you have this centralised operational approach, this would allow you to simplify the process.

Also, I would advise any DPO who, like me, is taught in a new industry, to take time at the beginning and make sure that they have processes and policies in place. If they don't have they need to make sure that they draft those processes and policies. That would be also one of the first steps to take, then have a governance, and create a team of people. Depending on the company, this can be a different approach as some companies are investing in resources that are under the management of a DPO or some other companies are investing in resources, which are driven by the DPO efforts. So, for example, as a DPO you can have a team, but not necessarily made of people that would be subordinated to yourself. This is much more complicated because you need to create and build up relationships and build up partnerships, maybe with privacy leads in different geographic areas, or if you are a B2B company like us, with HR privacy leads.

So, it is important to have processes and procedures in place that would help you, for example, tackle how to respond to data subject requests or how to approach a personal data privacy breach. You also need to know if your personal data privacy breach process is embedded in an incident response process, but also have the tools to give the people the signal that if a personal data privacy breach happens, the DPO is the right person to go to as opposed to having different people covering different types of incident, which would confuse people. It is important to pinpoint some basic aspects and then once you cover this, you can go a step further and develop your program, have some training for the people in your team, and have generic training for the company. If you can do that with dedicated modules with different types of functions, that would be perfect. And then also find the functions or the gaps that would require filling with a specific type of training, and you can go there and fill that gap. These are just some common-sense steps that each company can take. I believe it's very complicated to cover such a huge amount of divergent legislation, which are also changing each day, and I believe that you cannot be 100% compliant as a company and no DPO should have such a target, but what we can do is to make sure that we mitigate risks, we identify risk, we communicate within the company, and we find ways and resources to minimise these risks.

Discover how Moller-Maersk leverage OneTrust DataGuidance for their privacy research at www.dataguidance.com

Turkey: Personal Data Protection Authority announces Binding Corporate Rules

On 10 April 2020, the Personal Data Protection Authority ('KVKK') announced its long-discussed Binding Corporate Rules ('BCRs') that allows intra-group data transfers among multinational companies. Burcu Tuzcu Ersin, LL.M. and Burcu Güray, from Moroglu Arseven, discuss the introduction of BCRs in Turkey, and how these will help in the facilitation of cross-border data transfers.

Due to the difficulties in the implementation of cross-border data transfer rules determined under the Law on Protection of Personal Data No. 6698 ('the Law'), the KVKK was expected to issue new rules set for intra-group cross-border data transfers in parallel with the BCR approach accepted under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). Considering the market needs, the KVKK introduced an alternative cross-border data transfer method specific to group companies, which is modelled after the EU's BCR approach.

Current cross-border data transfer regime under the Law

As per Article 9 of the Law, cross-border data transfers shall be based upon the following legal grounds:

- the data subject giving his/her explicit consent; or
- the cross-border transfer being based on one of legal basis stipulated under the Law:
  - the receiving country must be accepted as safe with adequate level of data protection by the Personal Data Protection Board ('the Board'); or
  - if the level of data security is not adequate, then the data controller in Turkey and the data receiver abroad must execute a written undertaking letter (of which the minimum content is already determined by the Board) and seek the approval of the Board for the data transfer.

The list of the countries with an adequate level of protection is yet to be published by the Board, which means at the time of publication, all countries are unsafe in terms of data transfers. The lack of this list causes operational and legal problems for multinational companies, which, necessarily transfer personal data due to organisational, infrastructural, and reporting purposes.

The KVKK stated in its announcement that, although the undertaking letter procedure makes bilateral data transfers easier, it may be inadequate for the data transfers between multinational group companies. The undertaking letter process is indeed insufficient for the intra-group cross-border data transfers by taking into consideration the complexity of the group structure. Besides, in practice, there are drawbacks with the use of undertakings, due to the uncertainty in the implementation of the undertakings for the data transfer under the same corporate group.

Considering the practical needs and corporate group structure, the KVKK has announced the BCRs to overcome the inadequacy in the current implementation of cross-border data transfer rules under the same corporate group, as an alternative method.

What are BCRs?

BCRs are defined as data protection rules

applicable for cross-border transfers that allows multinational group companies, operating in countries with inadequate level of protection, to undertake an adequate level of data protection for the intra-group data transfers.

In the GDPR, BCRs are designed to allow multinational companies to transfer personal data from the European Economic Area ('EEA') to group companies located outside of the EEA in line with the applicable data protection legislation. In parallel with the EU approach, the BCRs introduced by the KVKK would allow multinational companies to transfer personal data from Turkey to a member of same corporate group, located in a country with inadequate level of data protection. BCRs themselves would be considered as a commitment of adequate data protection for intra-group cross-border data transfer in such circumstances.

BCRs must include all general data protection principles and adequate safeguards for protecting personal data in the corporate group. The KVKK issued a statement ('the Statement') on the necessary content of the BCRs, as well as a standard application form on its official websites[1].

Application and approval process

Multinational group companies intending to base their intra-group cross-border data transfers on BCRs need to make necessary preparations for BCRs in line with the Statement and fill out the application form published by the KVKK, and make an application to the KVKK for the approval of their BCR by submitting all documentation related to application.

Data controllers who are located in Turkey within the same corporate group are authorised to make the application before the KVKK. If the corporate group does not have a group member located in Turkey, one of the group members must be authorised to submit the application. The application can be made by hand or via postal service to the KVKK. The documents to be submitted for the application are the application form, the Binding Company Rules text, and all other information and documents related to the BCRs application. If necessary, the KVKK is entitled to request additional information from the applicant.

Applications will be concluded by the KVKK within one year of the official application date. If necessary, the KVKK can extend this period for six months.

If the application is approved by the Board, the KVKK will notify the relevant parties and make an announcement, if necessary. The Board has particularly noted that the BCRs are not approved for an indefinite period. If necessary, the implementation of BCRs can be suspended or terminated by the Board.

Required content

To shed a light on the implementation of BCRs, the KVKK issued the Statement detailing the essential points and content required to be included in BCRs. The elements and principles that are to be found in the BCRs are determined in line with the EU practices to that end. Accordingly, the main matters that need to be included in the BCRs can be summarised as follows:

- Binding nature of BCRs: BCRs need to be binding and contain obligations for each participating member of the corporate group. The corporate group needs demonstrate how the BCRs are made binding on the group members, as well as their employees. Service agreements need to be executed between the data controllers and data processors included into the BCRs. BCRs need to expressly confer rights on data subjects to enforce the rules as third-party beneficiaries and include undertakings of group members to that end. Group members should accept Turkey's jurisdiction over the BCRs. Further information on liability and financial capacity of the group needs to be also expressed within the BCRs. BCRs must be transparent and easily accessible by the data subjects;
- Effectiveness: BCRs must include the following practices:
  - proper trainings and works to create awareness in the group;
  - internal complaint mechanism in the group;
  - regular compliance audits; and
  - appropriate staff for monitoring the compliance with BCR;
- Coordination with the Board: BCRs should contain a clear duty for all group members to co-operate with the KVKK and to comply with the advice of the KVKK on BCRs. Audit rights of the KVKK should also be included in the BCRs;
- Processing and transfer of personal data: BCRs must contain descriptions of the material scope of the BCRs (nature of transferred data, type of data subjects, data categories, transfer methods, legal basis of transfer, and data transfer flows among group members), so that the KVKK could examine the compliance of the processing in third countries. The group structure and contact details of the group members need also to be expressly stated in the BCRs. A contact person would be obliged to keep an updated list of group members participated in the BCRs;
- Mechanisms for reporting and recording changes: BCRs can be modified but they should include a duty to report modifications without delay to all group members and to the KVKK;
- Data protection safeguards: BCRs should include a description of the data protection principles on data transfers from Turkey, including onward transfers in line with the Law. BCRs should regulate participant group members' obligations where a local legislation applicable to a group member prevents the company from fulfilling its obligations under the BCRs;
- Accountability and other tools: each data controller in the group shall be responsible for and be able to demonstrate compliance with the BCRs. In this context, BCR members need to apply appropriate technical and organisational measures, such as maintaining proper records of processing activities in line with the KVKK's instructions and to that end, conduct risk analysis, when necessary; and
- auxiliary information and documents: applicants can insert certain non-mandatory auxiliary information in the BCRs for the ease of application process, such as a reference to the relevant sections of the international conventions signed by transferee countries related to the protection of personal data, or the local legislation on the protection of personal data and the presence of an authorized personal data protection authority of the transferee countries.

The BCRs introduced by the KVKK would allow multinational companies to transfer personal data from Turkey to a member of same corporate group, located in a country with inadequate level of data protection

Conclusion

The introduction of the BCRs by the KVKK is an important step for multinational companies operating in Turkey as, at the time of publication, no countries are accepted as having an adequate level of data protection and available legal solutions for cross-border data transfers (explicit consent, the execution of an undertaking letter, and the approval of the Board) do not meet the needs of multinational companies. In the present state of affairs and in the absence of the KVKK identifying a list of the countries which have data protection adequacy, BCRs are the major alternative legal basis for multinational group companies which require the ability to conduct cross-border data transfers and practices.

Group companies, hereupon, need to examine their operational needs and cross-border data flows carefully and, depending on their specific circumstances, should choose the most appropriate mechanism from the cross-border data transfer alternatives.

Burcu Tuzcu Ersin LL.M. Partner
btuzcu@morogluarseven.com
Burcu Güray Senior Associate
bguray@morogluarseven.com
Moroglu Arseven, Istanbul

Find more Insight articles, written by members of our 500+ network of lawyers and privacy professionals, at www.dataguidance.com/insights

1. Available at: https://www.kvkk.gov.tr/Icerik/6730/PUBLIC-ANNOUNCEMENT-ON-BINDING-CORPORATE-RULES

Macau: GPDP's authorisations exempt data controllers from "mere bureaucratic formalities"

The Office for Personal Data Protection ('GPDP') published, on 15 April 2020, three authorisations in relation to data collection and processing.

In particular, the GPDP highlighted that several public and private entities had been collecting and processing personal data of employees and visitors entering and leaving establishments due to the implementation of measures for the prevention and control of COVID-19 ('Coronavirus'). In this regard, the GPDP issued Authorisation No. 01/2020 on the exemption from notification obligations when collecting and processing personal information of individuals entering and leaving establishments for the purpose of implementing Coronavirus measures. Within the scope of such authorisation, public and private companies can be exempt from notification requirements when processing personal data and, when referring to transfers of personal data, the obligation notification can be completed in a simplified form.

In addition, the GPDP issued Authorisation No. 02/2020 on the exemption from notification obligation when processing data with biometric characteristics for the purpose of identification and attendance, as well as Authorisation No. 03/2020 on the exemption from notification requirements when processing biometric data for security purposes.

Coronavirus exemptions

The GPDP highlighted that many public and private entities had implemented prevention and control measures during Coronavirus. While the Personal Data Protection Act (Act 8/2005) ('the Act') usually requires data controllers to notify the GPDP when engaging in data collection and processing, the three authorisations released by the GPDP provide for a relaxation of such requirements, in order to facilitate the management of the Coronavirus pandemic, as well as the handling of biometric data for specific purposes.

Julia Herold, Partner at DSL Lawyers, told OneTrust DataGuidance, "The Government of Macau has imposed, on every individual entering governmental departments, the obligation to issue a health declaration in which they note if they have a fever, cough, or flu symptoms, and state that they have not left Macau in the last 14 days. This declaration is accessible via a QR code, and individuals have to input their personal data, such as name, date of birth, gender, ID card number, as well as phone number. Authorisation No. 01/2020 exempts data controllers from filing the prescribed notification to the GPDP, but they still have to file a simplified notification form, which is available on the GPDP website. [However], Authorisation No. 01/2020 will cease when the restrictions and preventive measures on the spread of Coronavirus are no longer necessary."

In terms of scope of application, Herold highlights that, "Authorisation No. 01/2020 would mainly benefit governmental departments, such as tax departments, courts, and registry offices, as well as some large institutions where a large number of people visit, including banks and hotels, and that choose to implement the health declaration system. In respect of Authorisation No. 02/2020 and Authorisation No. 03/2020, most private companies

would benefit from these if they wish to implement the collection of biometric data to monitor attendance of their personnel and to exercise access control for the purposes of security."

Biometric data

The authorisations released by the GPDP do not strictly refer to personal information in the context of a global health crisis. Although Authorisation No. 01/2020 consists of a temporary exemption of notification requirements during Coronavirus, the two other authorisations will apply on a long term basis. The type of data collected can include an internal ID number, photo, date and time of entry, employment position, and fingerprints, and its collection will require the consent of the data subject. In addition, Authorisation No. 02/2020 and Authorisation No. 03/2020 note that the collection and processing of biometric personal data should only be used for the specific reasons outlined therein, and should not affect other administrative management, compensations, and benefits to the employees.

Only Authorisation No. 01/2020 will provide controllers with the capacity to disregard a data subject's right to object to the collection and processing of data, if such action is deemed necessary to prevent the spread of Coronavirus

Herold noted that, "Both Authorisation No. 02/2020 and Authorisation No. 03/2020 are unrelated to the Coronavirus pandemic, and are intended to simplify the process of biometric data processing. However, all rights of the data subjects and obligations of the data controllers under the Act remain unchanged. [Authorisation No. 02/2020 applies] for the purpose of monitoring punctuality, [and Authorisation No. 03/2020 applies] for security purposes. [Both authorisations] exempt the data controller from filing a notification to the GPDP, however the processing of biometric data requires the consent of the data subject."

Data subjects' rights

With regards to data protection requirements under the Act, Authorisation No. 02/2020 and Authorisation No. 03/2020 address data retention, and note that the biometric data collected should be deleted within 30 days following the termination of the relationship between the data subject and the data controller. Article 21 of the Act, which addresses the obligation requiring a data controller to notify the public authority, will not apply in cases where one or more of the authorisations apply. However, it is important to note that the right to information, access, objection, and the right to not be subject to automated decisions, as respectively addressed in Articles 10, 11, 12 and 13 of the Act, will remain in force. Only Authorisation No. 01/2020 will provide controllers with the capacity to disregard a data subject's right to object to the collection and processing of data, if such action is deemed necessary to prevent the spread of Coronavirus.

Herold added, "[With regards to Authorisation No. 01/2020], the right of objection is impacted in cases where the health declaration is an obligation under an Executive Order, and without such declaration, the data subject would not be permitted to enter the premises of governmental departments and entities that have implemented the system. However, a simplified notification form will still need to be filed. In respect of Authorisation No. 02/2020 and Authorisation No. 03/2020, [rights to information, access and objection to the processing] are not impacted, given the need to obtain the data subject's consent, they only exempt the controllers from filing notifications which, in reality, were mere bureaucratic formalities. In addition, the security requirements remain the same as required under the Act, as data controllers must implement measures to prevent loss or unauthorised access to the data."

Mona Benaissa Privacy Analyst
mbenaissa@onetrust.com

Comments provided by:
Julia Herold Partner
jherold@dsl-lawyers.com
DSL Lawyers

EU: Commission and EDPB guidance may "limit full potential" of Coronavirus tracing apps

The European Commission ('the Commission') published, on 16 April 2020, a common EU Member States toolbox ('the Toolbox') for the use of mobile applications to support contact tracing during the COVID-19 ('Coronavirus') crisis, as well as guidance ('the Guidance') on the same.

Moreover, the European Data Protection Body ('EDPB') adopted, in its 23rd plenary session, Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak ('the Tracing Guidelines') which aim to clarify the principles governing the proportionate use of location data and contact tracing tools. Olivier Proust, Partner at Fieldfisher (Brussels), told OneTrust DataGuidance, "The Tracing Guidelines adopted by the EPBD show that there is a conflict between two opposing objectives: the protection of public health on the one hand and the protection of privacy on the other [...] The EDPB seems to have accepted that a certain degree of privacy-intrusiveness will be necessary and is unavoidable in the fight against Coronavirus."

Key requirements for tracing apps

Both the Toolbox and the Guidance outline key requirements for tracing apps to ensure that they respect individuals' privacy and comply with data protection regulations. Raluca Puscas, Partner at FILIP & COMPANY, told OneTrust DataGuidance, "One important highlight is that they both address apps which are downloaded, installed and used on a voluntary basis by individuals. In addition, the Toolbox lists other essential requirements of the apps, such as that they must be approved by the national health authority, that privacy is preserved through the use of encryption, and that personal data is deleted as soon as they are no longer needed [...] The Guidance further complements the Toolbox, by setting out several other features and requirements which the apps should meet to ensure compliance with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) ('the ePrivacy Directive'). For example, the apps should be designed in such a manner that the national health authorities (or entities carrying out tasks in the public interest in the field of health) are the data controllers. This is also aimed at ensuring that the underlying policies, requirements and controls are aligned and implemented in a coordinated way."

Individual control over tracing apps

The Guidance notes that individuals remaining in control of their personal data is a determining factor in building individuals' trust in the use of contract tracing apps. One key aspect of this is ensuring that the use of such apps is voluntary. Nancy Kalli, Senior Associate at ALG Manousakis Law Firm told OneTrust DataGuidance, "Tracing apps are not a panacea, as false positives will always occur to a certain degree and they are raising many privacy issues and require vigilance [...] As consent is to be used as a lawful basis for processing, it should be freely given, specific, explicit and informed, within the meaning of the GDPR. As such, the consent should be expressed through a clear affirmative action of the individual excluding implicit consent [...] The users will decide if they wish to provide

additional personal information (e.g. phone number) to the public health authorities in order to get further support and guidance which can be possible via an 'opt-in' option through the apps."

The Tracing Guidelines adopted by the EPBD show that there is a conflict between two opposing objectives: the protection of public health on the one hand and the protection of privacy on the other

Comparing the EDPB's Tracing Guidelines with the Commission's Toolbox and Guidance, in particular with regards to individuals' consent and Member State action, Proust pointed out, "It is interesting to note that the EDPB says that contact tracing apps should be used on a voluntary basis and that it is not necessary to obtain the user's consent. In fact, the EDPB says that the most relevant ground for processing the personal data via the app is the necessity for the performance of a task in the public interest [...] This means that the national Parliaments of the EU Member States will need to pass new laws quickly to allow their national health authorities (and possibly other controllers) to process such data in the public interest."

Location data and data minimisation

Both the Guidance and the Toolbox highlight the importance of data minimisation, noting that using location data is not necessary nor recommended for the purpose of contact tracing apps. Puscas continued, "As the goal of contact tracing apps is not to monitor the movements of the individuals (nor to monitor the enforcement measures), but only to determine proximity (and to guide the individuals on measures to take, such as to self-quarantine), location data does not appear necessary for the purpose of contact tracing functionalities."

In addition, Kalli noted, "Undoubtedly, there is an attempt to strike a balance between data minimisation, as part of privacy in general, and the safeguarding of public interest and public health [...] The EDPB is in favour of a 'decentralised solution' using the Bluetooth low energy communications data (or data generated by equivalent technology) to determine proximity. Data minimisation will affect the development and use of effective contact tracing apps data, as the processing will need to be limited to what is necessary and pre-agreed with the user and, at the same time, effective."

Concluding remarks

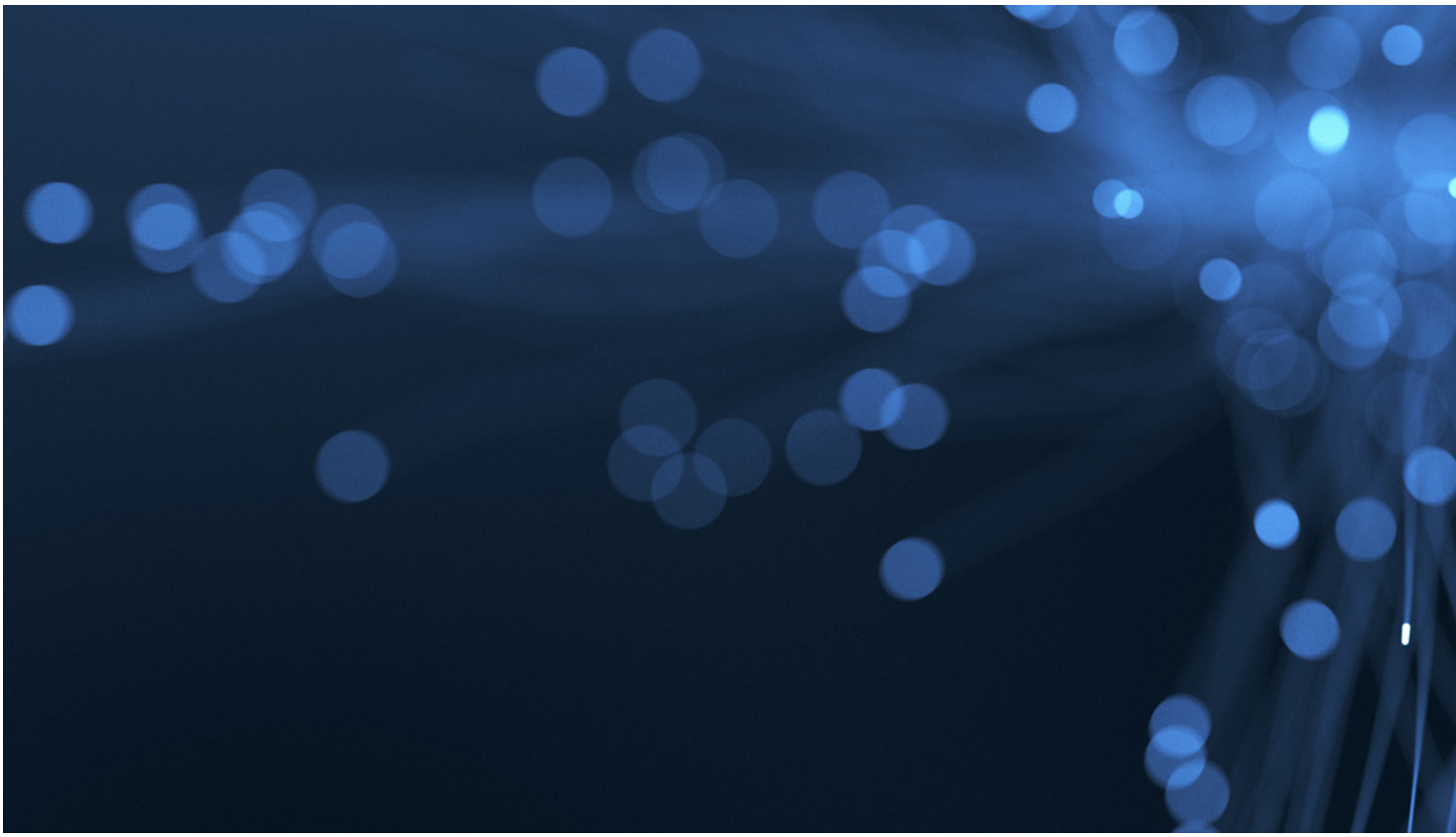
The approaches of the EDPB and the Commission present certain similarities as well as variations with regards to their treatment of tracing apps and their recommendations for the development of such apps to address the Coronavirus crisis. Proust concluded, "Unlike what we have seen in other countries like South Korea, the contact tracing apps that are going to be developed in Europe will be much less intrusive [...] On the one hand, the Commission and the EDPB are imposing certain measures to safeguard the fundamental right to privacy of individuals. But by doing so, they are also limiting the full potential of mobile apps as a tool that can be used to combat the Coronavirus [...] Overall, the EDPB takes a stricter position compared with the Commission and imposes certain limitations. For example, while the Commission recommends using anonymised and aggregated data on the mobility of populations as a means to predict the evolution of the disease and monitor the effectiveness of decision making by Member States' authorities on measures such as social distancing and confinement, the EPDB warns about the risks of relying on anonymised data, namely because it is notoriously difficult to anonymise it."

Souzana Georgopoulou Privacy Analyst

Comments provided by:
Olivier Proust Partner
olivier.proust@fieldfisher.com
Fieldfisher (Brussels)

Raluca Puscas Partner
raluca.puscas@filipandcompany.com
FILIP & COMPANY

Nancy Kalli Senior Associate
nkalli@alg.gr
ALG Manousakis Law Firm



USA: FTC issues blog post on using AI and algorithms

The Federal Trade Commission ('FTC') issued, on 8 April 2020, a blog post ('the Blog Post') on the use of artificial intelligence ('AI') technology and algorithms.

In particular, the Blog Post emphasises that the use of AI tools, whether in health, financial or other industries, should be transparent, explainable, fair, and empirically sound, while always fostering accountability.

Furthermore, the Blog Post recommends that businesses using AI tools should, among other things, provide consumers with information on how automated tools are being used, be transparent when collecting sensitive data, and where necessary, provide consumers with an adverse action notice when making automated decisions based on information from a third-party vendor.

The need to be transparent with AI usage

K.C. Halm, Partner at Davis Wright Tremaine LLP, told OneTrust DataGuidance, "As noted in the FTC guidance, AI is used for a broad variety of tasks in many different parts of our lives. For example, AI tools and systems (such as machine learning, neural networks, computer vision, natural language processing and other methods) power AI applications that make recommendations on investments, credit and housing. AI is also used to help diagnose certain medical conditions, track missing or exploited children, and enhance cybersecurity and network optimiation. And, in this time of social distancing (and associated binge watching) many of us benefit from the video and music content recommendations, dynamic targeted ads and virtual assistants that are all enabled by AI tools and systems."

The FTC stresses the importance of transparency in the use of AI and further highlights that organisations should not deceive customers about AI especially when it is used in the background, providing examples of complaints where users had allegedly been deceived with the use of fake profiles, followers, or subscribers, which led to enforcement actions taken by the FTC.

In this sense, the FTC, recommends that organisations be meticulous when collecting audio or visual data and notes that secretly collecting any sensitive data for an algorithm may also give rise to an FTC action.

Halm continued, "Organisations using AI tools and systems must ensure that they do so in a manner that complies with the many existing laws that may apply, including those involving limitations on the use of biometric data, non-discrimination laws surrounding certain protected classes, such as those involving housing, employment and access to credit. As the FTC points out, existing law reaches the use of AI in a variety of different ways, including when making decisions about lending or credit, when using AI for customer service or other engagement with the public (i.e. through chatbots), and in hiring. Further, a number of new laws have recently been adopted that are likely to slimit certain uses of

AI. For example, in Illinois employers that use AI in the video hiring process are required to provide notice and obtain consent form the interviewee prior to use of the technology."

Steps to implement recommendations

The FTC notes that organisations using AI should think about how to hold themselves accountable and consider looking into the use of independent standards or independent expertise.

In addition, the FTC outlines that before the deployment of AI, operators of algorithms must be able to answer key questions on their data sets and models and how representative they are, the accuracy and predictions of Big Data, as well as whether relying on Big Data would raise ethical or fairness concerns. Moreover, the FTC notes that the use of such outside tools and services are increasingly available as AI is used more frequently, and companies may want to consider using them.

The FTC notes that organisations using AI should think about how to hold themselves accountable and consider looking into the use of independent standards or independent expertise

Halm concluded, "Many companies currently use AI in a manner that is transparent and accountable. These principles are often reflected in internal governance and policy documents that organisations adopt to make sure that their use of AI is ethical and trustworthy [...] To ensure compliance with the FTC guidance and other potentially applicable laws, companies using AI should:

- develop and adopt governance principles or policies to ensure any AI being used is ethical and trustworthy;
- ensure that decisions or outcomes affecting an individual's quality of life, autonomy, or range of opportunity are justifiable and transparent to potentially affected persons; and
- ensure continuing compliance by conducting regular tests and audits of the AI systems to ensure that they are not leading the company to take actions that may be unlawful, biased or discriminatory."

Alexander Fetani Privacy Analyst
afetani@onetrust.com

Comments provided by:
K.C. Halm Partner
Davis Wright Tremaine LLP
kchalm@dwt.com

Follow OneTrust DataGuidance on LinkedIn and Twitter to keep up to date with articles like this, new resources and privacy developments.

WEBINAR

Key Takeaways: A practical guide to breach notifications: Australia, EU, and California

On 27 April 2020, OneTrust DataGuidance held a webinar with Alec Christie and James Wong, Partner and Associate at Mills Oakley Lawyers in Sydney.

Data breaches are a leading concern among multinational organisations. This webinar provides a practical guide to key breach notification requirements across Australia, the EU, and California. Our speakers look at the similarities and differences between requirements across each jurisdiction and outline a step-by-step framework which can be used by organisations to ensure they are prepared for a data breach.

Cyber insurance

In order to plan an effective data breach response plan, organisations can take practical measures. Firstly, our speakers highlight the importance of cyber insurance. This measure could protect organisations against malicious and accidental data security incidents. For example, cyber insurance can assist with fines associated with privacy breaches, and provide assistance with emergency response plans.

Planning a data breach response plan

Our speakers emphasise that an effective data breach response plan is key to managing compliance. This response plan should be tried and tested to be workable for each organisation, and should be able to accommodate and comply with the requirements of each country the organisation operates in. Among other things, our speakers recommend a system which can identify a breach, assess the risk, and then facilitate the appropriate reporting. As highlighted by our speakers, it is not a case of 'if' a data breach will occur, but 'when.'

Security frameworks

Multi-jurisdiction compliance can be supported by using existing privacy standards. In this case, our speakers discuss ISO 27701 and personal information management systems ('PIMS'). As a global standard, these systems are beneficial to avoid starting from scratch when looking at data breach planning. Our speakers also highlight that these standards can be useful when looking at vendors and third-party contracts.

US data transfers on anti-competitive agreements

The GDPR, CCPA, and the Australian Privacy Act all contain data breach notification requirements. However, the content of the notification, and who must be notified can differ between the laws. For example, under the CCPA, the Attorney General must only be notified if a data breach affected more than 500 Californian residents. On the other hand, if the breach meets the relevant requirements, both the affected persons and supervisory authority must be notified under Australian and EU law.

Exceptions to notification requirements

When looking at exceptions to data breach reporting, there are key differences between the CCPA, the GDPR, and the Australian Privacy Act. Under the CCPA, an organisation can use their own compliant notification procedures without the prescribed form or timing. Under the GDPR, notifications to individuals are not necessary if technical and organisational steps have been taken to mitigate the risk to individuals. Similarly, under Australian law, an organisation does not need to provide any notification if serious harm is mitigated before the harm occurs.

How OneTrust DataGuidance helps

OneTrust DataGuidance™ is the industry's most in-depth and up-to-date source of privacy and security research, powered by a contributor network of over 500 lawyers, 40 in-house legal researchers, and 14 full time in-house translators. OneTrust DataGuidance™ offers solutions for your research, planning, benchmarking, and training.

OneTrust DataGuidance offers a GDPR Benchmarking tool, which includes California, Brazil, Thailand, Russia, Japan, and which is currently being expanded to include Australia as well as China. The tool assists organisations to understand and examine core requirements under each law in order to determine their consistency for gap analysis and assessment, and contribute to the development of global compliance programs.

OneTrust DataGuidance solutions are integrated directly into OneTrust products, enabling organisations to leverage OneTrust to drive compliance with hundreds of global privacy and security laws and frameworks. This approach provides the only solution that gives privacy departments the tools they need to efficiently monitor and manage the complex and changing world of privacy management.

OneTrust Privacy

PRIVACY MANAGEMENT SOFTWARE

PRIVACYCONNECT ONLINE EVENTS

Focus on regulatory requirements, updates, and trends while learning how to implement in practice

- Earn 2 CPE Credits
- Network with Professionals
- Share Best Practices for Compliance
- Engage in a Panel Discussion

REGISTER FOR A FREE EXPERT-LED VIRTUAL EVENT IN YOUR CITY

REGISTER | PRIVACYCONNECT.COM

Data Protection Leader is published bi-monthly by OneTrust Technology Limited, Dixon House, 1 Lloyd's Avenue, EC3N 3DS, London, United Kingdom

Website: www.dataguidance.com