Volume 2, Issue 2
March 2020
dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

THE CORONAVIRUS PRIVACY DILEMMA

Eduardo Ustaran discusses the privacy concerns and implications as a result of the spread of coronavirus 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.

Katherine Sainty, Sainty Law
Katherine is the founder and team leader at Sainty Law. Katherine is a corporate and commercial lawyer who specialises in digital, technology and media law. Katherine delivers strategic, innovative and cost effective solutions for her clients by applying her strong commercial expertise, extensive industry experience, sophisticated project management techniques, and broad regulatory skills. She has been recognised in Chambers Global, The World's Leading Lawyers, as pre-eminent in her field. Katherine frequently presents to audiences and provides expert commentary on current commercial and regulatory issues, most recently on digital industries, privacy and data protection, and cyber resilience issues.

Mark Goddard, Computacenter
Mark is an experienced information risk professional who is used to working effectively in complex, multi-stakeholder environments as part of a team and autonomously. Mark has over 10 years experience of successfully managing and delivering a wide range of demanding and cost-effective information risk programmes including data protection, information security and business continuity. Marks specialties include, Security Policy Framework, breach management, risk assessment, and information security management systems.

Toks Oyegunle, Privacy Lyceum
Toks Oyegunle, a Privacy & Cybersecurity Specialist, is the Managing Consultant of Privacy Lyceum, a Consultancy and Training company.
He is currently responsible for the implementation of a global privacy program across 127 companies spanning 27 countries for Merlin Entertainments.

Raymund Enriquez Liboro, National Privacy Commission, the Philippines
Privacy Commissioner
Raymund Liboro is a seasoned ICT convergence and communications and public administration professional.
Having been appointed as the country's first Privacy Commissioner in March 2016, he fast tracked data protection policy development in the country with the issuance of the Data Privacy Act's Implementing Rules and significant policy circulars within the first year of NPC's establishment — effectively working for the country's data privacy and protection rules to be at par with global data protection regulations.

Dr. Karsten Krupna, krupna LEGAL
Karsten Krupna is the founder of the law firm 'krupna LEGAL' and specialized in data protection and IT law. He has advised national and international clients from various sectors for many years. A special focus of his practice is on cybersecurity. Karsten Krupna advises and supports his clients in all areas of expertise, e.g. with regard to data protection law from audits to the design and implementation of business models in compliance with data protection law or with regard to IT law in the planning, design and support of IT projects.

Tumi Atolagbe, the British Council
Tumi has undertaken a variety of roles across the technology sector, and has developed knowledge of the data protection compliance sector. Tumi is currently an Information Governance and Risk Advisor (Privacy and Security) (Global Information Services) at the British Council, having previously worked as a Lead Policy Officer at the ICO.

Dan Or-Hof, Or-Hof Technology & IP Law
Dan Or-Hof has more than 20 years of daily practice in technology and IP Law for topics such as the Internet of Things, Big Data, Cloud environments, authentication and digital signatures, proprietary and Open Source licensing, Data Protection and Information privacy. Dan was formerly head of an international Israel based law firm's IT, Internet and Copyright department. Dan is a member of the Privacy Protection Public Council, a member of the International Associations of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional (CIPP/US and CIPP/E).

Image production credits
Cover / page 4 image: MATJAZ SLANIC / Signature collection / istockphoto.com
Page 6 image: Yarra Riviera / Essentials collection / istockphoto.com
Page 10 image: NiseriN / Essentials collection / istockphoto.com
Page 18 image: gremlin / Signature collection / istockphoto.com
Page 24 image: Ben Neale / Unsplash
Page 27 image: martinhosmart / Essentials collection / istockphoto.com
Page 28 image: kycstudio / Signature collection / istockphoto.com
Page 29 image: akinbostanci / 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
Petra Molnar, Mona Benaissa, Keshawna Campbell

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

EDITORIAL

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

Carrying out an objective assessment of the justification for requesting and processing this data therefore remains essential

Editorial: The coronavirus privacy dilemma

2020 is proving to be a challenging year for the world. Right from the start, news of horrific bush fires in Australia were followed by warnings that World War III was imminent. And now we have the coronavirus. The scale and severity of the disease is not unprecedented but the level of panic around it seems to be. As a consequence, extreme measures to handle the situation appear to have become the norm in a very short period of time. Some of those measures have a direct impact on people's privacy. In some places, the whole population is being subject to intense surveillance while the medical data of those infected with the virus is widely shared across organisations and countries. It may well be in the name of saving the planet from a deadly epidemic, but is it truly necessary and is it the right thing to do?

The privacy implications of the attempts to control the spread of coronavirus have become particularly visible in Asia. Once this global crisis is finally under control, China will likely be commended for the clinical efficiency with which it eventually managed to suppress an outbreak that could have affected billions of people. But that will certainly come at a cost. There are reports of 'epidemic maps' showing the precise location of confirmed and suspected cases in real time so people can avoid going to the same places. There is even an app that lets users check if they have been on a train or plane with someone who contracted the virus. These are indeed effective measures, but they require the collection and dissemination of detailed medical data at a massive scale. Similarly, innovative approaches to tackling the problem have been adopted in Korea and Singapore, and on the whole, they appear to have had success despite the wide and obvious privacy intrusions.

The nature of this dilemma suggests that the right approach must lie in finding the right balance. The right to privacy is not an absolute right, even in Europe. Regulators and courts know that, and their decisions reflect the reality that some interferences with the right to privacy are compatible with the law. The jurisprudence around cases that involve the ability of public authorities to interfere with the fundamental right to privacy in the interests of national security or public safety has consistently demonstrated that it is possible to find a reasonable balance. The numerous and complex rulings of the Court of Justice of the European Union on these types of cases tend to focus on two concepts: necessity and proportionality. So these parameters will also be applicable to the sharing and dissemination of coronavirus-related personal data.

Where does this leave us in practice? In an employment context, for example, how far can employers go in terms of monitoring their employees' health, finding out about their exposure to the disease and making business-wide decisions on that basis? In Italy, the biggest coronavirus hotspot outside Asia so far, the data protection authority is adamant that employers must refrain from demanding that their employees disclose personal data related to the coronavirus and their health. European data protection law may allow the collection and use of this data - either by relying on the necessity to comply with a legal obligation or even substantial public interest - but long-standing obligations regarding transparency, fairness, purpose limitation and data minimisation will continue to apply. Carrying out an objective assessment of the justification for requesting and processing this data therefore remains essential.

Data gathering and data sharing in the context of the fight against the coronavirus presents a global test for privacy frameworks around the world. Privacy and data protection laws cannot and should not get in the way of a common-sense approach to saving lives. For that reason, all such frameworks allow the use and sharing of data when necessary for that purpose. At the same time, the parameters set out in the law cannot be ignored - even at times of crisis. Disproportionate decisions and measures are often the result of knee-jerk reactions, and when that happens at a global scale, everyone is at risk - no matter how often you wash your hands.

How to plan a global privacy program:
Five critical success factors to consider

'If you fail to plan, you plan to fail.' A global privacy program rollout is a considerable undertaking with multiple moving parts, and a realistic and effective plan will help with the understanding of the scale and scope of the project and increase the ability to successfully deliver the privacy program globally. Toks Oyegunle, Managing Consultant at Privacy Lyceum, provides insight into how to plan and implement a successful global privacy program, and what factors must be considered throughout this process.

When planning, or implementing, a privacy program, it is helpful to use a simple five-factor framework as a basis to discuss key areas that need to be considered, questions that must be asked, and facts that should be established to ensure success. These five factors are:

1. the foundation (team, vision, mission, and strategy);
2. the organisation (structure, culture, and geography);
3. the law (regulations, compliance, and risks);
4. the tools (productivity tools, systems, and privacy frameworks); and
5. the deliverables (training, data mapping, gap analysis, and reports)

The foundation: team, vision, mission, and strategy

The foundation represents the starting point of the project, the fundamental issues that must be clarified before you start the rollout of your global privacy program. As we start, there are a few things we need to put in place: we need a team in place to do the work; a vision to guide us to the successful destination; a mission to keep us on track; and a strategy to detail what exactly we plan to do to get the vision actualised.

The Team

The team is probably the best place to start, as here the goal is to establish who will be included in the team, what will they be doing, and why. Think of the team as the group of people tasked with the responsibility to deliver this project globally. Let us start with the team leadership. Some organisations are more mature than others, and may have more established privacy management and privacy processes, for example they may already have a Chief Privacy Officer, a data protection officer, or a similar role tasked with the leadership of this function. In this case, the task starts with this individual and they will probably have a team in place. In most cases, the privacy teams tend to be small, so this individual may only have a few other people in their team.

What if you do not have an established privacy office, or there is currently no role tasked with the leadership of privacy in the organisation? This does happen quite regularly due to the relatively new status of privacy compared to other organisational functions, and if this is the case with your organisation, do not panic, but realise you will need a team that is set up specifically to deliver this privacy program. In this case, there will probably be a project sponsor that initiates this and ideally this will be a relatively senior resource. The role of the project sponsor is important, as is the executive approval they have for the project. This is because it will have a direct impact on the project budget which feeds directly into the ability to staff the team with the right resources. The project sponsor

Toks Oyegunle Managing Consultant
systematic.alchemy@gmail.com
Privacy Lyceum Limited, London

may be a strategic team member, but not necessarily an operational one. While they may attend steering committee meetings and receive executive briefings, they will probably not be involved in the day-to-day running of this project, however, this is the first resource required to start to build the team.

You would also need someone who would drive this project across the organisation globally, they will really be doing the job of a program/project manager as a global privacy program is a program consisting of multiple privacy projects spread across different locations. Therefore, regarding the team you need someone at the executive level as a project sponsor, you need someone at the management or senior management level as the program manager, and then you need privacy managers and privacy analysts to do the day-to-day operational side of the project. The number of people required in the core team will be a function of your organisational size and structure. If you are doing everything centrally and the organisation is large, then you need a bigger team, on the other hand if you have a decentralised structure with resources also deployed locally, then your central team can be smaller as you can delegate tasks to the decentralised units.

Vision

With a team in place, there is a need for a clear vision. Ideally, this should be a privacy vision statement that documents a future state for the organisation regarding privacy. This is not a long document, but a brief statement of a paragraph or two that describes how the organisation sees itself regarding privacy in the future. Simply put, the vision statement describes where, as an organisation, you are going regarding privacy, including privacy governance and privacy operations.

Mission

Alongside the privacy vision statement, there is a need for a privacy mission statement. The privacy mission statement should capture what the organisational mission regarding privacy is. Many people confuse a vision statement with a mission statement, assuming that they are the same thing, but they are different. The vision is where you are going, and ultimately, the vision is a destination, a future state to achieve. The mission is what you do daily to get you to that desired destination. For example, the vision shows a tangible, quantifiable result, while the mission captures the intangible aspects, like attitude and beliefs, required to achieve the vision.

Strategy

The privacy strategy is quite important as it is a document that will take the desired vision, coupled with the chosen mission, and use them as a basis to create a realistic plan that can successfully actualise the vision. The strategy will detail the sequence of activities, tasks, and deliverables required to get us from the current state today, to the desired state in the future. When this is done properly your global privacy program becomes increasingly clear with project deliverables, project timelines, and resources required becoming much easier to identify.

The organisation: structure, culture, and geography

The goal of a global privacy program is to implement a new normal regarding privacy across your organisation globally. In line with this, you need a firm understanding of your organisation from the onset. This section discusses a few aspects of the organisation that are critical to success.

Structure

How is your organisation currently structured globally? This is a question that you need to ask and understand as you need an approach that works with the current structure. Some organisations have a very strong centre, they adopt a head office model where everything tends to be managed centrally, and

if this is the case it is very likely that the privacy program will need to be managed centrally too. Alternatively, there are organisations that adopt a more distributed structure where the units are more autonomous, or they report to regional head offices. If this is the case, you may need to adapt your program accordingly. It will be helpful to understand where your organisation fits into the two extremes, between a strong centre and a weak centre, and think about how this will impact your privacy program.

Culture

The organisational culture is another factor that needs to be understood and managed effectively. Is it a well-entrenched bureaucratic culture, typical of large mature organisations with an established order? Or do you have an organisation that is less structured and more open to innovation? Is the culture resistant to change, as opposed to an organisation where change is embraced? Rolling out a new privacy program globally is a change management project, so a firm understanding of how the organisation reacts and adapts to change is required for success. Without understanding and aligning with the culture, you may find that you come across some resistance, or that the project is not received very well, simply because it has not been packaged or presented the way that your stakeholders are used to and expect. Ensure you understand the culture and make sure that as you roll your privacy program out, and that you are aligning it to the culture of the organisation as it already exists across different locations.

Geography

Geography is used here to refer to the geographical spread of the organisation. Ideally you would start with a verified list of all the entities in the organisation, their addresses, and details of their leadership. Some organisations have 20 subsidiaries across five countries, some may have 100 subsidiaries across 30 or 50 countries. Irrespective of what it is, it is a metric you must identify and document because it feeds directly into the next factor we will discuss, which is the law.

The law: regulations, compliance, and risks

The law is a major driver of the privacy industry, indeed the recent spurt of growth and interest in privacy globally is synonymous with the implementation of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). This section will discuss the law within the context of your global privacy program.

Regulations

Privacy laws are typically established by countries or regions to protect the personal data and rights of their citizens and residents, for example the GDPR in the European Union and the California Consumer Privacy Act of 2018 ('CCPA') in California. Major organisations, on the other hand, tend to have global operations conducted by different entities domiciled in different countries. It is necessary to know all the relevant privacy laws applicable to your organisation, which can be deduced partly from a list of countries you are physically operational in, in addition to an overview of the markets you serve, whether you have a physical presence there or not.

> **Organisations must realise that customers are increasingly aware of privacy issues and the rights they have regarding their personal data**

Since the introduction of the GDPR in 2018, there has been a flurry of activity in the privacy law space with many countries and regions coming up with their own similar regulations, such as the 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. Additionally, many countries in Africa and the Asia-Pacific have new privacy laws, and there are many states in the US with new privacy laws at different stages of development. The landscape for privacy laws globally is increasingly dynamic, and there is a need for privacy professionals to be on top of this by understanding what laws are relevant to their organisations and why, because this is what will drive your global privacy compliance efforts.

Compliance

One of the key deliverables from your global privacy program will be compliance with applicable privacy laws. Your ability to be compliant will be influenced by your ability to understand the relevant laws you must be compliant with and what compliance with each law requires. The key question to ask here is, what laws need to be complied with, and what is needed to demonstrate compliance with these laws. The answer is typically a matrix which clarifies areas of focus for the project. Consider what compliance means to your organisation and what is your understanding of being compliant with a specific regulation?

Different business models require different approaches to compliance personalised for them. There is a need to review and agree on what being compliant looks like for your organisation and how do you intend to demonstrate compliance once it is achieved.

Defining privacy compliance globally can indeed be challenging, especially with the proliferation of multiple privacy laws across different jurisdictions. An approach many organisations have taken is to use their GDPR-compliance project as the privacy compliance reference point, and to tweak this in line with the different requirements of other privacy laws they need to comply with globally. Indeed, there is a school of thought that believes that because the GDPR is a robust regulation with an increased focus on accountability, adopting GDPR-compliance as a preliminary global privacy compliance standard is a good risk management strategy.

Risks

It is impossible to discuss a global privacy program without exploring risks when the very nature of the project is broadly to comply with privacy regulation to mitigate regulatory and financial risk. Most of the newer privacy regulations provide for regulatory sanctions and significant financial penalties in the event of data breaches, amongst other events. As you progress with the privacy program rollout globally, you will no doubt highlight various risks across the organisation. It may be helpful to create a risk register of all risks, and categorise all risks using a standard risk scoring methodology, which will enable appropriate risk assessment and prioritisation. Consider the relevant mitigation actions required for each identified risk and establish who the risk owners are and how the risk mitigation process will be managed. Organisations must realise that customers are increasingly aware of privacy issues and the rights they have regarding their personal data, the constant breaches announced in the news, and the subsequent fines have sensitised the public into how organisations are using their personal data.

The tools: productivity tools, systems, and privacy frameworks

As part of the global privacy program rollout, you will need various tools to get the job done, some of which will help you work more effectively, while others will make you work more efficiently. This section explores some tools you should consider to increase your chances of success.

Productivity tools

Let us explore the productivity tools that will be helpful as you embark on the global privacy program rollout. A global privacy program rollout is a program consisting of multiple projects, and there is the need for a good project

management tool. Using a tool to manage resources, milestones, deliverables, and deadlines will help you retain overall oversight and control of what is happening globally at any point in time. Please note things can get complex very quickly as you try to manage different projects, different people, and different deadlines across different countries and time zones, and your project management system will help to keep this manageable. A few other tools that will come in handy and will help you to systematise the global rollout include templates, checklists, scripts, and question and answer documents. You need various email and communication templates that are sent to stakeholders at different stages of each project, you need checklists to clarify what needs to be done at each stage and in what order, you need scripts that will be used to deliver webinars and workshops, and you will need question and answer documents to help people get their questions answered before they need to ask. Do not underestimate the importance of these tools to the success of your project, they are simple tools with a significant impact.

Systems

The growth of the privacy industry has seen an explosion in privacy technology, and we now have many vendors offering systems to help with every aspect of privacy operations and management. From data discovery through to data mapping, from data subject access request ('SAR') management to consent management, from cookies management to incident response, from privacy policy/notice management to vendor management and risk management, there are software solutions that can help you. If you want increased insight into what tools are out there, there is a Gartner report that collates and categorises privacy management tools and would be a good place to start.

A decision you need to consider early on is whether you will do your global privacy program manually or whether you will invest in a software solution. An appropriate system has multiple benefits, for example, they offer automation which helps you to get more done in less time, a huge plus when you are taking a program globally. Many tools also offer systems integration which means they can interact with your existing technology landscape and automatically help you with data discovery, data mapping, and even dealing with SARs from the public.

Privacy frameworks

Adopting the right privacy framework is quite important as this is a tool that will help to provide structure and direction to your privacy program. Think of a framework as an approach, a set of principles or guidelines that help to direct the correct implementation of your privacy program. There are various frameworks available and you will need to select one that is a good fit for your organisation. Many would argue that the GDPR itself provides a framework that you can use for your privacy program, but then, so does the CCPA. There are other privacy or data protection management frameworks that you may use. The important thing is to use your knowledge of your organisation, its geography, and culture, to guide the appropriate choice of the framework.

The deliverables: training, data mapping, gap analysis, and reports

There is a need for tangible deliverables from your privacy program, namely: how will you showcase the results of your hard work and what will you deliver to your stakeholders at the end of each project. With the increased emphasis on accountability required by the GDPR, organisations must now demonstrate compliance, and this is achieved with increased actions and documentation which will form most of the deliverables from your privacy program.

Training

Most privacy programs will include a requirement for privacy training or data protection training across the organisation. There is also a need for a comprehensive privacy awareness campaign which serves to increase the general awareness of staff regarding privacy matters and any imminent changes in privacy law. Privacy training is ideally delivered in a two-fold approach. Initially, some general privacy training should be arranged for all employees irrespective of their role, as this should provide the general basics of privacy within the context of the organisation. It helps employees understand the new privacy expectations and culture that is being propagated. In addition to this, is the need for role specific privacy training where detailed privacy education is provided within the context of the role the employee has within the organisation. The awareness campaigns may be delivered via flyers, screensavers, posters, newsletter articles, and webinars, amongst other available options.

> **The gap analysis phase of your privacy project will no doubt uncover some privacy gaps and risks**

Data mapping

As part of privacy management, there is a time-bound, regulatory enforced requirement to respond to personal information requests from data subjects and consumers, and there is also a similar requirement to respond to data breaches. These requirements can only be effectively fulfilled based on a comprehensive understanding of where, how, and why your organisation uses personal data. This leads to data mapping, a central focus for most privacy programs, and you will no doubt need to conduct a data discovery exercise to identify everywhere that your organisation collects and processes personal information. Then you will need to map the movement of all identified personal data through its lifecycle. Doing this properly in one location is challenging enough, especially when you consider how much personal information is used across functions such as human resources, marketing, operations, and others. Therefore, scaling this globally can become complex quickly and many organisations choose to use excel for this, however, you are well advised to use a proven tool to systematise and automate this process for your global privacy program. Bear in mind that in addition to using this internally for SARs and breach management, you will also have a legal requirement to demonstrate this, for example, according to the Article 30 requirement of the GDPR which states that you must document all processing activities that store and/or collect personal information.

Gap analysis

The gap analysis phase of your privacy project will no doubt uncover some privacy gaps and risks that need to be rectified. They will vary and may range from outdated privacy policies that need rewriting, to websites that need new consent clauses or specific systems that require a comprehensive security review. These will need to be documented as some will trigger new remediation projects. The documentation of these gaps is critical as it demonstrates the results of your privacy program. This is proof that your organisation is not only aware of the identified privacy issues, but it already has a plan in place to remediate them. The ability to demonstrate this goes a long way to show regulators and auditors that you are clearly on top of your privacy responsibilities.

Reports

Your project sponsor, the executive team, and senior management will require various reports from your privacy program. These will vary and will be driven by their specific requirements. Reports regarding risks identified and risks mitigated are standard, and there will be other reports needed to help them understand how privacy is faring across the organisation in general. This is another area where investing in the right privacy management tool is important, as some come with extensive reporting capabilities which should make this part of the project relatively easy.

REGISTRATION OPEN

PRIVACY CONNECT

Workshops by OneTrust

150 FREE REGIONAL & INDUSTRY EVENTS

PRIVACY	COOKIES
CCPA	VENDOR RISK
LGPD	MARKETING
PDPA	PUBLISHER

STAY UP-TO DATE ON LOCAL REGULATIONS | CASE STUDIES
OPERATIONAL BEST PRACTICES | CPE CREDITS

REGISTER TODAY

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

Privacy Talks

OneTrust DataGuidance spoke with Mark Goddard, Group Data Protection Officer at Computacenter as part of the 'Privacy in Motion: Tech' series. Mark offers his advice on how to determine who is and who is not the data controller or data processor, as well as discussing the differences between data controllers and processors, and the key considerations for data protection at Computacenter.

Key considerations

Computacenter is a reasonably large organisation consisting of 15,000 people spread across over 10 countries. It is a FTSE 250 listed company, so it is a reasonably large company. One of our key considerations with a large amount of systems and a large amount of data in those systems is making sure that we understand our statutory roles and responsibilities, and that we apply those to the extent that they are applicable under data protection law.

> **One of the ways that large organisations, or any organisation, can provide accountability is by documenting their approach to data protection.**

Controller v. processor

Computacenter is an IT services organisation, meaning we will sell you a laptop, or more likely 100 or 1,000 laptops, we will help you set those laptops up, if you would like us to, and we will also provide a service desk, and other services for your users who are using those laptops. On the service desk side, we record the incoming calls from end users for the purposes of quality and monitoring, and anybody who is used to the service will have heard that phrase before. That is our purpose and we are recording that information and retaining that information for a purpose and method determined by Computacenter. We are the controller of that data for that purpose. However, the underlying purpose of that is the contracted service desk purpose, and when we take that information recorded in that call and turn it into a ticket so an engineer will turn up at the end users' desk and hopefully sort out their problem, we are processor of that data because our customer is determining that purpose, and that means of processing.

Internal impact

One of the key things under data protection is the accountability principle provided by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). One of the ways that large organisations, or any organisation, can provide accountability is by documenting their approach to data protection. So we are absolutely committed to ensuring that we have the right documentation in place, for example the records of processing, and we have to maintain records of processing both as a controller and as a processor of personal data, and we also have to manage the Data Protection Impact Assessment, which of course, as we know only applies to the data controller of data. So, it is very important to understand whether we are the controller or the processor of that data so that we can maintain and create the right document set.

Recommendations

Let us make no bones about it, it can be very difficult to determine who the controller and who the processor of data is. Very experienced data protection professionals can, after due consideration, arrive at different conclusions. Where it is not clear who is the data controller, who is data processor, or even if there is the existence of joint controllers, after careful consideration, I would advise people to take a purposive approach. What I mean by a purposive approach is to go back to Article 5 of the GDPR, and the principles of data protection, and apply those principles regardless of whether you are a controller or processor to ensure that there is a lawful basis of processing. For example, to ensure that you are only keeping the data for as long as is necessary and that you are only collecting and using the right amount of data. If you take that purposive approach, even if it transpires in the long term that your assessment of whether you are a controller or a processor was not necessarily correct, you will not be that far away from the mark and it be very difficult for anyone to meaningfully criticise you regarding your compliance.

Australia: Complying with the Consumer Data Right

The Consumer Data Right ('CDR') will have the potential to empower consumers, however, it may also increase the regulatory burdens and compliance requirements for businesses generating or collecting data both within and outside of Australia. Katherine Sainty, Director at Sainty Law, provides an overview of the CDR, and discusses what businesses may need to consider in order to be compliant.

On 1 August 2019, the Government of Australia passed the Treasury Laws Amendment (Consumer Data Right) Bill 2019 ('the Bill'), giving Australians greater control and access to their data in certain designated sectors. The Bill has had a tumultuous history, in 2017 the Government announced its intention to create the CDR following the Productivity Commission's inquiry into the use of data, however, the Bill lapsed ahead of the Federal Election. With its reintroduction, the CDR is touted as one of the most significant moves by the Government towards empowering consumers.

The CDR will allow consumers to access their data held by service providers and share it with trusted and accredited third parties, such as banks and comparison sites. The data under the CDR regime will include:

- transaction data, such as data relating to balances and date of transactions;
- customer data, such as data relating to customer details including name, account number, mobile phone, and direct debit account; and
- product data, such as the product type, name, and price.

The CDR will improve competition, consumer choice, and convenience as data can be communicated with third-party comparison sites to increase consumer negotiation power, allowing them to compare products and providers to seek out the best deal for their money. Service providers are required to give customers open access to data on their product terms and conditions, forcing businesses to be more transparent, innovative, and price competitive on the products offered to consumers.

Where will the CDR apply?

The CDR has a broad geographic application, covering data generated or collected within and outside Australia. The CDR will apply to data collected outside Australia if it is by an Australian company registered under Parts 21.2 or 5B.1 of the Corporations Act 2001, or an Australian citizen or permanent resident.

Who will the CDR apply to?

The CDR will initially apply to the banking sector, before being phased

into the energy and telecommunications sectors. After that, it will gradually apply to other industries on a sector-by-sector basis. The additional sectors required to implement the CDR will be designated by the Treasurer of the Commonwealth of Australia, based on advice from the Australian Competition and Consumer Commission ('ACCC') and the Office of the Australian Information Commissioner ('OAIC').

When will the CDR apply?

The ACCC announced, on 20 December 2019, that its plans to roll out the CDR in the banking sector which will go live on 1 July 2020, enabling consumers to direct major banks to share their data in relation to credit and debit cards, deposit accounts, and transaction account data to accredited recipients of CDR data. Mortgage and personal data will be able to be shared after 1 November 2020, however the ACCC has made it clear that it will continue to consult with various stakeholders, including industry, consumer, and privacy groups, which may alter these intended roll out dates.

Who will regulate the CDR?

Given that the CDR inherently intersects competition and consumer law, as well as privacy law, the CDR will be jointly governed by the ACCC and the OAIC. The ACCC will take the lead when it comes to issues revolving around the designation of new sectors of the economy to be subject to the CDR and the establishment of the relevant rules, whereas the OAIC will regulate on matters concerning privacy and confidentiality, as well as to ensure compliance with the supplementary CDR privacy safeguards, discussed below.

What about privacy?

The CDR privacy safeguards have been specifically designed to include further protection not already covered by the Australian Privacy Principles ('APPs') under the Privacy Act 1988. For this reason, the APPs will be 'switched off' and substituted with the CDR privacy safeguards for accredited data recipients of CDR data, for example, those who are 'licensed' to receive data through the CDR system. However, the APPs will continue to apply to the CDR data held by data holders of the original data that the right to transfer applies to, and to designated gateways who are entities designated as responsible for facilitating the transfer of information between data holders and accredited persons.

What does this mean for your business?

The CDR will initially affect businesses within the banking, energy, and telecommunications sectors, meaning there will be an increased regulatory burden on these organisations. If your business is in the banking, telecommunications, and energy sectors, or has clients in those sectors, then you should be prepared for these changes.

Ensure your privacy safeguards and measures are in place by reassessing your compliance arrangements and checking the status of your current data protection systems to meet the new standards. Businesses should have an adequate functional system in place to respond to consumer data directions when they request access to or transfer of their data. As both consumers and the ACCC can bring an action against you for not complying with the CDR, having a well-established process for dealing with complaints and privacy issues is crucial for the compliance and growth of your business.

Katherine Sainty Director

katherine.sainty@saintylaw.com.au

Sainty Law, Sydney

Find further Insights like this on the OneTrust DataGuidance Regulatory Research Platform.

Comparing privacy laws:
GDPR v. Australian Privacy Act

OneTrust DataGuidance and Mills Oakley have teamed up to produce a GDPR v. Australian Privacy Act Benchmarking Report in order to assist organisations in understanding and navigating the similarities and differences between the GDPR and the Australian Privacy Act, and to help organisations achieve global compliance.

The Privacy Act contains a few similar provisions to the GDPR, for instance, both define special categories of data and outline similar requirements in relation to the right to access and the right to be informed. However, there are also a number of divergences between the two laws, particularly in relations to legal basis, controller and processor obligations, as well as civil remedies.

The Benchmarking Report provides an easy comparison between the two laws in an easily readable format.

To see other Benchmarking Reports available on the OneTrust DataGuidance platform, such as GDPR v. CCPA and GDPR v. Russian Law on Personal Data, head over to: platform.dataguidance.com/research-and-reports.

WEBINAR

Key takeaways: GDPR's practical impacts on Australasian businesses

On 25 February 2020, OneTrust DataGuidance held a webinar with Alec Christie and James Wong, Partner and Associate at Mills Oakley Lawyers in Sydney.

The webinar discussed the impact of the GDPR in Australasia. Our speakers outline key considerations for businesses in Australasia, including the extra territorial scope of the GDPR, and mechanisms to ensure compliance, such as geoblocking. Through a discussion of enforcement under the GDPR, and how businesses can manage operations EU, this webinar provides a straightforward guide to the practical implications of the GDPR on Australasian businesses.

Key takeaways

Territorial scope of the GDPR in Australasia

For global organisations, Article 3(2) of the GPDR addressing territorial scope provides a central point of determination as to whether the GDPR will apply. In short, the GDPR will apply if a business is offering goods or services in the EU, or monitoring behaviour of data subjects within the EU. For example, our speakers note that this would apply to companies operating an advertising campaign in the EU without the need for a purchase or exchange of goods. In terms of monitoring behaviour, our speakers highlight the importance of 'geoblocking' for companies operating on a multinational basis as businesses need to be prepared to treat the personal data of EU citizens in accordance with the GDPR.

Steps to achieving compliance with the GDPR

There are steps Australasian businesses can take to manage compliance with the GDPR. Our speakers note that businesses need to analyse whether they are subject to the GDPR before entering into a GDPR compliance program, as well as ensure they have the technical capability to action compliance. For example, they must be able to fulfil data subject rights, including the right to erasure and access. In addition, our speakers emphasise that businesses need to look at their existing third-party contacts, as the GDPR may also apply to these. Having said this, business may wish to limit the impact of the GDPR, by isolating operations in the EU. Our speakers state that even if an Australasian business is not subject to the GDPR they should still be aware of its requirements when conducting operations in the EU in order to avoid accidental advertising or monitoring.

GDPR enforcement in Australasia

Australasian businesses and organisations should be aware that many European countries have signed a reciprocal enforcement of foreign judgments treaty with Australia. In practice, this means that a judgment made in a European court could be enforced in Australia. Therefore, the GDPR may have financial implications for Australasian businesses. As pointed out by our speakers, while the key concepts of privacy law are similar in both Australiasian and EU legislation, the GDPR has established formal enforcement mechanisms with substantial fines.

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.

REGULATOR SPOTLIGHT

OneTrust DataGuidance sat down with Raymund Liboro, Privacy Commissioner & Chair at the National Privacy Commission ('NPC'), Philippines in October 2019. Raymund discusses the significance of the NPC's recent decision to participate in the Asia-Pacific Economic Cooperation Cross Border Privacy Rules ('APEC CBPR') system as well as how the NPC is looking to establish international standards through work with other jurisdictions.

What is the significance of the NPC's recent announcement of participation in the APEC CBPR system?
Three years ago when we embarked on the journey of building the NPC and guiding industry towards the path of resilience, accountability, compliance, and the practice of ethics, we drew up a roadmap for responsible companies to guide them towards joining, and intrinsic to that roadmap is the adoption of global frameworks. This part of the options that we have, while for global frameworks you have the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') in the EU and other standards, even the Ibero-American network have their own standards. I guess it is really part of the maturing process for organisations in trying to achieve a state of what we call accountability and assurance to their customers and stakeholders.

So, I must say that this is, again, part of and intrinsic to, the overall picture that we are trying to paint for our stakeholders. The good thing is that three years after the introduction of the CBPR, we have decided to enrol in the CBPR because by our appreciation, industries have achieved that certain maturity to accept responsibilities and to level up their game when it comes to accountability and compliance, and the CBPR is definitely one of the standards or frameworks that can be adopted.

How is the NPC working with other jurisdictions to establish international standards?
For achieving accountability or attaining accountability and compliance, and to achieve data privacy resilience, you have to come up with a myriad of approaches. There is no single road, there is no silver bullet in the approach towards achieving those. Again, part of our adoption of global frameworks would also be to engage other jurisdictions in bilateral agreements or partnerships. This signifies the country's readiness. At the same time, this signifies our intent to seek out other jurisdictions where we can establish a common baseline for cross-border data transfer or responsible data transfer.

The Memorandum of Understanding ('MoU') with Singapore signals the first MoU that we have struck with another jurisdiction. More are coming. We find this vital, we find this very important as again, even establishing these small victories with other jurisdictions proves a lot about our practices in the country, the standards that we maintain, and the recognition of other jurisdictions, and that is very, very important when it comes to international data transfers. So, the MoU again is the easy part coming up with the body, and adding to the body and the spirit of that understanding is the more exciting part. We are already talking about modalities of collaboration, such as our data protection officer ('DPO') sharing best practices with their DPO's and *vice versa*.

We are also talking about dual DPO meets and talking about possibilities of sandbox approaches for companies to undertake, if necessary. So, there are many exciting ways on how to go about it. We hope that this would also set the standard for best practices when it comes to establishing bilateral agreements or understanding with another jurisdiction, such as Singapore.

How do you see the new ASEAN Data Protection and Privacy Forum developing?
This is a very exciting space because in our little part of the world, that significant development we will figure out in the next few years in the global privacy sphere. The Association of Southeast Asian Nations ('ASEAN') is composed of ten Member Nations, and the combined population of six of the ASEAN alone, so the Philippines, Singapore, Malaysia, Vietnam, Indonesia, and Thailand, is that of the EU, almost equally.

> **I think the synergy among the ASEAN Member Nations will be an exciting thing to watch, and there will be really exciting developments in the privacy sphere**

So, in terms of economic activity and in terms of potential transfers of data, you are really talking about a huge market in the ASEAN, and for the ASEAN Members to put it in the agenda, to come up with a framework, and also with an adequate initiation, such as the ASEAN Privacy Forum led by Singapore, the Philippines, and Malaysia, which incidentally are the Member Nations that have comprehensive laws in place.

We are committed to helping our neighbours, such as Thailand and Indonesia, who have all just started their privacy regimes. The Philippines enacted the Data Privacy Act of 2012 (Republic Act No. 10173) ('the Act'), Thailand enacted their privacy law in 2019, Indonesia is on the way to enacting a comprehensive law, and

CONTINUED

Raymund Liboro Privacy Commissioner & Chair at the National Privacy Commission, Philippines

the other Member Nations have really shown interest in pursuing their own privacy laws. There is this ten Member Nation which again, the economic potential and the market potential of this region is tremendous.

We are talking now about privacy with other nations that have established their laws beforehand and others are building their laws up. It is a good mix of experience and those who are really trying just to get on board. We have the benefit of learning from the other networks, we have the benefit of learning from decades of practice by other jurisdictions, and other regions, like the EU, but we also have the agility now to introduce more new, exciting concepts and innovation when it comes to data privacy and protection. I think the synergy among the ASEAN Member Nations will be an exciting thing to watch, and there will be really exciting developments in the privacy sphere.

So, while we are just starting everybody is talking about how to be on the same page in a way, how interoperability can be established right at the get go, and how harmonisation can be put on top of each others' agenda. I guess that really bodes well for the entire region.

What areas have been a focus for the NPC, and what are its priorities for 2020?

For the Philippines, we have been very deliberate in our regulatory approach. We believe in a risk-based approach, an evidence-based approach, and we are very empirical in our approach. So, whilst the Act was enacted in 2012, it was only in 2016 that the NPC was founded and we embarked on a three-year programme then that basically spells out how we will lift privacy in the country and project the Philippines as a responsible place for data. We emphasise awareness, then with time, compliance followed with enforcement. We believe that this is a natural order of things with a more aware citizenry. You would have companies that would see the imperative of complying and being accountable. In 2020, I believe we have a much more aware audience at this time, and they expect a lot from our controllers and processors, and even from the Government.

So, we will continue harnessing and promoting compliance, accountability, and the practice of ethics in all of our stakeholders. One thing for sure is that enforcement would also be found. We have received lots of complaints and we had a 500% increase in complaints in 2019 compared to 2018. People are aware, they are slowly understanding their rights, and they are asserting these rights. As a regulator, we have to respond also to the way they will uphold and assert their rights. Therefore, compliance and enforcement would still be the main focus for 2020.

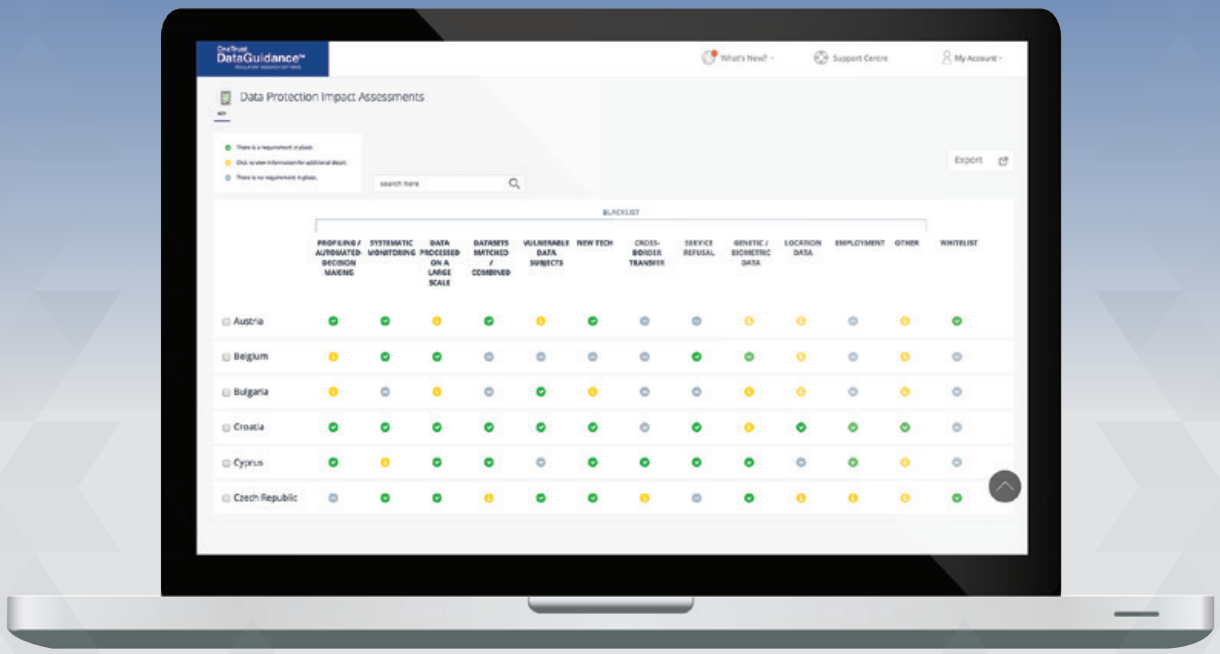
Monitor and understand the APEC CBPR system with the APEC CBPR Comparison chart now available with OneTrust DataGuidance Regulatory Research.

OneTrust DataGuidance™

REGULATORY RESEARCH SOFTWARE

Data Protection Impact Assessment Comparison

Understand and determine whether a certain type of processing activity will trigger the requirement to conduct a DPIA based on EU-level guidance, and national blacklists and whitelists issued by Data Protection Authorities across the EEA.



- Identify and minimize the data protection risks of a project or plan
- Determine what processing activities trigger the requirement to conduct a DPIA
- Compare national blacklists issued by DPAs across the EEA analyzing the most common processing activities
- Review and understand national whitelists and other exceptions to conducting a DPIA
- Access DPA guidelines, checklists, templates, and tools for performing a successful DPIA

Try it for free when you sign up for a trial at **DataGuidance.com**

Germany: Are companies now facing fines in the millions?

Dr. Karsten Krupna Partner
k.krupna@krupna.legal
krupna LEGAL, Hamburg

On 14 October 2019, the German Data Protection Conference ('DSK') published its future model for the determination of fines for violations of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR')[1]. The aim of the model is to guarantee a consistent level of penalties set by German supervisory authorities in proceedings against companies. Dr. Karsten Krupna, Partner at krupna LEGAL, provides an overview of the scope of application and binding effect of the model of the DSK's for the calculation of fines and its content, as well as the possible effects of fines and an outlook on the possible consequences for business practice.

Compared to other European countries, the German data protection supervisory authorities have so far been considered very moderate in imposing fines. While the Portuguese data protection authority has imposed a fine of €400,000 and the French data protection authority imposed a €50 million fine, the British Information Commissioner's Office recently sanctioned a data protection violation with more than €200 million. In contrast, in Germany, since 2018, fines with a total volume of €485,490 have been imposed within one year. According to the 'Welt am Sonntag' of May 2019, this amount is based on the information provided by the supervisory authorities from 15 of the 16 federal states. Based on the total amount mentioned above, the average fine imposed in Germany is around €6,000. With these amounts, it is not surprising that the German supervisory authorities have been considered moderate in a European comparison. As far as can be seen, the fact that the application of the framework for setting fines in Germany was perhaps also based on a different self-image of official practice, was not discussed.

Whether a possible misunderstanding between the media perception and the authorities' self-image was also a reason for the step taken by the DSK cannot be determined. The calculation of the fine focuses on the turnover of a company. The DSK considers this as a 'suitable, adequate, and fair starting point for ensuring effectiveness, proportionality, and dissuasion[2].' For the potentially affected companies, however, the main question arises as to what consequences are to be expected with regard to the level of future fines. In October 2019, the Berlin data protection authority imposed a fine of around €14.5 million on a real estate company. Compared to the aforementioned annual amount from the survey result, this represents an increase of approximately €14 million due to only one case. Is this a taster of the new fining practice in Germany?

Scope and binding effect of the DSK model

The model of the DSK only applies in fine proceedings against companies. Therefore, it is not applicable to fines imposed on 'associations or natural persons outside their economic activity.' Lastly, the concept has no binding effect on cross-border cases, other data protection authorities in the EU, or the courts[3].

Determination of the fine on the basis of the DSK model

The central starting point for the model of the DSK is the previous year's

turnover of the respective company. This is based on the broad and therefore controversial concept of a company, in line with Recital 150 of the GDPR. The fine will then be determined systematically in the following five steps:

1. the company concerned is allocated to a size class on the basis of its turnover;
2. the average annual turnover for this size class is ascertained;
3. an economic basic value is calculated;
4. a factor for the seriousness of the violation is determined, which is multiplied by the previously ascertained basic value; and
5. the result determined under (4) is adjusted on the basis of other circumstances speaking for and against the company concerned, insofar as these were not yet taken into account in the previous determination.

In detail, the methodology applies as follows.

Categorisation of companies by size class

Firstly, the company is allocated to one of four size classes on the basis of an annual turnover table. Within a range of up to €2 million for micro companies ('A'), the table further classifies between small companies ('B'), medium-sized companies ('C'), and large companies ('D'). D companies are defined as those with an annual turnover exceeding €50 million.

If the class size is defined as a 'rough framework,' a more detailed division into subgroups is made within each class. In the case of A companies, i.e. companies with an annual turnover of up to €2 million in the previous year, for example, there are three subgroups, which are described as follows:

- subgroup 1 ('A.I'): previous year's turnover up to €70,000;
- subgroup 2 ('A.II'): previous year's turnover between €70,000 and €1.4 million; and
- subgroup 3 ('A.III'): previous year's turnover between €1.4 million and €2 million.

If, for example, the company concerned had a turnover of €900,000 in the previous year, it must be allocated to the size category of company A and then to subgroup A.II.

By contrast, the largest class in terms of company D contains seven subgroups. These range from a previous year's turnover between €50 million and €75 million, which is subgroup D.I, to the last subgroup D.VII, in which companies with a previous year's turnover of more than €500 million are classified.

Determination of the average annual turnover of the corresponding subgroup

In the second step, the average annual turnover of the subgroup in which the company was classified is determined. The subgroups for the size class of micro companies are then given the following average annual turnover:

- subgroup A.I: €350,00;
- subgroup A.II: €1,050,000; and
- subgroup A.III: €1.7 million.

Within each size category, A. to D., an average annual value is thus determined for the respective subgroup. There is only one exception for the subgroup D.VII, because from an annual turnover of more than €500 million, the percentage fine of 2% or 4% of the annual turnover is taken as the maximum limit, so that for the respective large enterprise a calculation is made on the basis of the actual turnover.

Calculation of the basic economic value

Based on the average annual turnover of the subgroup, the 'basic economic value' of the company is now calculated by determining a daily rate. For this purpose, the average annual turnover ascertained for the company concerned is divided by 360 (days).

The following daily rates are then calculated for the subgroups for the size class of A companies:

- subgroup (A.I): €972;
- subgroup (A.II): €2,917; and
- subgroup (A.III): €4,722.

By comparison, the daily rate for a company in subgroup D.VI is already €1.25 million. The calculation for the strongest subgroup, in terms of annual turnover, D.VII, is once again special. As in the determination of the average annual turnover, the daily rate is also determined here on the basis of the actual turnover.

Multiplication of the basic value by the seriousness of the violation

In the fourth step, the previously determined daily rate is now multiplied by a factor that is intended to reflect the seriousness of the violation. For this purpose, the seriousness of the accusation is firstly determined for the individual case on the basis of the criteria under Article 83 (2) of the GDPR. The degree of seriousness of the violation is classified in the categories 'minor,' 'medium,' 'serious,' and 'very serious.' For the degree of seriousness, a factor is then ascertained from a table by which the basic value is multiplied. Within the table or, ultimately, in the choice of the multiplication factor, a distinction is made between formal violations according to Article 83 (4) of the GDPR and material violations according to Article 83 (5) and (6) of the GDPR.

If the degree of the offence is assessed as 'serious,' the following multiplication factors result, for example:

- formal violations: 4 to 6; and
- material violations: 8 to 12.

However, in the case of a material and very serious violation, there is no clear limitation of a factor. Moreover, the factor to be multiplied is at least 12, although in this case the factor may not be arbitrarily determined. In any case, the limit is set by the individual case related fine framework.

Adjustment of the determined fine

The completion of the calculation methodology for the framework of fines is probably the most interesting step in practice. In this last step, the previously calculated amount of the fine is adjusted on the basis of all circumstances that speak for and against the company concerned, insofar as these have not previously been taken into account when classifying the degree of seriousness and determining the multiplication factor. According to the concept of the DSK, this includes 'in particular all circumstances relating to the violator (cf. the catalogue of criteria of Article 83 (2) of the GDPR) as well as other circumstances, such as a long duration of the proceedings or an imminent insolvency of the company.' After this adjustment, the fine is fixed in accordance with the concept.

Expected effects on the determination of fines in Germany

The turnover-oriented concept of the DSK is comparable to the Federal Cartel Office ('Bundeskartellamt') guidelines for the determination of fines in antitrust proceedings[4], which, as is well known, leads to high fines in cartel law. In this tendency, it is to be feared that companies with high turnover in particular will have to expect significantly higher fines. This is at least the case if no significant corrections are made by adjusting the basic value, in step No. 5. The calculation of the daily rate in steps No. 1 to No. 3, and the multiplication factor to be determined in the fourth step of the concept of the DSK, mean that even minor formal violations may result in fines in the millions for companies with high turnover. It is questionable whether, and how in practice, a previously calculated fine in the millions can still result in a fine of €100,000, for example, by means of a correction in step No. 5. In any case, it is to be feared that, despite the possible adjustment, the amount determined in steps No. 1 to No. 4 will at least have a certain 'anchor effect' for the calculation of the final fine. However, it may be assumed with regard to the aim of the concept, that this anchor effect was intended.

Consequences for practice

In general, it can be expected that the German data protection authorities will no longer be considered to be moderate in setting the level of fines in the future. Instead, companies will have to be prepared for higher fines, as the most recent fine of €14.5 million imposed in Berlin shows. Should a company come into the focus of a supervisory authority, a cooperative and solution-oriented collaboration is recommended in any case. This is, on the one hand because, according to the law and in the spirit of improving data protection practice, the supervisory authority does not have to impose a fine at all. On the other hand, constructive cooperation allows the supervisory authority to reduce the level of fines.

However, due to the various open aspects in connection with the fine model of the DSK, it can also be assumed that German courts will increasingly deal with the determination basis and the proportionality of a fine. In particular, it will have to be clarified whether the previous year's turnover of the company should be a relevant point of reference and whether, despite Recital 150 of the GDPR, an antitrust law definition of a company according to Article 101 and Article 102 of the Treaty on the Functioning of the European Union should be applied. The question also arises as to how the average annual turnover is to be determined for companies which have no turnover from the previous year.

Irrespective of the expected practice of determining fines and the legal questions regarding the fine concept, companies may also attempt to use the DSK's provisions for their own purposes. Thus, the concept could be used in the future to carry out their own risk evaluation under data protection law with regard to potential fines in a more substantiated manner and without the general reference to the maximum percentages or amounts in the millions mentioned in Article 83 of the GDPR. Violations in the company identified by internal data protection audits could rather, in line with the concept, at least roughly be determined and summarised by potential fines. In this way, the management is in any case given a somewhat more concrete picture of the potential financial risks. This basis could also facilitate the prioritisation of necessary data protection measures and the calculation of any provisions.

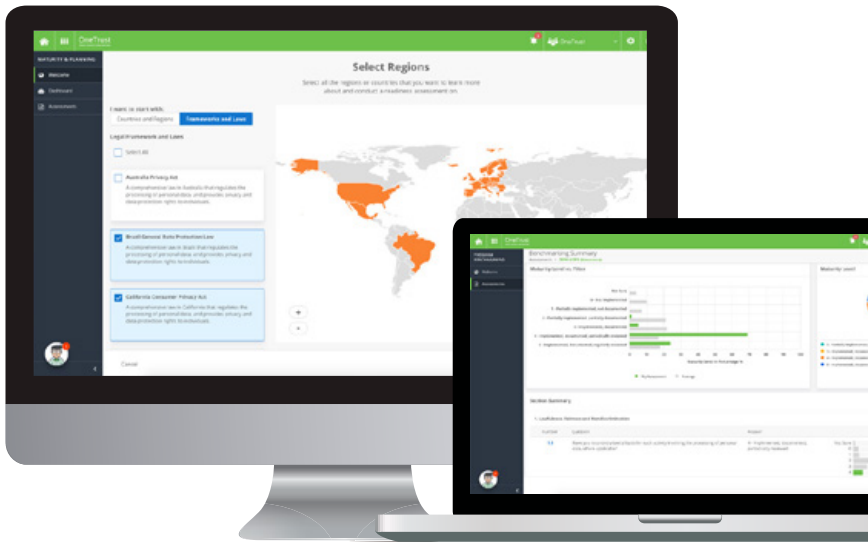
The DSK model can even be taken into account in company acquisitions. For example, the buyer can use the concept to assess the data protection violations identified in the course of due diligence at the target, justify the resulting risks more transparently to the seller, and finally, negotiate the identified potential risks of a fine, e.g. within the scope of the purchase price. In the sense of a more concrete evaluation basis, insurers are also likely to be interested in using the model when developing their products.

1. Concept of the independent German federal and state data protection authorities for the determination of fines in proceedings against companies, available in German at: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bußgeldkonzept.pdf
2. Own translation by the author.
3. Concept (fn. 2), p. 1.
4. Bundeskartellamt, Leitlinien für die Bußgeldzumessung in Kartellordnungswidrigkeitenverfahren vom 25.06.2013, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Leitlinien/Bekanntmachung%20-%20Bußgeldleitlinien-Juni%202013.pdf?__blob=publicationFile&v=5

OneTrust Maturity & Planning and Program Benchmarking Solutions

DEMONSTRATE ACCOUNTABILITY & ORGANIZATIONAL READINESS, PRIORITIZE REQUIREMENTS FOR COMPLIANCE & PROVIDE EXECUTIVE-LEVEL VISIBILITY

- Quickly assess your organizational readiness for compliance and plan your privacy programs accordingly
- Built-in readiness assessment templates across privacy and security frameworks such as the CCPA, GDPR, Privacy Shield, ISO 27001, NIST and APEC CBPR
- Powered by the OneTrust DataGuidance Regulatory Research Portal, the most comprehensive source for privacy, security, and third party risk research



CHOOSE FRAMEWORK

Assess maturity against relevant laws & frameworks

ASSESS MATURITY

Guidance and collaboration in the assessment process

BENCHMARK

Benchmark your maturity against industry peers

PLAN REMEDIATION

Identify gaps with intelligence engine recommendation for remediation

REPORT ON PROGRESS

Dashboards and reports to demonstrate progress to board and executives

RE-ASSESS OVER TIME

Layer on new regulations and frameworks as your business and the regulatory landscape evolves

READY TO GET STARTED? **TRY FREE FOR 14 DAYS AT DATAGUIDANCE.COM**

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

ATLANTA | BANGALORE | HONG KONG | LONDON | MELBOURNE
MUNICH | NEW YORK | SAN FRANCISCO | SÃO PAULO

OneTrust is the #1 most widely used privacy, security and third-party risk technology platform trusted by more than 4,500 companies to comply with the CCPA, GDPR, ISO27001 and hundreds of the world's privacy and security laws. OneTrust's primary offerings include OneTrust Privacy Management Software, OneTrust PreferenceChoice™ consent and preference management software, OneTrust Vendorpedia™ third-party risk management software and vendor risk exchange and OneTrust GRC integrated risk management software. To learn more, visit OneTrust.com.

INTERVIEW

OneTrust DataGuidance spoke with Tumi Atolagbe, Information Governance and Risk Advisor at the British Council in November 2019. Tumi shared her views on what guidance is now needed from regulators with regard to the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') as well as the key steps taken within the organistation in its readiness for the GDPR.

What were the key steps taken within your organisation in its readiness program for the GDPR?

Our department was keen to ensure that the GDPR was not just a one-time thing, a standalone gesture that was a tick-box exercise and then forgotten about. So, in building a compliance program which lasted and was part and parcel of everything that we did, we took the GDPR and Privacy by Design concepts and built them into our project management standards. Now what this means in practice is that as a project driven organisation, key considerations to the GDPR and Privacy by Design must be thought about at the outset of any new project initiation and then woven into the fabric of its implementation.

On an operational level, we took steps to uplift our major contracts to bring them in line with the GDPR requirements with vendors and suppliers. Our internal policies also underwent a transformation program through the Information Governance minimum standards portfolio. Now, what this means is that any internal policies which account for the processing of personal information can adequately guide our employees on what their obligations are when handling that information.

All of this was then backed up by an internal communication strategy. This was designed to convey key messages to the business about what we doing to prepare for the GDPR. This was done to ensure that we were not just doing this in silo, and actually, we are going to bring the wider business along with us on this journey.

Since the implementation of the GDPR, have your key focus areas changed in your role?

Implementing the GDPR was a broad and extensive process. So, as we move forward now, it is about identifying with which tasks we are confident that the business are aware of in terms of their obligations when handling personal information, and that actually, they have got a solid first line of defence approach to their obligations as well.

As we hone in now on what needs more of our focus, it is about preparing our organisation for the Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ('the Draft ePrivacy Regulation'). We need to consider what the requirements are for this and how will this pose new challenges to the business.

So, as new and emerging technologies become more prevalent, we are now focused on equipping our organisation with the tools needed to deploy these in a privacy strong environment. For example, a key focus area of my role now is to build the artificial intelligence ('AI') framework for the British Council. My focus is to do that with privacy at its centre, focus, and core.

How have you built your program to ensure ongoing compliance?

Embedding the data protection and privacy requirements into the project management standards means that the organisation is very much aware of what their obligations are under the GDPR. I think having these requirements in the product management standards now means that our organisation can consider everything from a privacy perspective, and this is to ensure now that compliance is ongoing rather than a stand-alone gesture.

I also think that compliance is a two-way street. So, we as a data protection team are readily available to provide advice, assistance, and guidance on data protection matters. However, at the other end we've got the project teams who are now mandated on a quarterly basis to report back to do management control checks about how they are complying with the GDPR, and demonstrating this. And these controls cover a number of matters, such as anti-fraud and child protection, but for us an information governance and risk management obviously, the focus for us is data protection.

Have national variations regarding the derogations permitted for under the GDPR impacted your organisation and in which ways?

Due to the nature of our organisation, we are vulnerable to national variations, globally but also across the EU, with regard to how those countries have implemented the GDPR. We are an international organisation, we operate in over 100 countries, but looking at the national variations for the GDPR, we are definitely vulnerable in areas such as children's consent and the age that that consent can be given.

In addition, let's look at statutory obligations with regard to retention periods and certain records management processes. Germany, for example, is very clear and strict on what their retention periods of applicant data are, such as human resources data and CVs, for example. In the UK, there's a bit more scope for organisations to decide on what the retention period is. Looking at the statutory obligations, this has a knock-on affect on employment legislation, for example. Employment legislation varies massively across the EU, and this then affects how we have to handle our employee personal information across the organisation.

With all of that, we have a network of information governance advisors, like myself. They operate regionally and we are a team that specialises in global data protection laws. So, as a mandatory minimum, we look

Embedding the data protection and privacy requirements into the project management standards means that the organisation is very much aware of what their obligations are under the GDPR.

Tumi Atolagbe Information Governance and Risk Advisor at the British Council

to the UK Data Protection Act 2018 and then conduct local law analysis on which of those are stricter, and then scale those into our regional privacy programs.

What aspects of the GDPR do you feel require further guidance from the regulators and why?

As new and emerging technologies such as Big Data analytics and machine learning become more prevalent, organisations such as ourselves definitely feel the pressure to keep up with these and become more agile in how we deliver our goods and services. So, as we explore the benefits of these new, innovative technical processing ideas, what will these looking like in terms of archiving in the public interest or statistical historical and scientific research purposes, and actually with these, what are the ethical considerations for what we should be thinking about when we deploy these new technologies? I also think it is not just about the guidance, the GDPR has given us, such as articles, recitals, and national guidance from data protection authorities. What we need now is case law. We have seen some very high-profile cases with regard to cookies, damages, and what the threshold is for that. And I think what we need with those is now for the regulatory fines to come together and help us signal to our board about the associated risks of getting things wrong.

How do you expect EU data protection law to continue to develop in the coming years?

Intellectual property and data protection is a massive area which overlaps. How do we advise our organisation when something is intellectual property and when it is someone's personal data, when it is both, or how about when it's neither. We're trying to communicate our rationale for deciding this to an individual making a request. As I mentioned before, we've got new and emerging technologies, and these pose massive and quite niche privacy issues. Original concepts like data controller and data processor, with regard to algorithms, for example, and deciding on processing, what would the future of this look like. And also, we have got the European Commission's High-Level Expert Group on Artificial Intelligence. They have given us an assessment list on how to make trustworthy AI, what are the legal guidelines, and what are the technical issues. So yes, that is useful, but something binding across the EU either from the European Union or from national data protection authorities, or even statutory implementation, would definitely be worthwhile in seeing where this area goes in the future.

The 'Thought Leaders in Privacy' interview series is filmed across the world with leading privacy professionals discussing how privacy connects with businesses and society.

You can now watch all of our 'Thought Leaders in Privacy' interviews through the OneTrust DataGuidance Video Hub.

platform.dataguidance.com/videohub

Israel: Data protection compliance and loyalty schemes: Part 1

The Israeli Privacy Protection Authority ('PPA') has recently published its report[1] ('the Report') on compliance with the Protection of Privacy Law, 5741-1981 ('the Privacy Law') and the Protection of Privacy Regulations (Data Security) 5777-2017 ('the Regulations'). Dan Or-Hof, Founder of Or-Hof Technology and IP law firm, discusses the Report and what it reveals about the state of compliance concerning privacy and data protection.

While the review behind the Report had focused on various parts of the Israeli economy, the Report only contains findings on loyalty schemes.

Two important deficiencies that the Report highlights:

- local entities and branches of international corporations rely on the privacy and information security practices of their corporate headquarters. They do not implement appropriate controls and measures under Israeli privacy laws; and
- fewer than 50% of the inspected entities secure data adequately.

Over the 2018-2019 period, the PPA conducted a sweeping review on the state of privacy compliance in Israel in relation to the following parameters:

- data protection governance;
- database management;
- information security; and
- outsourcing.

The PPA review is commendable and has raised awareness of privacy and information security compliance. However, as the PPA lacks sufficient enforcement powers and resources, Israeli businesses have yet to achieve adequate compliance levels.

In the framework of the review, sectors inspected were, for example, mental health clinics, educational online platforms for children and educational institutions, data storage services, tourism, non-profit organisations, trade unions, and loyalty schemes.

Of all the sectors inspected, the PPA marked loyalty schemes as one of its most significant regulatory targets. The reason for this lies in the unique characteristics of loyalty schemes, in terms of privacy protection. Loyalty schemes control or process large amounts of sensitive identifiable information about customers, including their consumption habits. They also share such information with third parties and interact with their clientele, either directly or through outsourcing services.

These unique characteristics require loyalty schemes to adhere to strict provisions under the law in relation to all parameters of the compliance review, namely, data protection governance, database management, information security, and outsourcing.

In that sense, though the Report only refers to loyalty schemes, it can shed light on the general state of privacy compliance in Israel.

For the purposes of the compliance review, the PPA set the following compliance scale:

- high level of compliance (80% to 100%);
- medium level of compliance (50% to 80%); and
- low level of compliance (less than 50%).

In accordance with the above scale, the below reviews the parameters, starting from the lowest scoring.

Outsourcing

Out of all the examined parameters, outsourcing was found to have scored the lowest in relation to compliance. According to the Report, 68% of inspected entities have a low and inadequate level of compliance with outsourcing rules. Another 14% have a medium level of compliance, and only 18% comply with the rules satisfactorily.

Deficiencies in relation to outsourcing

The main deficiency concerns the processing of personal information by third parties, while inspected entities had not taken sufficient steps in advance to assess the level of risk to which data subjects might be exposed.

Therefore, the Report suggests that:

- inspected entities that use the services of third parties for processing data must examine the information security risks involved in such engagements beforehand;
- inspected entities must execute a contract with third-party outsourcing service providers, and include all provisions of Article 15(a)(2) of the Regulations. These include the outsourcing service provider's obligation to report, at least once a year, to the database owner about the service provider's performance according to the Regulations and the agreement, and notify the database owner when a security event occurs; and
- inspected entities must implement appropriate controls and supervision measures to ensure that the outsourcing service provider processes personal data in accordance to the Regulations and the agreement.

Data protection governance

According to the Report, 35% of inspected entities have a low and inadequate level of compliance

with data protection governance rules. Another 20% have a medium level of compliance, and 45% comply in a satisfactory manner.

Deficiencies in relation to data protection governance

The Report suggested that:

- database managers were not appointed as required;
- database documents were not created and managed;
- roles and responsibilities were assigned to a specific officer in a manner that may give rise to a conflict of interest;
- there is lack of control and supervision by the representatives or Israeli branches of international entities on privacy and information security procedures concerning loyalty schemes, and a lack of aligning such procedures with the law; and
- procedures and employee training material which should address privacy protection only referred to information security.

Surprisingly, the PPA mentioned the obligation to register databases, although this requirement under the Privacy Law is not enforced in practice, and the large majority of database owners in Israel fail to register their databases. The PPA has indicated that database owners should register their databases and make sure that the identity of the registered database managers reflects the identity of the actual managers.

Information security

According to the Report, 20% of inspected entities maintain a low and inadequate level of compliance with information security rules. Another 32% have medium levels of compliance, and only 48% comply in a satisfactory manner.

The deficiencies in relation to information security

The Report suggests that there is:

- deficiencies in managing authorised access to databases;
- a lack of restrictions on using portable devices and lack of proper encryption; and
- entities with ISO 27001 information security management standard who had mistakenly thought themselves exempt from regulations and inspection procedures.

In response, the PPA suggested that:

- businesses ensure that there are access authorisation mechanisms in accordance to Articles 8 and 9(a) of the Regulations;
- businesses manage portable devices properly, including by restricting access to databases through these devices, implementing appropriate security measures, and using adequate encryption methods;
- entities with ISO 27001 certification follow the PPA Directive 3/2018 and comply with the requirements under the applicable laws, in addition to their ISO 27001 certification procedures and controls;
- entities ensure that they have in place the necessary information security measures and controls, and that all matters listed under Article 4 of the Regulations are maintained and reviewed periodically; and
- entities must provide information security and privacy training for every new employee and on an annual basis for all employees.

Notably, the Regulations require database owners to conduct privacy training once every other year, not annually. Additionally, this requirement applies to database owners who are subject to medium and high levels of security under the Regulations, for example, database owners holding databases who are subject to basic levels of security under the Regulations are exempted. It would appear that the PPA has mistakenly broadened this requirement.

Database management

According to the Report, 20% of inspected entities have a low and inadequate level of compliance database management rules. Another 23% maintain a medium level of compliance, and 57% comply in a satisfactory manner.

Deficiencies in relation to database management

The Report suggested the following:

- deficiencies in defining the databases and their purposes;
- lack of transparency regarding lawful grounds for collecting personal information;
- lack of proper notices in direct mailing activities; and
- data subjects are not informed of their right to request access to their personal data. Notably, the law provides data subjects with right of access to, and rectification of, their personal data. However, database owners are not required to inform data subjects of their right. It would appear that PPA guidance on this matter is not aligned with the provisions of the Privacy Law.

The PPA guidelines suggest:

- mapping all existing databases, and, accordingly, registering unregistered databases or updating existing registrations with the PPA Registrar of Databases;
- ensuring that registered details of databases include the purposes of managing the loyalty schemes and details relating to direct mailing and to the provision of direct mailing services, as applicable; and
- informing and allowing data subjects to exercise their right of access and rectification.

At the conclusion of each review, the PPA required each inspected entity to specify its commitments in writing by an executive officer in relation to remedying all deficiencies identified in the review.

Undoubtedly, the PPA's review has successfully spurred many businesses into conducting comprehensive self-assessments, resulting in a considerable improvement in terms of privacy and information security compliance. The PPA will consider examining in the future the relative level of compliance with other loyalty schemes.

Dan Or-Hof CIPP/E ; CIPP/US ; Founder

dan@or-hof.com

Or-Hof Technology and IP law firm, Tel Aviv

Part II of this article, where Dan examines the compliance deficiencies highlighted in the Israeli Privacy Protection Authority's report on the inspection procedure for entities that run educational sites and apps designed for minors, is available now on the OneTrust DataGuidance Regulatory Research Platform.

1. Available, only in Hebrew, at: https://www.gov.il/he/departments/news/customer_clubs_privacy

Uruguay: Decree on protection of data published in Official Gazette

The Decree No. 64/2020 ('the Decree') on the Regulation of Articles 37-40 of Law No. 19.670 of 15 October 2018 and Article 12 of Law No. 18.331 of 8 November 2008 ('the Law') was published, on 21 February 2020, in the Official Gazette and has been approved by the Council of Ministers. In particular, the Decree contains new provisions on the protection of personal data, and seeks to provide people with a level of protection in line with new technological developments and evolution of forms of data processing.

In addition, the Decree amends the Law with regard to:

- territorial scope;
- personal data breaches;
- data protection officers ('DPOs');
- proactive responsibility; and
- and security measures.

The Decree also implements the notion of Privacy by Design to ensure that the design of databases, processing operations, applications, and computer systems is made in line with principles including data minimisation, pseudonymisation, consent, and other measures established by the Uruguayan data protection authority ('URCDP').

Security measures

Florencia Castagnola, María Sofía Anza, and Ángeles Castaingdebat Castro, Partner, Senior Associate and Junior Associate at Guyer & Regules respectively, told OneTrust DataGuidance, "Data processors and controllers must adopt an active role in implementing adequate technical and organisational measures and must assure an adequate treatment of personal data. The adopted measures will need to be documented, periodically reviewed, and evaluated in order to prove their effectiveness. This document will need to be available upon URCDP's request".

In particular, the Decree introduces the concept of Privacy by Design and notes that the person in charge of processing must incorporate into the design of databases, processing operations, applications, and computer systems, measures aimed at complying with personal data protection regulations.

For instance, the technical and organisational measures adopted can include pseudonymisation and data minimisation,mechanisms to ensure the exercise of the data subject rights, and documentation of consent or other fundamental legal basis to the treatment of personal data. Moreover, the Decree notes that, due to the importance and volume of information processed by multiple organisations and possible security breaches, it is essential to establish a clear regime regarding the procedures to be performed in the event of such a breach.

Guillermo Duarte, Senior Associate at Bergstein Abogados, told OneTrust DataGuidance, "According to the Decree, the party responsible for the treatment of the data affected must communicate the breach to the URCDP within the next 72 hours of having become aware of the breach. This communication must contain relevant information such as the date of the breach, its nature, the personal data affected, and the possible impacts. Further, a notification must be made to the data owners in a clear and simple language. Finally, once the breach has been solved, a detailed brief must be filed with the URCDP describing the breach and the security measures adopted. This applies both to public and private entities without distinction."

Scope of Application

Castagnola, Anza, and Castaingdebat Castro added "In accordance with the Law and the Decree, the Uruguayan legal and regulatory framework is applicable in the following cases if the processing of personal data is conducted by a processor or controller located in Uruguay. The

Decree specifically sets forth that the person or entity responsible will be deemed as located in Uruguay when a stable activity is conducted within the country.

> **entities from the private sector which did not previously fall within the scope of the Law will now have to comply with its obligation.**

The Uruguayan legal and regulatory framework [also applies] if the processing of personal data is conducted by a processor or controller located outside of Uruguay, if:

- the processing activities are related to the offering of goods and services directed to Uruguayan inhabitants (according to the Decree, this will be evaluated through elements like the use of language, references to payment in national currency or references to related services offered in Uruguayan territory);
- the processing activities are related to the monitoring of the behaviour of Uruguayan inhabitants;
- established by international public law dispositions or set forth in a contract (contracting parties cannot exclude the application of the Law when processing activities fall within its scope); or
- means located in Uruguay are used for said processing (such as information and communication networks, data centres, and informatics infrastructure in general as stated in the Decree.)

As a consequence of the above, entities from the private sector which did not previously fall within the scope of the Law will now have to comply with its obligation (including the registration of data bases before URCDP)."

Data Protection Impact Assessment ('DPIA')

Under the Decree, the person or entity in charge of the treatment on personal data must carry out, prior to the start of the treatment and if necessary, an evaluation of the impact on the protection of personal data if the treatment involves, among other things, sensitive data as main business, personal information from vulnerable groups, treatment of personal data for purposes of data subject profiling, international transfers of data for which there is no adequate level of protection and large volume of personal data.

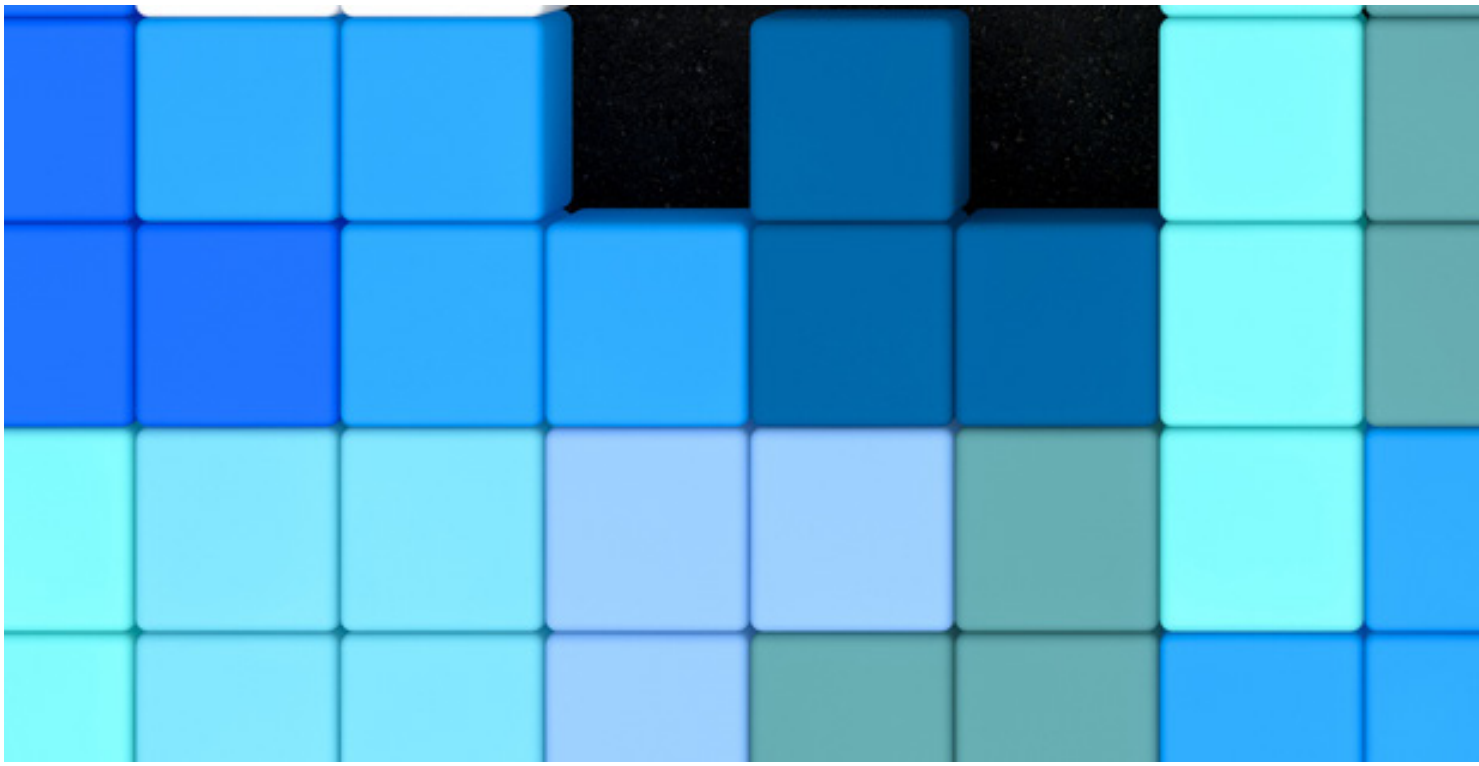
In addition, the Decree notes that DPIAs must contain, at a minimum:

- a systematic description of the treatment performed and its purpose;
- an evaluation of the treatment in relation to compliance with personal data protection regulations;
- an evaluation of the risks to the rights of the data subject; and
- a detailed list of security measures and mechanisms to demonstrate compliance.

DPO appointment

Duarte continued, "The DPO is responsible for formulating, designing and implementing data protection policies, monitoring the compliance with local legislation and regulation, and serving as a link to the URCDP. The Decree restated the requirements of the Law. That is, the entities required to appoint a DPO are public bodies (state or non-state) and private entities owned fully or partially by the State, private companies whose core business entails treating sensitive data (race and ethnic heritage, political preferences, religion, union affiliation, and information relative to health or sexual preference), and private companies who treat large amounts of data (i.e. more than 35,000 individuals). The Decree clarifies the Law's reference to sensitive data and sets forth what is understood as large amounts of data. The appointment of a DPO must be communicated to the URCDP within the first 90 days, from the date in which the data processing activities started." The Decree entered into force on 21 February 2020.

Mona Benaissa Privacy Analyst
mbenaissa@onetrust.com
Comments provided by:
Florencia Castagnola, **María Sofía Anza**, and **Ángeles Castaingdebat Castro**
Partner, Senior Associate, and Junior Associate
fcastagnola@guyer.com.uy
sanza@guyer.com.uy
acastaingdebat@guyer.com.uy
Guyer & Regules
Guillermo Duarte Senior Associate
gduarte@bergsteinlaw.com
Bergstein Abogados



Republic of North Macedonia: New law is "almost entirely aligned with GDPR"

The Directorate for Personal Data Protection ('DZLP') announced, on 18 February 2020, that the Parliament of the Republic of North Macedonia ('Parliament') had adopted, on 16 February 2020, the Law on Personal Data Protection 2020 ('the Law'). In particular, the Law seeks to harmonise national data protection legislation with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), even though North Macedonia is not an EU Member State. The Law applies to wholly or partially automated personal data processing, and addresses controller or processor establishment in the territory of the Republic of North Macedonia, as well as whether the data is processed on the territory of the Republic of North Macedonia or beyond its borders.

Derogation from GDPR

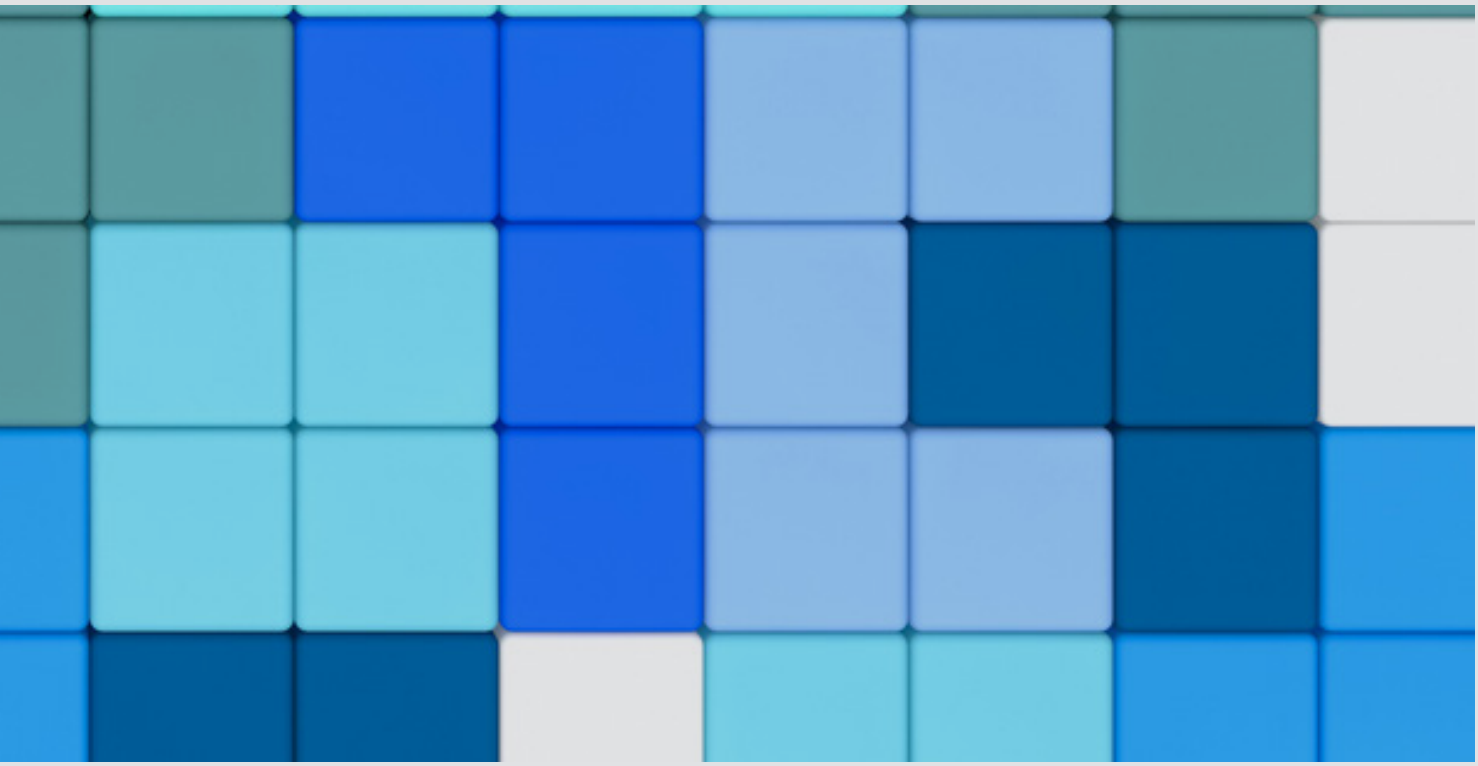
Anna Rizova and Zhulieta Markova, Partner and Associate respectively at Wolf Theiss, told OneTrust DataGuidance, "The Law is almost entirely aligned with the GDPR, but derogations are mainly introduced in terms of procedure and for certain specific data processing situations. The following derogations and special rules under the Law are to be noted [among others]:

- lower threshold for the exemption from keeping records of processing activities;
- special requirements for data protection officers, including fluency in Macedonian;
- the requirements for personal data transfers envisaged in the Law do not apply to transfers from North Macedonia to countries within the EU/EEA, which are subject only to notification before the Agency for Personal Data Protection ('the Agency'). Transfers to third countries, on the other hand, should comply with the transfer requirements set out in the Law (similar to the relevant provisions of the GDPR) and also require the prior approval of the Agency;
- unless explicitly required by law, the processing of health, genetic, and biometric data requires the prior approval of the Agency, even if it is based on the data subjects' consent; and
- processing for direct marketing purposes can only be conducted based on the data subject's consent."

Lawful grounds for processing

Article 10 of the Law contains the legal basis for the lawful processing of data. These are data subject consent, the fulfilment of a contract to which the data subject is party, legal obligations of the controller, the protection of the vital interests of the data subject or another person, public interest or the performance of a public function as established by law. The Law also provides the controller's legitimate interest or the legitimate interest of a third party as a lawful ground for processing, except where such interest overrides the interests or the underlying rights and freedoms of data subjects, especially when the data subject is a child.

In addition, Article 11 of the Law sets out the terms of consent. If consent is given in writing, the request for consent must be presented in a way that can be clearly distinguished from other terms, and it must be comprehensible and easy to understand.



In case of a child under the age of 14, processing is legal only if consent is given by the child's legal representative.

Transforming the DZLP

Gjorgji Georgievski and Marija Serafimovska, Partner and Associate at ODI Law, told OneTrust DataGuidance, "Under the Law, the existing data protection regulatory authority, DZLP, is transformed into the Agency. The Agency is empowered with much broader competencies than its predecessor to oversee the enforcement of the Law, investigate breaches of the Law, and bring legal proceedings where necessary. [The Agency's mandate] includes to:

- promote awareness of the risks, rules, safeguards and rights pertaining to personal data (especially in relation to children);
- advise national and governmental institutions on the application of the Law;
- hear claims brought by data subjects or their representatives, and inform data subjects of the outcome of such claims;
- establish requirements for Data Protection Impact Assessments ('DPIA');
- encourage the creation of codes of conduct and review certifications;
- authorise model clauses and Binding Corporate Rules;
- keep records of sanctions and enforcement actions; and
- fulfil any other tasks related to the protection of personal data."

The Law is almost entirely aligned with the GDPR, but derogations are mainly introduced in terms of procedure and for certain specific data processing situations.

In addition, if the DPIA shows that the processing will cause a high risk to data subjects, controllers must consult the Agency prior to the processing. Furthermore, in case of a personal data breach, the controller must notify the Agency immediately and not later than 72 hours after learning about it, unless it is likely that the breach will not result in a risk to the rights and freedoms of individuals. With regard to enforcement, Georgievski and Serafimovska added, "The Agency is empowered to impose administrative fines to a controller or processor in breach of the rules of up to 4% of the annual worldwide turnover of the preceding financial year. Additionally, an individual who has suffered harm as a result of the unlawful processing of their personal data has the right to receive compensation from the controller or processor for the harm suffered."

Way forward

Rizova and Markova continued, "Ensuring compliance with the Law will be a complex and time-consuming process, which will require the involvement of different stakeholders within the company. Practical measures should be taken, such as adopting the required internal documentation and putting in place appropriate technical and organisational measures. Taking into account that compliance with the new legal framework cannot be achieved overnight, Parliament has envisaged a transitional period of 18 months for companies to align their operations with the new requirements."

The Law entered into force on 24 February 2020.

Petra Molnar Privacy Analyst
pmolnar@onetrust.com

Comments provided by:
Anna Rizova and **Zhulieta Markova**
Partner and Associate
anna.rizova@wolftheiss.com
zhulieta.markova@wolftheiss.com
Wolf Theiss

Gjorgji Georgievski and **Marija Serafimovska**
Partner and Associate
gjorgji.georgievski@odilaw.com
marija.serafimovska@odilaw.com
ODI Law

Malaysia: PDPA amendments include introduction of data breach reporting

The Department of Personal Data Protection ('PDP') released, on 14 February 2020, Public Consultation Paper No. 10/2020 – Review of Personal Data Protection Act 2010 (Act 709) ('the Consultation Paper') which provided the proposed amendments ('the Amendments') to the Personal Data Protection Act 2010 ('PDPA').

In particular, the Amendments include expanding the PDPA's application to data processors, requiring data users to report incidents of data leakage to authorities, expanding data subject rights, and facilitating the cross-border transfer of personal data.

Key takeaways for businesses

Jillian Chia, Partner at Skrine & Co., told OneTrust Dataguidance, "[B]usinesses should be aware that the Consultation Paper proposes obligations on data users to appoint a data protection officer ('DPO'), the reporting of data breach incidents, and the implementation of certain measures, such as data portability, Privacy by Design and security from data collection endpoints. [In addition,] the possible introduction of civil litigation against a data user is a major point [...]. Previously, there was no right of civil action as actions could only be taken by the Public Prosecutor against a data user for breach of the PDPA. [Furthermore,] the proposed extension of the PDPA to Federal and State Governments is a key point to be noted. [The] non-application of the PDPA to Federal and State Governments is presently seen as one of the flaws or loopholes in the existing PDPA, given that government agencies process a substantial amount of personal data."

Ensuring Compliance

The Amendments introduce a number of new obligations for data users, including, among other things, the appointment of a DPO, the establishment of a Do Not Call Registry, and the requirement for data users to provide a clear mechanism on the way to unsubscribe from online services.

> **these Amendments impose additional compliance obligations on businesses and would be likely to increase compliance costs.**

Adlin Abdul Majid, Partner at Hishammuddin Allen & Gledhill, highlighted, "[...] these Amendments impose additional compliance obligations on businesses and would be likely to increase compliance costs." In addition, Chia noted, "In respect to data transfers, it is proposed that no white-listed countries are to be included, meaning transfers out of Malaysia may only be undertaken where exceptions apply, e.g. consent,

the performance of the contract, [...] and this may potentially be burdensome for businesses and be a hinderance to the exchange and sharing of data for commercial purposes."

Chia also commented, "[T]he possible exemption of business contact information from compliance with PDPA (or clarifies the scope of application), and the exception to allow data users to make the first direct marketing call may be welcomed by marketers as this sheds some restrictions on the usage of data for marketing purposes."

Adequacy

Malaysia has not been recognised by the European Commission as providing adequate protection for personal data. However, as outlined within the Consultation Paper, many of the Amendments have been adopted from other data protection legislation, including the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). Chia further discussed that, "While the Amendments are indeed a step in bringing the PDPA more in line with European standards, given the stringent criteria to achieve adequacy status, it remains to be seen whether these amendments alone would be sufficient."

Moreover, Majid further highlighted, "[T]he revision of the PDPA is intended to be in line with the requirements in the GDPR. Many of the requirements in the GDPR are proposed to be introduced into the PDPA, such as Privacy by Design and imposing direct compliance obligations on data processors, although some GDPR requirements are notably absent, such as the right to be forgotten."

Gaps and limitations

Finally, Chia clarified, "[T]here are no provisions in respect of the independence of the PDP, i.e. a supervisory authority independent from the government to enforce the PDPA. [In addition,] the [proposed] breach reporting requirements do not mention whether this would extend to the reporting of breaches to data subjects. [Furthermore,] while the extension of protection for data subjects is a welcomed objective, some of the proposed measures will significantly increase compliance costs. It is hoped that the revisions will be able to achieve a balance between protecting data subjects and imposing undue financial burden on data users particularly small- and medium-sized businesses."

What's Next?

Majid concluded, "[T]he revision outline is drafted in a general manner and does not set out in detail each requirement that would be introduced or amended. While this gives a broad overview of changes that will come about, it is important to also set out the scope of each requirement, to allow assessment of each requirement and potential practical issues arising. We hope that there will be a second public consultation, with details of the Amendments fully set out. All in all, this public consultation paper is a good step forward in bringing the PDPA to be in line with international standards."

The first public consultation is taking place from 14 February to 10 March 2020.

Keshawna Campbell Privacy Analyst
kcampbell@onetrust.com
Comments provided by:
Jillian Chia Partner
jc@skrine.com
Skrine & Co.
Adlin Abdul Majid Partner
aam@lh-ag.com
Hishammuddin Allen & Gledhill

WEBINAR

Key takeaways: Schrems II Case: The AG's Opinion

On 4 February 2020, OneTrust DataGuidance held a webinar with Julia Bonder-Le Berre, Senior Privacy Counsel at Hewlett Packard Enterprise, and Claire François, Counsel at Hunton Andrews Kurth LLP.

This webinar looked at the Advocate General ('AG') of the Court of Justice of the European Union's ('CJEU') Opinion in the so called 'Schrems II' case. This webinar explored, among other topics, data transfers, the validity and effectiveness of standard contractual clauses ('SCCs') and the EU-US Privacy Shield mechanism. Our speakers discussed the Opinion by addressing four key questions, and offered insight to look ahead at the practical implications of the AG's Opinion whilst awaiting the final decision from the CJEU.

Key takeaways

SCCs are valid

Our speakers discuss the importance of the safeguards provided by SCCs and how organisations can manage implementation. While SCCs compensate for deficient data protection standards to facilitate data transfers, the validity of SCCs depend on the safeguards the clauses provide. According to the AG's Opinion, it is advisable that organisations approach the use of SCCs on a case-by-case basis with consideration of third- country national law and the practical implications of terms on importers and exporters of data.

In particular, organisations should address the capabilities of each side to implement safeguards, and need to be well equipped to facilitate the adoption of safeguards and manage any obstacles that may restrict the terms of a SCC.

SCCs should not be considered a 'tick box' exercise

Our speakers highlight that when working with SCCs, both parties involved in a transfer of data need to ensure the other is capable of compliance. In the view of the AG Opinion, SCCs should not be signed without insurance or guarantee that the other party will comply in practice. Our speakers note by way of example that businesses could conduct regular audits of major vendors to check compliance with relevant clauses.

BCRs and alternative derogations

Within the discussion, our speakers consider potential alternatives to SCCs. With reference to the decision taken by the CJEU in 2015 which invalidated the EU-US Safe Harbor framework, our speakers highlighted that the use of Binding Corporate Rules ('BCRs') continue to enable data transfers within an organisation. In addition, alternative mechanisms to legitimise data transfers, such as derogations in relation to consent or contracts with data subjects, are subject to narrow interpretation.

The role of the Ombudsperson is not an adequate safeguard

With recognition that the AG's Opinion did not make a direct ruling on the impact or legitimacy of the EU-US Privacy Shield mechanism, our speakers note that there is still uncertainty. For example, the establishment of an Ombudsperson does not offer data subjects right to access, erasure, or rectification. In addition, the decisions taken by the Ombudsperson are not subject to independent judicial review.

Find previous webinars, jurisdictional overview videos, and interviews with Regulators, supervisory authorities, and thought leaders through the OneTrust DataGuidance Video Hub.

ALL NEW 2020

CCPA MASTER CLASS

WEBINAR SERIES

- Opt-Out Approaches
- Policy & Notice
- Latest AG Guidance
- Training Requirements
- CPREA

Join the Series Attended by Over 12,000 Privacy Professionals!

REGISTER

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

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