Volume 2, Issue 4
July 2020
dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

CHOPPY WATERS

Eduardo Ustaran discusses the impact of Schrems II on international data flows and what the CJEU's decision means for the future of data transfers 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.

Pierre Faller, Christian Dior
Following several years as Data Protection Officer (DPO) within European institutions and agencies where Pierre gained experience and visibility on future data protection regulations, including GDPR, Pierre worked at PayPal between 2017 and 2019 as Privacy Counsel. There, he handled the implementation of various legal GDPR requirements. Now at Christian Dior Couture since 2019, as DPO, Pierre is fully involved in the implementation of a Privacy governance program, at global level. In his spare time, Pierre is an active member of the International Association of Privacy Professionals (IAPP), and organizes as co-chair of the Paris KnowledgeNet Chapter, conferences, debates and roundtables in the area of privacy, data protection and governance.

Giorgia Vulcana, Coca Cola Company
Giorgia is the EU Privacy Counsel for Coca-Cola Europe and she serves as legal subject matter expert and counselor for the DPO Office in Brussels. After completing her studies in Rome, Madrid and Washington DC, she has worked in several lawfirms in Chile and France and as in-house for startups developing data-driven marketing solutions. Before joining Coca-Cola, she was working in the cybersecurity department of Deloitte in Brussels. Giorgia provides advice and training to different business functions, particularly Marketing and IT, to ensure compliance with the GDPR and to coordinate responses and implementation strategies. She has completed her studies in Italy, Spain and the US, she is Member of the Madrid Bar Association and is awaiting admission to the New York State Bar.

Dr. Dieter Kugelmann, Rhineland Palatinate Data Protection Authority
Since October 1 2015, Prof. Dr. Dieter Kugelmann is the Rhineland-Palatinate Commissioner for Data Protection and Freedom of Information. He was born in Landau (Palatinate) and studied law in Mainz and Dijon. After completing his doctorate on a subject from European media law in 1991, he passed the second state examination in 1993. In 2000 he habilitated at the Johannes Gutenberg University Mainz under Prof. Dr. Walter Rudolf on the informational status of citizens. Most recently, he was a full university professor for public law, with a focus on police law, including international law and European law, at the German Police University in Münster. His term of office is eight years; it will end on September 30, 2023.

Odia Kagan, Fox Rothschild LLP
Odia combines her in-depth knowledge of privacy and data security regulations and best practices, both domestic and international, with her keen understanding of emerging and information technologies to provide clients with practical advice on how to design and implement their products and services, consummate their M&A transactions and engage third-party vendors in the United States and abroad. Over the past few years, Odia has assisted more than 80 companies, from U.S.-based multinationals to startups, on their path to compliance with the EU General Data Protection Regulation (GDPR). She leverages her transactional experience leading M&A and tech transactions as well as her ability to break down complex concepts into easy-to-understand action items to provide effective, ongoing counsel to clients in their day-to-day operations.

Alec Christie, Mills Oakley
Alec Christie is a Partner in the Digital Law group of Mills Oakley based in Sydney, Australia. Alec and his team provide advice and solutions in relation to privacy, data/cyber security, electronic marketing/SPAM, e-commerce, sourcing, cloud computing, Big Data analytics, the Internet of Things and social business/marketing. Alec has been recognised as a 'Leading Lawyer' in the IT and IP practice areas every year since 1998, and since 2013 Alec has also been selected as one of the Leading Information Technology lawyers in Australia by Who's Who Legal and described as a "distinguished practitioner...lauded by clients for his excellent advisory work in...privacy."

James Wong, Mills Oakley
James is an Associate in the Digital Law group at Mills Oakley, one of Australia's largest and oldest national law firms. With his team, James helps clients navigate the opportunities and risks associated with the digital economy, providing solutions in relation to digital transformation (procurement/outsourcing), privacy and data protection, cybersecurity, emerging technologies and the regulation of digital business models. James is a member of Melbourne's fast-growing tech community and a World Economic Forum 'Global Shaper'.

Image production credits
Cover / page 4 image: pawel.gaul / Signature collection / istockphoto.com
Page 8-9 image: jez_bennett / Essentials collection / istockphoto.com
Page 14 image: DKosig / Portfolio / istockphoto.com
Page 18-19 image: Kate Ausburn / Unsplash
Page 24-25 image: slovegrove / Essentials collection / istockphoto.com
Page 28-29 image: real444 / Signature collection / istockphoto.com
Page 30 image: ArtRachen01 / Portfolio / istockphoto.com
Page 32-33 image: Victoria Palacios/Unsplash
Page 36 image: Nick/Unsplash

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

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

Throughout the years, different legal frameworks have attempted to place limitations on international data transfers for different reasons and with different degrees of success, but data has continued to flow

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

Editorial: Choppy waters

Most people know that water covers nearly three quarters of the Earth's surface. We also learn in school about the water cycle involving evaporation and precipitation, which basically means that water is always moving. And whether we learnt it in school or not, we all know that water is precious and vital for all forms of life, including our own. So, while it has become a cliché to say that data is the new oil, it is actually more accurate to say that data is like water - ever present, fluid and vital. Data is also big business - particularly personal data - but as with water, no matter how abundant it may seem, personal data must be handled responsibly and with respect. One of Earth's most powerful courts - the Court of Justice of European Union ('CJEU') - has now confirmed what this responsibility means in a global context and, as a result, we are in choppy waters.

With the relentless growth of digital networks over the past 30 or 40 years, global data flows have become an essential part of how we live, work and communicate. Like the water in our oceans and seas, data flows in interconnected and unrestricted ways. The internet owes its very existence to the objective of providing reliable communications during a serious international crisis. Throughout the years, different legal frameworks have attempted to place limitations on international data transfers for different reasons and with different degrees of success, but data has continued to flow. The CJEU decision on the Schrems II case unequivocally confirms that such limitations must indeed be maintained under European law. The real question is how to make such rules work in practice when the truth is that data is bound to continue to flow.

International data transfers are not the result of tech companies' business plans. They are the result of a technological evolution that has sought to meet our human demands. As progress was driven by our digital capabilities, international data transfers became essential for the modern world. That was true yesterday and remains true today, irrespective of the legal nuances that we now face. So the answer to any legal framework that seeks to restrict international data transfers in the name of the protection of personal data is not to stop the data from flowing. Data localisation is not a solution. It is short-sighted political wishful thinking. The CJEU is aware of that and has not called for the retention of personal data within the boundaries of the EU. What we need is creative but realistic ways to seek the protection sought by the law irrespective of the forces of the tide.

In the world of data, the tidal forces also move in many different directions. Much of the current focus is placed on transfers of data from the EU to the US, but it would be wrong to present Schrems II as purely a conflict between European data protection and American surveillance. The CJEU's decision is actually about finding a formula to navigate the turbulent waters of global data transfers that is compatible with the requirements of the GDPR and the political realities of the world we live in. Government access to data is one of such realities - in the US and everywhere else. The CJEU is steering us - as it has always done - in a direction of travel which seeks a balanced approach to that access rooted in democratic principles and effective remedies for individuals.

This leaves us looking for solutions. But we are not stranded in a dinghy in the middle of the ocean. We should rely on the CJEU's wise words to find a way forward based on privacy and data protection safeguards that ensure an adequate protection for our digital lives. Personal data will never stop flowing but that does not mean that we should be resigned to drown in a sea of legal conflicts.

Published by OneTrust DataGuidance™ | July 2020

INTERVIEW WITH:

GIORGIA VULCANO EU PRIVACY COUNSEL AT COCA COLA COMPANY

THOUGHT LEADERS IN PRIVACY

OneTrust DataGuidance met with Giorgia Vulcano, EU Privacy Counsel at Coca-Cola Company, in February 2020. Giorgia discussed GDPR compliance and explained the benefits that having a GDPR compliant program has had on the company, as well as how the program has been built to ensure ongoing compliance. She also discussed how her job role has changed as laws have been developing, and how she expects privacy laws and trends to develop in Europe over the next few years, especially within new technologies and data ethics.

What have been the benefits for your organisation in implementing a GDPR-compliant program?
So for me, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') is more than just the law. It has really set the environment for companies to play by the same rules in the markets, to abide to the same privacy principles, and therefore, to create incredibly valuable and ethical products and services that have an enhanced data protection for consumers, without losing the competitiveness. This is not just an opportunity for companies, but it's also an opportunity for consumers to actually access incredibly valuable experiences that are more sustainable, that are safer, and that are more human centered, and the social impacts for this is amazing. I think that today, because of the GDPR, we can create and innovate in a completely different way that is much more sustainable and ethical.

Since the implementation of the GDPR, have your key focus areas changed in your role?
Before even talking about how the key focus areas of my job have changed, the first thing that really has changed was my approach. So, I am a lawyer, and in my day to day job, the people that I talked to the least were lawyers. I work in cross-functional teams, which doesn't mean meeting with them once a week, but working with them on a daily basis and we work together as a team throughout the whole product lifecycle. We combine our skills, our backgrounds, and our experience to embed privacy in the design of a product or a service and ensure that it stays across the whole product lifecycle. For me, this is incredibly innovative, I think it's really the future, and it has helped me also to really empathise with the business and understand how they work, what is their goal.

> **Consumers are looking for products and services that have a purpose, that are sustainable, that are ethical, and that embed privacy, and I feel like the whole ecosystem around this is fostering this even more**

It has also changed how my profile is developing. I'm starting a course on legal coding, which you know, is something I would have never expected years ago. But today, I realise that it's not enough to talk about the law without understanding all the other aspects around data, including IT, and I see the same thing on the other side. So, also, I see people and business and marketing and agile coaches talking the GDPR language, so I think that's really that has been the biggest change for me

How have you built your program to ensure ongoing compliance?
The GDPR is not a one-time thing. The GDPR is a long-term commitment, and I have been really empathising with the business to understand the context and build up tools, decision trees, guideline, and function specific trainings to really give them all the tools and the measures that they need to implement the GDPR in their day-to-day work. This is the most sustainable approach that you can build in, because it's not just the responsibility for legal, it's really the responsibility for every employee to abide by the GDPR but I think that legal has an important role in building up these tools.

We also built up a GDPR intranet site that has everything. It has the templates, it has the frequently asked questions, it has the right contacts, and it allows employees to either reply to very simple, straightforward questions, but also to have a good understanding of what the roadmap is to build a GDPR compliance project. We worked really hard to provide those tools through to the employees and to also help them understand how to create value for the consumers through data protection.

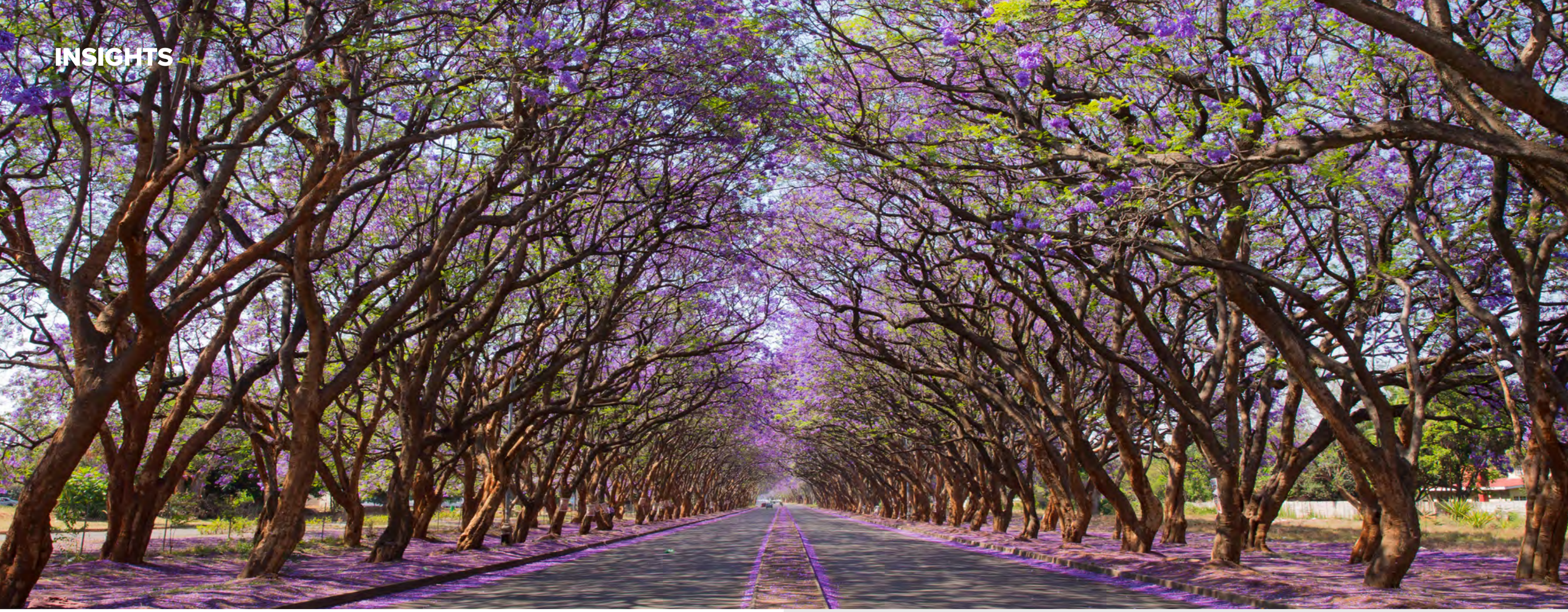
What further developments in European privacy law do you expect to see over the next few years?
Today, the perception from consumers of what is valuable is much more elaborate than before. Consumers are looking for products and services that have a purpose, that are sustainable, that are ethical, and that embed privacy, and I feel like the whole ecosystem around this is fostering this even more. There is a peak in privacy legislation. There are changes in the online environment. Just recently, there have been announcements of limiting or eliminating the use of third party cookies for tracking. There is a great shift in focus towards data ethics and on the importance of embedding data ethics in products and services.

There is also a completely different way of working in the sense that the responsibility is not just on legal to make sure that we are GDPR compliant, but there is a recognition of how the GDPR is bringing value to the data subjects through data protection enhancements and it becomes really a joint effort, a cross functional team working together and providing their expertise and their vision on how to embed privacy in the design of products and services. I think that throughout all this, the key is really transparency, and being straightforward with consumers and telling them what's happening.

Nowadays, we have tools and technologies that bring us to tell consumers how we're passing their data, but in the future, we'll have technologies like blockchain that, in their design, are already embedding that transparency. So, I'm very excited and curious to see how things will further develop.

*Find more interviews like Giorgia's for free via the **OneTrust DataGuidance Video Hub**.*

Access the Video Hub and other free resources at: www.dataguidance.com



Zimbabwe: Cybersecurity and Data Protection Bill

Privacy and data protection have both become major issues for the global economy in recent times. Section 57 of the Constitution of Zimbabwe 2013 (as amended) ('the Constitution') currently provides for the right to privacy, however, on 15 May 2020, the Cybersecurity and Data Protection Bill (H.B. 18, 2019) ('the Bill') was published in the Government Gazette. Whilst at the time of writing, the Bill is not yet in force, the Bill aims to provide some general data protection rules and clarify privacy rights within Zimbabwe. Nobert M. Phiri and Tanatswa S. Mataranyika of Muvingi & Mugadza Legal Practitioners, provide an overview of the Bill and how it may affect businesses in their approach to data protection and cybersecurity.

The Bill is an important and commendable milestone in realising privacy rights and the protection of personal data in Zimbabwe. However, the prospects of the Bill are dependent on the implementation of its statutory provisions. Data privacy regulates all stages of the processing of personal data. However, it is important to note from the outset that cybersecurity threats and vulnerabilities have predated the COVID-19 ('Coronavirus') pandemic, given the vast technological advancements pervading trade markets. The Coronavirus pandemic merely magnifies the potential risk of infringement of personal data and privacy rights in countries where protective legislative frameworks have not been developed for enforcement.

The purpose of the Bill, according to it memoranda, is to:

- consolidate cyber-related offences and provide for data protection with due regard to the Declaration of Rights under the Constitution, and the public and national interest;
- establish a Cybersecurity Centre and a data protection authority ('DPA'), and to provide for the collection of evidence of cybercrime and unauthorised data collection and breaches; and
- provide for admissibility of electronic evidence for such offences.

The Bill also seeks to create a technology-driven business environment by encouraging the development and lawful use of technology, and to increase cybersecurity in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives, and data subjects. Discussed below are some of the main issues identified with the Bill with some brief comments.

Section 4 of the Bill

Section 4 of the Bill deals with the application of the Bill. The clause defines the parameters of privacy and data and what it entails. However, it oddly makes reference to the Protection of Personal Information Act, which is yet to be gazetted as law.

> **The Bill is a welcomed development in advancing privacy and data laws in Zimbabwe**

Section 4 Application

'This Act [the Bill] shall apply to matters relating to access to information, protection of privacy of information and processing of data wholly or partly by automated means: and shall be interpreted as being in addition to and not in conflict or inconsistent with the Protection of Personal Information Act [Chapter.....].'

Section 5 of the Bill

Section 5 of the Bill establishes a Cybersecurity Centre and provides for the designation of the Postal and Telecommunications Regulatory Authority of Zimbabwe ('POTRAZ') as the Cybersecurity Centre. It is commendable that the Cybersecurity centre has been established, but it remains to be seen if POTRAZ will be able to manage this added and important responsibility.

Section 5 Designation of Postal and Telecommunications Regulatory Authority as Cybersecurity Centre

'The Postal and Telecommunications Regulatory Authority established in terms of the Postal and Telecommunications Act [Chapter 12:05] is hereby designated as the Cyber Security Centre.'

Sections 7 and 8 of the Bill

Sections 7 and 8 of the Bill provide for the designation of PORTAZ as the DPA and the functions thereof. Again, PORTAZ has more responsibilities and duties added to its already existing mandate.

Section 7 Designation of PORTAZ as DPA

'The Postal and Telecommunications

Regulatory Authority established in terms of the Postal and Telecommunications Act [Chapter 12:05] is hereby designated as the Data Protection Authority.'

Sections 9-14 of the Bill

Sections 9-14 of the Bill provide the minimum standards and general rules for a data controller processing data. Such provisions are welcome in ensuring the protection of privacy and data rights. Below are Section 9 and 13 of the Bill.

Section 9 Quality of Data

'(1) The data controller shall ensure that data processed is—
(a) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;
(b) accurate and, where necessary, kept up-to-date;
(c) retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed.
(2) The data controller shall take all appropriate measures to ensure that data processed shall be accessible regardless of the technology used and ensure that the evolution of technology shall not be an obstacle to the access or processing of such.'

These provisions seek to enhance privacy and data law in Zimbabwe through regulating transfer of personal information internationally.

Section 13 Sensitive information

'(1) In relation to the processing of sensitive personal information—
(a) the processing of sensitive data is prohibited unless the data subject has given consent in writing for such processing;
(b) the consent may be withdrawn by the data subject at any time and without any explanation and free of charge;
(c) the Authority shall determine the circumstances in which the prohibition to process the data referred to in this section cannot be lifted even with the data subject's consent taking into account the factors surrounding the prohibition and the reasons for collecting the data.'

Sections 15-18 of the Bill

Sections 15-18 of the Bill provide for the levels of security, integrity, and confidentiality of data controllers or their representatives in the protection of data from destruction, unauthorised alteration or access, and other unauthorised processing, and the notification of the DPA of any security breaches. These provisions are a welcome development. Below is Section 18.

Section 18 Security

'(1) In order to safeguard the security, integrity and confidentiality of the data, the controller or his or her representative, if any, or the processor, shall take the appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data.'

Sections 26-27 of the Bill

Sections 26-27 of the Bill outline the protection of the rights of data subjects who are children or who may otherwise be incapable of exercising their rights due to some other legal incapacitation in terms of the Bill. These provisions entrench children rights as enshrined in the Constitution.

Section 26 Representation of data subject who is a child

'Where the data subject is a child, his or her rights pursuant to this law may be exercised by his or her parents or legal guardian.'

Sections 28-29 of the Bill

Sections 28 and 29 outline the rules on permissibility and non-permissibility of the transfer of data outside the Republic of Zimbabwe and the requirements for the authorisation or non-authorisation of the same. These provisions seek to enhance privacy and data law in Zimbabwe through regulating transfer of personal information internationally.

Section 28 Transfer of personal information outside Zimbabwe

'(1) Subject to the provisions of this Act, a data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out.'

Section 29 Transfer to a country outside the Republic of Zimbabwe which does not assure an adequate level of protection

'(1) A transfer or a set of transfers of data to a country outside the Zimbabwe which does not assure an adequate level of protection may take place in one of the following cases—
(a) the data subject has unambiguously given his or her consent to the proposed transfer;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request'

Section 33 of the Bill

Section 33 of the Bill sets out the offences and the penalties.

Section 33 Offences and Penalties

'(1) Any member of staff of the Authority or any expert, contractor, sub-contractor who violates the provisions of this Act shall be guilty of an offence and liable to a fine not exceeding level seven or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.'

Zimbabwean businesses have increasingly evolved to e-commerce. Such a shift has had an impact on how personal data is processed, stored, and transferred, triggering concern as to whether contracting parties, particularly the consumers, are adequately protected in the cyber-environment. The Bill should thus deal with principles on data privacy such as collection limitation, use limitation, and security safeguards. The current law results in a lot of legal uncertainty and risk between the consumers and the business enterprises. Thus, the Bill is a welcomed development in advancing privacy and data laws in Zimbabwe.

While some institutions may adopt international best practice on collecting and processing confidential information, there remains a need for specific law on data collection, handling, and disclosure.

Nobert M Phiri Partner
phiri@mmmlawfirm.co.zw
Tanatswa S Mataranyika Associate Intern
tmataranyika@mmmlawfirm.co.zw
Muvingi & Mugadza Legal Practitioners, Alliott Group, Harare

Discover more insights from contributors and in-house analyst at dataguidance.com

OneTrust DataGuidance met with Dr. Dieter Kugelmann, Commissioner at the Rhineland-Palatinate Data Protection Authority, Germany in October 2019. Dr. Kugelmann discusses his thoughts on recent amendments to German federal law and trends that the authority have noted in regards to compliance activities, especially with respect to Articles 12, 13, and 14 of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').

What have been the key areas of focus for your authority since the entry into effect of the GDPR?
There have been significant changes really for our authority. First of all, there was a real big need for a consultation, questioning us about what the GDPR is all about, which is now getting better as the people are better informed. However, this public awareness also, of course, raises more complaints, which is good on the one hand because complaints mean that people care about their data, but it is more work for us. So, the tripling of complaints is a fact that we have to cope with.

We have also had to cope with the data breach notifications. They have really exploded for our authority and for all other authorities in Europe and Germany too, because now it is obligatory and we have to find procedures to get along with these data breach notifications. Those were the significant things, and perhaps lastly, what we do now is really enact more orders. Under the Data Protection Directive (Directive 95/46/EC) in the old system, it was more cooperation, it was more recommendation, it was more, 'please don't do that.' Now, we are really acting as an authority with binding legal acts, and we are before the courts, which is absolutely fine because finally then the courts can say what their interpretation is.

What trends have you noted regarding organisations' compliance activities, especially with respect to Articles 12, 13, and 14?
Well, Article 12, 13, and 14 are, in my view, the most complicated and most challenging of all of the GDPR because they have a lot of processes, and we have seen that enterprises which are bigger can cope with it, but small and medium enterprises really have problems.

Actually, in Germany, as a supervisory authority, we think that it is too complicated so it could be changed. Some modifications would be good because it is just too hard for smaller enterprises to fulfil all of their obligations and actually, we see in practice that if we look at any notification, or at any declaration, we find something because it is hard to be perfect. However, most companies have at least tried it, so we would say, 'well, if you tried, it is the first step.' It is complicated enough, and if you are not data driven, for example if your company is a bakery or something, we would be mild about it.

What are your thoughts regarding the recent amendments of the federal law and what impact will it have for organisations?
Germany has seen a sort of a backlash as the amendments made concern more than 150 laws, some of them are more technical and some only the notions, but where it really gets to material modifications, it had to be taken into account that the economy should be able to comply with it. There are certain points where, in my opinion, it does not make sense, and the problem is the communication. The communication of the Parliament, of the Government, of the lawmaker, who say, 'Well, don't take data protection that seriously and try to find solutions.' I do absolutely agree that we should find solutions in practice, and we can change the law at points in certain regards, but not in those regards. The most relevant thing discussed in Germany is at what level you need to have a known data protection officer in an enterprise and how doctors handle data within the medical area.

What has been the workload of the DSK over the last year, and what are the key takeaways for organisations?
This year, I am the chair of the DSK, and what we had as a main material topic is artificial intelligence ('AI') so we produced a declaration in April 2019 on what the GDPR says on AI from our perspective. What we did is to develop a guidance on marketing on the internet because we have some special German rules concerning that, and we explain that they do not exist anymore as now we have GDPR. Therefore, what the result of this is that tracking is only allowed if you have consent, and actually, we implemented that.
So, our authority for example, we actually enacted orders and this order is now before the court. What we also do is collect our experiences of the GDPR, so we will create a report to give to the European Data Protection Board because the Commission will enact a report and we wanted to contribute our experiences. This also means the good and the bad ones. We see where the provisions of the GPDR are maybe not clear enough or where maybe possible changes can made, then on the other hand, what in our opinion should be kept. So, we are playing on the European level playing field, and that's another thing, we had to cope with getting a common opinion across the DSK, and then to go to Europe and to discuss it with 27 colleagues, so that's some organisational problems. But I think we are managed quite well.

What are your authority's priorities in 2020?
We will try to give more support to the European Data Protection Board and look at how we can strengthen our contribution to the debate in Europe, and how can we be more visible perhaps, on a formal organizational side, but also in other aspects. So, I think these are some aspects on a general level, and for my authority in Rhineland-Palatinate I can say that actually what we want to try is to quicken our procedures because we had to learn, of course, like every other stakeholder, how to cope with the GDPR, and with complaints. We were not really prepared for how many data breach notifications we would receive so we wanted to get better at that timewise, and also to cooperate better with our European colleagues.

EU: A privacy guide for AI vendors

With the increased adoption of artificial intelligence ('AI') driven solutions across many industries, regulators are starting to focus on the specific privacy challenges associated with these technologies. Dan Whitehead, Senior Associate at Hogan Lovells International LLP, discusses the range of issues that companies who sell AI solutions need to be taking into account along with practical solutions for compliance.

The use of AI-driven solutions in commercial applications is becoming increasingly pervasive with a sub-branch of AI that is commonly referred to as machine learning being integrated into everyday settings in ways that are already being taken for granted. Machine learning technologies, which are the focus of this article, are used to assist financial institutions in being able to make real-time decisions on whether to accept or reject consumer credit applications, by technology companies to interpret and act upon verbal commands made through home assistants, and healthcare providers to facilitate the search for drugs that could help to defeat COVID-19 ('Coronavirus').

The successful design, development, and use of machine learning is often heavily dependent upon the collection and use of personal data. As a consequence, it is a field that is becoming of increasing interest to data protection authorities.

One such example being the UK Information Commissioner's Office ('ICO'), with the regulator publishing two detailed sets of guidelines on this topic during the past six months and making AI one of its three long-term strategic priorities. Similar efforts are being made in other European countries such as Spain and Germany, while the EU is currently consulting on the broader proposals for regulating AI that goes beyond privacy concerns following the publication if its white paper in February this year.

Why machine learning differs from other technologies

Although it is true that the same general principles of data protection apply to machine learning as to any other technologies that involve the processing of personal data, there are also certain specific characteristics that make such systems different from a common software application, which are discussed below.

Reliance on predictions and inferences

Software that is developed based on 'conventional' programming techniques is commonly only able to receive instructions for a defined set of pre-programmed scenarios. The algorithm will then produce a predictable output based on a number of inputs (e.g. the total price of your order in an online shopping transaction, based on the contents of your shopping basket). Unless the software has been programmed erroneously, then it is commonly expected that the output will be accurate 100% of the time.

Machine learning is different. One of its primary advantages over conventional programming methods is its ability to be able to handle new scenarios that it has not seen before based upon past experiences. However, the drawback of this approach is that the outputs it generates are merely predictions and inferences and not concrete results, meaning that their accuracy may potentially be lower.

Opacity

It can often be difficult for humans to fully comprehend the basis on which a machine learning algorithm has reached a prediction or classification. This is particularly the case with more sophisticated forms of the technology, such as deep-learning algorithms which involve the use of complex artificial neural networks which is often said to create a 'black box' effect. As a consequence, it can be difficult for controllers to provide meaningful information to end-users about the logic involved in making automated decisions or their potential consequences, as required by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').

Use of training data

Where 'supervised learning' techniques are used, then the machine learning model is developed through a process of training. This involves feeding the algorithm a set of example training data (e.g. pictures of faces to train a facial recognition tool), from which the algorithm learns to make inferences in relation to previous unseen scenarios, based on the 'experiences' it derives from such data. This learning process is critical to the development of many machine learning technologies that are in use today. However, in order to perform to a reasonable level of accuracy, it is necessary for large sets of training data (which will commonly include personal data) to be collected and processed.

Automated decision-making

The inferences produced by machine learning models are in many cases then used to generate automated decisions about individuals (e.g. identifying possible known criminals, through facial recognition, based on CCTV images captured in a shopping centre). These decisions will often not involve any form of human review on a case-by-case basis, making it more difficult to detect errors or biases that may have arisen in the production environment.

Six key compliance issues for AI vendors

These distinguishing characteristics form the basis for identifying many of the material privacy challenges that arise in connection with machine learning. For vendors that are involved in the design, development, and sale of models based on such technologies, six examples of the types of common issues that arise under EU data protection law include:

Controllership

It is common industry practice for providers of software solutions to consider themselves to be processors on behalf of their customers, who are each deemed to be a controller. However, this clear distinction between the role of the controller and the processor is often difficult to maintain in the context of machine learning for two reasons.

Firstly, vendors will in many cases wish to 're-purpose' personal data they receive from their customers; converting it into training data in order to make further improvements to their models. Secondly, the decision-trees and neural networks that are regularly used to make predictions, may be sufficiently complex and opaque in nature so that it would be difficult to argue that a customer, who has had limited involvement in the development of the model or knowledge of how it works, is solely responsible for determining the purposes and means of the processing.

Consequently, it is necessary for vendors to carefully consider their controllership status under the GDPR, taking into account the various phases in which personal data may be processed during a model's lifecycle.

Processing of training data

One example of where vendors will almost certainly be considered a controller is in connection with the use of training data. As a consequence, they will commonly be considered solely responsible for ensuring that any personal data that forms part of the training data set is sourced fairly, lawfully and transparently.

This may be particularly challenging where special category data is involved (e.g. in the training of healthcare applications or facial recognition tools). In such circumstances careful consideration will need to be given to whether a relevant exemption is available under Article 9 of the GDPR, taking into account the derogations set out under the local law of the relevant EU Member State.

Bias and discrimination

Although machine learning models make predictions based on past data, and often independent of direct human influence, this does not guarantee they are free from bias or prejudice. In fact, one of the major ethical dilemmas concerning the rise of AI technologies is the possibility for discrimination to be accidentally designed into models by default.

Inherent bias, which results in discrimination on the basis of certain characteristics, such as ethnicity, gender, age, or disability, may be caused by a number of factors. These factors may include unbalanced training data sets, where there is disproportionate representation of one group compared with others, and where the training data reflects historic patterns of discrimination. Bias may also derive from a model that, in a live production environment, is actively taking into account certain inputs which either directly or indirectly result in discriminatory effects. For example, an automated recruitment tool that is able to identify an applicant's gender, may recommend the payment of a lower salary to a successful candidate that is known to be female compared with what it would have recommended being paid to an equivalent male peer, based on it having been taught that the mean average salary for women is lower.

From a privacy perspective, the obligation for a controller to prevent bias in its processing activities derives from the duty to process personal data fairly, taking into account the fundamental rights and freedoms of individuals as outlined under the Charter of Fundamental Rights of the European Union. The GDPR's recitals also confirm that in these circumstances there is a duty to implement appropriate technical and organisational measures, including the adoption of appropriate mathematical and statistical procedures to prevent bias.

Therefore, taking into account the relevant anti-discriminatory laws that apply in the jurisdiction in which they operate (e.g. the UK Equality Act 2010), vendors must consider how they will avoid the potential for bias in the course of the design and development of their models.

Compliance should not be an after-thought, but instead form part of the design and build requirements when the machine learning models are first being developed

Statistical accuracy

In the context of machine learning, statistical accuracy is in general terms a measure of how often a model produces the correct prediction which reflects a ground truth. While not identical to the principle of accuracy under the GDPR, given that many models will involve the production of outputs that are classified as personal data, there are often similarities between the two concepts.

For the majority of models, it won't be feasible to reach a 100% level of statistical accuracy. However, it is important that vendors consider what reasonable steps they can take in the design, development, and testing stages to ensure that accuracy levels are at a reasonable and justifiable level in the circumstances and have appropriate measures in place to identify inherent weaknesses that may exist.

'Explainability'

Due to the potential opacity of models that are based on machine learning, it can be difficult to fully understand how a decision or prediction was reached based on a series of inputs. This is particularly significant in cases where such predictions and decisions impact upon individuals.

The ICO has recently published extensive guidelines that set out its good practice recommendations on explaining AI to end-users. While these guidelines are not legally binding, they provide a useful indicator of the authority's expectations on how many organisations that utilise machine learning technologies will potentially need to enhance their existing approach to transparency.

From a vendor's perspective, it is likely that the onus for adequate end-user transparency will primarily fall upon the shoulders of the customer. Nonetheless, vendors will need to be mindful of the consequences of increased regulatory focus in this area, which will likely result in customers expecting more information to be disclosed about how models operate in practice and the basis upon which inferences and predictions are being made.

Solely automated decision-making

Article 22 of the GDPR sets out the right for individuals to not be subject to decisions based solely on automated processing. In some cases this right will not arise because either the decisions are not fully automated, due to them including an element of human involvement, or they do not produce a legal effect or similarly significant effect on the individual who is subject to the decision (one of the pre-conditions of Article 22's application).

However, there are a growing number of circumstances where machine learning is being utilised to make decisions that may have a material impact on an individual's finances, career or even liberty. Examples include automated decisions on applications for credit, recruitment recommendations, and identification of potential criminals through facial recognition.

From a vendor's perspective, while the ramifications of Article 22 may be more immediately felt by their customers who are dealing directly with the end-users subject to these decisions, it remains important to have an appreciation of whether the model in question may give rise to additional rights. For instance, where a solely automated decision is challenged, it is possible that the vendor will need to be capable of providing a justification for why the decision was correct in the circumstances and undertake a manual review to verify its accuracy.

Complying in practice

When considering how to develop an appropriate governance framework to address the myriad of compliance challenges that have been identified in this article, vendors need to focus on two key areas: being accountable and ensuring that the principle of Privacy by Design and Default is integrated into the AI development lifecycle.

The precise measures that need to be adopted in order to comply with the accountability and Privacy by Design principles will ultimately depend on the circumstances and nature of the model being used.

There are however a number of commonalities in this approach:

- **Build a strong governance team**: It is important that there is senior leadership in this area. Technical teams, including developers, data scientists and system architects need to be involved, working closely with the vendor's data protection officer and legal to identify solutions for how the issues identified above can be practically addressed in a compliant manner.
- **Undertake a Data Protection Impact Assessment ('DPIA')**: DPIAs are important in being able to identify many of the key risks that may present in any given scenario, and form an important component of the documentation that may need to be disclosed to a data protection authority upon request.
- **Consider compliance measures from the start**: Compliance should not be an after-thought, but instead form part of the design and build requirements when the machine learning models are first being developed.
- **Test and monitor performance**: Testing models before they are used in a production environment should help to detect potential frailties, such as bias with respect to particular protected groups or lower than expected levels of statistical accuracy. Ongoing monitoring is also important, particularly in the case of models which are subject to regular updates and ongoing improvements through the use of additional training data.
- **Adopt appropriate policies and procedures**: Have in place policies and procedures which govern how privacy challenges will be addressed in this field from a practical perspective and ensure that employees are adequately and regularly trained so that they understand the company's expectations.

Final thoughts

With increasing scrutiny of the AI industry by regulators and policy makers, it is inevitable that organisations looking to procure machine-learning solutions will become more conscious of the risks involved. It is therefore vital that vendors integrate compliance practices into their product development cycles now, in order to avoid the need for retrospective changes to be made in the future, in response to customer or regulatory pressures.

Dan Whitehead Senior Associate
dan.whitehead@hoganlovells.com
Hogan Lovells International LLP

WEBINAR

Key takeaways: Data privacy in the Middle East

The Dubai International Financial Centre ('DIFC') announced, on 1 June 2020, that His Highness Sheikh Mohammed bin Rashid Al Maktoum had enacted, on 21 May 2020, DIFC Data Protection Law No. 5 of 2020 ('the 2020 Law') and that the Board of Directors of the DIFC Authority had also issued new Data Protection Regulations ('the Regulations'). In this webinar, our expert speakers provide an overview of the new Law and some of the Middle East region with a special focus on the key updates brought by the new data protection law. Among other topics, our speakers look at data privacy in the Middle East from a legislative, operational and regulatory viewpoint as well as the impact of the COVID-19 ('Coronavirus') pandemic on the implementation of data protection legislation in the Middle East in general. In terms of the DIFC, the webinar outlines similarities and differences between the DIFC Data Protection Law No.1 of 2007 and the 2020 Law.

Key takeaways

The evolving Middle East landscape

Prior to 2004, various legislation with data protection provisions existed, for example cybersecurity legislation. However, in 2004, the DIFC adopted the first comprehensive data protection law in the Middle East region. The Data Protection Law No. 9 of 2004 was later replaced by Law No.1 of 2007 and subsequently Law No.5 of 2020. Next, the Qatar Financial Centre adopted the Data Protection Regulations No.6 of 2005 and in 2016, Qatar introduced the Personal Information Privacy Protection Law which became effective in January 2018. In 2015, the third of the free zones, Abu Dhabi Global Market, introduced its Data Protection Regulations. From this point national laws continued to emerge. For instance, Turkey's Law on Protection of Personal Data came into effect in 2016, 2019 saw Bahrain adopting the Personal Data Protection Law No. 30 of 2018, and Lebanon adopting the Electronic Transactions & Personal Data Law. Among others, Egypt, UAE Federal and Saudi Arabia are yet to enact data protection legislation.

Where we are today

Organisations will need to embed privacy considerations into their business models, considering investing in security and privacy programs. As part of this, organisations should consider ethical data sharing practices as well as any specific requirements of the country in which they are operating, whether there are established data protection laws or whether generally high standards of data protection should be applied. As a scenario for implementation, the Coronavirus poses various data privacy challenges in the Middle East, for instance regarding cost-related issues of ensuring protection of personal data and the hiring privacy professionals during an economic crisis. Furthermore, the new data protection law in DIFC will have impact on all the regulated businesses.

On 1 July 2020 the new law will become effective and from 1 October the law will be enforceable. The companies with offices and business in DIFC will need to appoint a Data Protection Officer ('DPO') in order to be compliant with the law. As in the GDPR, the new law stresses the importance of providing the adequate resources, be adequately equipped to carry on activities and to maintain independence. In the region, there have been consultations on different aspects of data protection laws in countries such as Jordan, UAE Federal, Saudi Arabia and Qatar and we expect to see some developments in these countries in the next 12 to 18 months, perhaps modelled on the GDPR. Sector-specific legislation have also emerged containing, for instance data localization requirements for health data in the UAE.

Data protection in the DIFC

Compared to the previous Law of 2007, the 2020 Law is not hugely different. However, it brings a new outlook in some areas which will have an impact on businesses operating in the DIFC.

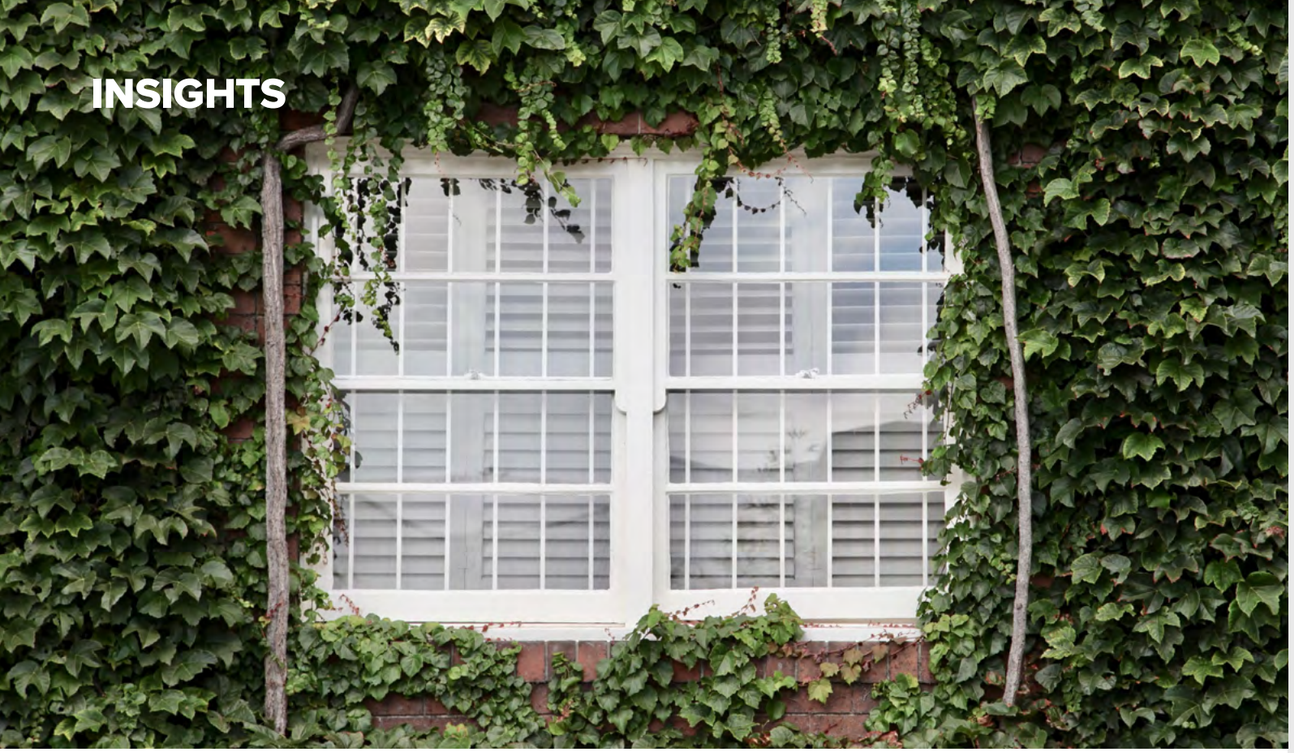
Accountability has been enforced with the introduction of DPO requirement and other controls such as prior consultation and processor provisions.

Data subject rights remain largely the same, but have been aligned to absorb the impact of emerging technology and international data protection laws, considering also that it may not be possible for personal data to be erased in some scenarios such as blockchain.

Security breach reporting has been enhanced with the processor must now play a larger role in accountability overall and for breach reporting, and the data subject him or herself must be informed in certain cases.

International transfers are realigned and enhanced to align with current international standards. Adequacy standards are set out in further detail and updated, processors are more accountable, and additional existing mechanisms approved by the European Commission, such as Binding Corporate Rules ('BCRs') can be recognised.

Data protection principles remain the same but now also promote the concepts of structure, governance and a risk-based approach to compliance.



EU: EDPB's draft guidelines on Privacy by Design and by Default

On 13 November 2019, the European Data Protection Board ('EDPB') published its draft Guidelines 4/2019 on Article 25: Data Protection by Design and by Default[1] ('the Guidelines'). The Guidelines aim to advise on how to best implement the principles of Privacy by Design and by Default, as set out in Article 25 of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and what the implementation of Privacy by Design and by Default means in practice for organisations collecting and processing personal data. Odia Kagan, Partner and Chair of GDPR Compliance & International Privacy at Fox Rothschild LLP, discusses the content of the Guidelines and how they can best be implemented within organisations.

Who is obligated?

Privacy by Design and by Default is a requirement for all controllers, independent of their size, including small local associations and multinational companies alike. The complexity of implementing Privacy by Design and by Default will vary based on the individual processing operation.

Privacy by Design and by Default: What is it?

The principles of Privacy by Design and by Default are set forth in Article 25 of the GDPR, and consists of the core obligation to effectively implement data protection principles and data subjects' rights and freedoms by design and by default.

Therefore, it is required that controllers implement appropriate technical and organisational measures and necessary safeguards, designed to implement data protection principles in an effective manner and to protect the rights and freedoms of data subjects.

Controllers must have data protection designed into, and as a default setting, in the processing of personal data and be able to demonstrate the effectiveness of the implemented measures.

The measures must be fit to implement the data protection principles effectively by reducing the risks of infringing the rights and freedoms of data subjects.

Safeguards are a second tier after measures. They are necessary to ensure the effectiveness of the implementation of data protection principles throughout the lifecycle of the personal data being processed.

Article 25 of the GDPR does not oblige controllers to implement any prescribed technical and organisational measures or safeguards, as long as the chosen measures and safeguards are in fact appropriate at implementing data protection into the processing. Measures and safeguards should be designed to be robust and be able to be scaled up in accordance with any increase in risk of non-compliance with the principles.

When must you assess?

Controllers must implement measures and safeguards designed to effectively implement the data protection principles at the time of determining the means of processing. At the time of processing itself, the controller must regularly review the effectiveness of the chosen measures and safeguards.

What do you take into account when implementing?

- State of the art:
  - controllers must have knowledge of, and stay up to date on, advances in technological and organisational measures, how technology can present data protection risks to the processing operation, and how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects in face of the technological landscape; and
  - where existing standards and certifications exist - controllers should take these into account;
- Cost of implementation:
  - controllers shall plan for and expend the costs (in terms of money or economic advantage, but also resources in general, including time and human resources) necessary for the effective implementation of all of the principles; and
  - incapacity to bear the costs is no excuse for non-compliance with the GDPR. At the same time, effective implementation of principles must not necessarily lead to higher costs;
- Nature, scope, context, and purpose of processing:
  - nature: the inherent characteristics of the processing;
  - scope: size and range of the processing;
  - context: relates to the circumstances of the processing, which may influence the expectations of the data subject; and
  - purpose: pertains to the aims of the processing
- Risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

Privacy by Default

- Collect only what you need: Organisational measures supporting processing operations should be designed to process, at the outset, only the minimum amount of personal data necessary for the specific operations. This should be particularly considered when allocating data access to staff with different roles.
- Protect it: Information security shall always be a default for all systems, transfers, solutions, and options when processing personal data.
- Process only as needed: Processing operations performed on personal data should be limited to what is necessary.
- Retain only for as long as needed:
  - any retention should be objectively justifiable and demonstrable by the data controller in an accountable way, and if personal data is not needed after its first processing, then it shall by default be deleted or anonymised; and
  - anonymisation of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of re-identification, is regularly assessed.
- Limit access:
  - you must limit who can have access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it when necessary, for example in critical situations;
  - the controller is obligated not to make the personal data unduly accessible in the first place. This can be done using technical tools and protocols to limit search engines from indexing the data, such as 'robot.txt' files. These should be respected by the recipient controllers even though they aren't binding; and
  - even in the event that personal data is made available publicly with the permission and understanding of a data subject, it does not mean that any other controller with access to the personal data may freely process it themselves, for their own purposes – they must have a separate legal basis.

What are the design and default elements for each data protection principle?

Transparency

- Clarity: clear and plain language, concise and intelligible;
- semantics: clear meaning to the audience in question;
- accessibility: easily accessible for the data subject (e.g drop down menus and hyperlinks);
- contextual: at the relevant time and in the appropriate form:
  - no more than one click away from accessing information; and
  - use pop-ups and hover overs;
- relevance: relevant and applicable to the specific data subject;
- universal design: accessible to all, including the use of machine-readable languages to facilitate and automate readability and clarity;
- comprehensible: fair understanding of what can be expected with regards to the processing, particularly for children or other vulnerable groups; and
- multi-channel: different channels and media, beyond the textual.

Lawfulness

- Relevance: use of the correct legal basis;
- differentiation: differentiate between the legal basis used for each processing;
- specified purpose: appropriate legal basis clearly connected to the specific purpose of processing;
- necessary: processing must be necessary for the purpose;
- autonomy: the data subject should be granted the highest degree of autonomy as possible with respect to control over personal data;
- consent withdrawal: data subject should easily know what they consented to and withdrawal should be as easy as giving consent;
- balancing of interests: where legitimate interests is the legal basis, carry out an objectively weighted balancing of interests; and
- legal basis: establish the legal basis before the processing takes place. If the legal basis ceases to apply, cease the processing.

Fairness

- Autonomy: grant the data subjects the highest degree of autonomy possible with respect to control over their personal data. Do not make it hard to avoid data sharing or adjust privacy settings;
- interaction: data subjects must be able to communicate and exercise their rights with the controller;
- expectation: processing should correspond with data subjects' expectations;
- non-discrimination: do not discriminate against data subjects;
- non-exploitation: do not exploit the needs or vulnerabilities of data subjects;
- consumer choice: do not 'lock in' users;
- power balance: avoid or mitigate asymmetric power balances;
- respect rights and freedoms: respect the fundamental rights and freedoms of data subjects;
- ethical: see the processing's wider impact on individuals' rights and dignity;
- truthful: act as you declare to do and do not mislead data subjects;
- human intervention: incorporate qualified human intervention

capable of recovering biases that machines may create; and
- fair algorithms: provide information about the processing of personal data based on algorithms that analyse or make predictions about data subjects, such as work performance, economic situation, health, personal preferences, reliability or behaviour, and location or movements.

Purpose limitation

- Predetermination: determine the legitimate purposes before designing the processing;
- specificity: specify the purpose of each processing;
- purpose orientation: the purpose of the processing should guide the design of the processing and set processing boundaries;
- necessity: the purpose of the processing determines what personal data is necessary for the processing;
- compatibility: any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design;
- limit further processing: do not connect datasets or perform any further processing for new incompatible purposes;
- review: regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation; and
- technical limitations of reuse: use technical measures, including hashing and cryptography, to limit the possibility of repurposing personal data.

Data minimisation

- Data avoidance: avoid processing personal data altogether when this is possible for the relevant purpose;
- limitation: limit the amount of personal data collected to what is necessary for the purpose;
- necessity: data is not necessary if it is not possible to fulfil the purpose by other means;
- relevance: be able to demonstrate the relevance of the data to the processing in question;
- aggregation: use aggregated data when possible;
- pseudonymisation: pseudonymise personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately:
  - if names are not necessary, pseudonymisation keys should be used and frequently rotated; and
  - if precise locations/addresses are not required - macro areas should be considered;
- anonymisation and deletion: where personal data is not, or no longer necessary for the purpose, anonymise or delete it;
- data flow: the data flow shall be made efficient enough to not create more copies, or entry points for data collection than necessary; and
- 'state of the art:' apply available and suitable technologies for data avoidance and minimisation.

Accuracy

- Data source: data sources should be reliable in terms of data accuracy;
- degree of accuracy: each personal data element shall be as accurate as necessary for the specified purposes;
- measurably accurate: reduce the number of false positives/negatives;
- verification: depending on the nature of the data, in relation to how often it may change, verify the correctness of personal data with the data subject before and at different stages of the processing;
- erasure/rectification: erase or rectify inaccurate data without delay;
- accumulated errors: mitigate the effect of an accumulated error in the processing chain;
- access: give data subject an overview and easy access to personal data in order to control accuracy and rectify as needed;
- continued accuracy: personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps;
- up to date: personal data must be updated if necessary for the purpose; and
- data design: use of technological and organisational design features to decrease inaccuracy, e.g. drop-down lists with limited values, internal policies, and legal criteria.

Storage limitation

- Deletion: have clear internal procedures for deletion;
- automation: the deletion of certain personal data should be automated;
- storage criteria: determine what data and length of storage is necessary for the purpose and must know what personal data is processed and why;
- enforcement of retention policies: enforce internal retention policies and conduct tests of whether the organisation practices its policies;
- effectiveness of anonymisation/deletion: make sure that it is not possible to re-identify anonymised data or recover deleted data, testing whether this is possible;
- disclose rationale: be able to justify why the period of storage is necessary for the purpose, and disclose the rationale behind the retention period;
- data flow: beware of and seek to limit 'temporary' storage of personal data; and
- backups/logs: determine which personal data and length of storage is necessary for back-ups and logs.

Integrity, confidentiality, and availability

- Information security management system ('ISMS'): have an operative means of managing policies and procedures for information security. For some controllers, this may be possible with the help of an ISMS;
- risk analysis: assess the risks against the security of personal data and counter identified risks;
- resilience: the processing should be robust enough to withstand changes, regulatory demands, incidents, and cyber attacks;
- access management: only authorised personnel shall have access to the data necessary for their processing tasks;
- secure transfers: transfers shall be secured against unauthorised access and changes;
- secure storage: data storage shall be secure from unauthorised access and changes;
- backups/logs: keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control;
- special protection: special categories of personal data should be protected with adequate measures and, when possible, be kept separated from the rest of the personal data;
- pseudonymisation: personal data and back-ups/logs should be pseudonymised as a security measure to minimise risks of potential data breaches, for example using hashing or encryption;
- security incident response management: have in place routines and procedures to detect, handle, report, and learn from data breaches;
- personal data breach handling: integrate management of notification (to the supervisory authority) and information (to data subjects) obligations in the event of a data breach into security incident management procedures; and
- maintenance and development: regularly review and test software to uncover vulnerabilities of the systems supporting the processing.

Odia Kagan Partner and Chair of GDPR Compliance & International Privacy

okagan@foxrothschild.com

Fox Rothschild LLP, Philadelphia

1. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

Privacy Talks

OneTrust DataGuidance met with Pierre Faller, Data Protection Officer at Christian Dior in February 2020. Christian Dior is a French luxury goods company founded in 1946. Pierre gives his recommendations for managing internal privacy policies and notices as well as giving his opinion on data protection related case law.

What are your recommendations regarding management of internal privacy policies and notices?
You have to get the top-down approach and that's the toughest part. I think, first of all, a new person into business, especially your data protection officer ('DPO'), needs to understand how the business works with these core values of a business, and that takes some time. After a couple of months, I believe you are able to understand the 'what's,' the 'why's,' etc. of different teams.

Then, you need to understand any gaps and show that you understand how to fill these gaps, document them, and then present this documentation to the top management. The top management should then act on it, support you, and actually, that is an obligation under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), without being too specific, that is Article 38, which gives the responsibility of the data controller in any business to support the work of a DPO through moral support, let's say a message, a memo, or even video.

What trends have you noted with respect to third-party management?
During the first few months of implementation since the GDPR came into force and, until the end of 2018, third parties and contractual negotiations were pretty tough because no one worked to the same standards, no one had specific guidelines to follow, and so everyone was on different pages, until the contractual agreements were finalised. If you had a phone call with a privacy expert, and that privacy expert talked to you about some new features which you had never heard of before, it was quite a surprise, and therefore, you needed to pause a moment to really understand what that other person is delivering.

> **The main trend that I've seen growing over the last couple of months has been the link between data protection laws and consumer laws, meaning that you are no longer really dealing with only the data subjects, you are also dealing with the clients.**

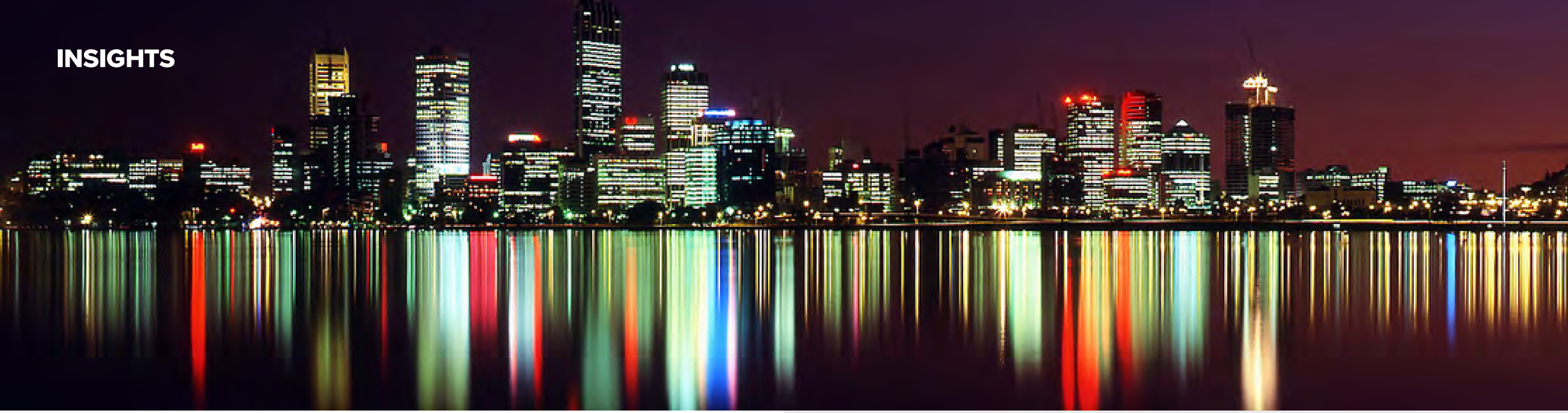
The other aspect is more like a checks-approach. All businesses should run the same sort of checks, such as know your partner and know your customer. These sorts of checks should be done regularly if you are a business working with another business. These checks are sometimes too long, such as a questionnaire of 60 questions, and so on, therefore it's too complicated for small businesses. So, I think one of the major inputs in the past couple of years has been to reduce these or to make it in two parts: the preliminary questionnaire and then the more fully fledged approach if you still have some risks.

How do you see case law on data protection developing?
The main trend that I've seen growing over the last couple of months has been the link between data protection laws and consumer laws, meaning that you are no longer really dealing with only the data subjects, you are also dealing with the clients, and the clients have certain rights, and businesses have certain obligations under consumer rules. There's been a growing list of cases like this, in Europe at least, and it's still a small evolution, but I think as this grows, we should keep an eye on this throughout 2020/2021.

Are there any laws in particular which you are currently assessing the impact of with respect to data subject rights?
Privacy has become global. Everyone is aware of the California Consumer Protection Act of 2018 ('CCPA') in the US, and South Korea and Japan developing their own laws. I think if your business is worldwide, it has to take into consideration how these different aspects and variations, sometimes small, sometimes large. In terms of ease, the CCPA's 'do not send my data' is the equivalent of the GDPR opt-out and I do not consent anymore. Is it the same? Is it different? And also, I think we have to look at the very soon, next-to-be-new laws, such as in Mexico and Brazil in particular. Therefore, businesses have to keep an eye on these evolutions and but also keep an eye on case laws as well, as they evolve very fast.

Pierre Faller Data Protection Officer
Christian Dior

Pierre recently joined our PrivacyConnect Industry Expert Panel to talk about current challanges in the retail industry.



Australia: OAIC and ACCC outline their enforcement approach for the Consumer Data Right

On 8 May 2020, the Office of the Australian Information Commissioner ('OAIC') and the Australian Competition and Consumer Commission ('ACCC') jointly published their Compliance and Enforcement Policy ('the Policy') for the Consumer Data Right ('CDR'). The Policy explains how the OAIC and ACCC will encourage compliance and respond to breaches. Enforcement will be very consumer-focused to engender trust in the new regime. With the CDR soon to apply to banks with roll-out to retail, energy, telecommunications, and other sectors to follow, current and future CDR participants, and their outsourced service providers, should be well advanced in preparing their systems, processes, and staff so as to ensure full compliance with the CDR. Alec Christie and James Wong, from Mills Oakley, discuss the Policy, what sectors may be affected by the enforcement approach taken towards the CDR, and how companies can prepare for this.

Who is the Policy relevant to?

The Policy is relevant to the following, (together 'CDR Participants'):

- data holders and their service providers, which are subject to certain obligations to give effect to the CDR. The first data holders under the CDR regime will be the big banks; and
- data recipients and their service providers, which need to be accredited by the ACCC before they may receive consumer data from the data holders with the consent of consumers, and they are also subject to various CDR requirements.

The legal, risk, privacy, and compliance functions of (current and future) CDR Participants should take heed of the Policy.

A recap on the CDR and its Framework

The CDR is intended to promote consumer choice and convenience by giving consumers greater control over their data and its portability, comprising of (collectively, 'the Framework'):

- amendments to the Competition and Consumer Act 2010, the Privacy Act 1988 (No. 119, 1988) (as amended) ('the Privacy Act'), and the Australian Information Commissioner Act 2010 ('the Legislation'), including the addition of the 13 Privacy Safeguards;
- rules made under the Legislation ('the Rules'); and
- consumer data standards made under the Rules.

The Framework is co-regulated by the OAIC and the ACCC (together, 'the Regulators'). The Commonwealth Scientific and Industrial Research Organisation's Data61[1] is charged with developing technical standards to support the operation of the Framework and the CDR regime.

> **In the Policy, the Regulators state that they will prioritise and focus on pursuing enforcement so as to provide the 'greatest overall benefit to consumers'**

The application of the CDR will increase over time, starting with the major banks on 1 July 2020, with other banks and financial services organisations (e.g. superannuation and insurance), the retail energy, and telecommunications sectors to follow.

How will the Regulators enforce CDR?

In the Policy, the Regulators state that they will prioritise and focus on pursuing enforcement so as to provide the 'greatest overall benefit to consumers.' This prioritisation will, in practice, consider factors such as:

- the nature and extent of the conduct, including the period during which the conduct occurred and the number of related breaches;
- whether the conduct was deliberate, repeated, reckless, or inadvertent;
- the actions of the business in relation to the conduct (e.g. whether the conduct was self-reported, the timing of the self-report, and any rectification and/or remediation); and
- whether the business demonstrates a corporate 'culture' of compliance.

Of particular note, the Policy sets out forms of conduct that will always be grounds for the serious consideration of enforcement action by the Regulators, referred to as 'priority conduct:'

- refusal by a data holder to share consumer data: where a consumer validly requests and a data holder repeatedly refuses to disclose, or frustrates the process of disclosure of, consumer data (and refusal is not permitted under the Framework);
- misleading or deceptive conduct: for example, 'holding out' that you are accredited as a data recipient when you are not, and making false or misleading representations about the nature/benefits of a CDR service;
- invalid consent: where a data recipient collects consumer data without valid consent from the consumer (i.e. as and in the form required under the Framework);
- misuse or improper disclosure of consumer data: intentional misuse or improper disclosure of consumer data by a data recipient (e.g. where the consumer has withdrawn their consent); and
- insufficient security controls: failure to implement and maintain sufficient controls to protect consumer data.

Enforcement tools the Regulators may use include:

- administrative resolution: the Regulators may recommend improvement to internal practices and procedures and/or accept a voluntary written commitment to address areas of non-compliance. Compliance with voluntary commitments may be monitored;
- infringement notice: the ACCC may issue CDR Participants with an infringement notice where it believes that a breach has occurred;
- court enforceable undertaking: the Regulators may accept a formal written commitment from a CDR Participant to undertake or refrain from certain conduct (e.g. carry out an internal audit). Failure to comply with an enforceable undertaking may see the Regulators seek court orders against the CDR Participant. This has proved a popular tool with the OAIC under the Privacy Act;
- suspension or revocation of accreditation: the ACCC may suspend or revoke accreditation of a data recipient if they consider this is necessary to protect consumers. As a result, the data recipient will no longer lawfully be able to receive CDR data;
- determination and declaration: the OAIC may investigate, then make a determination to either dismiss or substantiate a breach of a Privacy Safeguard or privacy/confidentiality Rule. Determinations can include declarations or orders for the compensation of affected consumers; and
- court proceedings: the Regulators may initiate legal action for a breach of the Framework. The court may then make a range of orders, including civil penalties (for corporations, up to the greater of AUD 10 million (approx. €6 million), three times the value of any

benefit obtained, and 10% of domestic annual turnover), injunctions, and the disqualification of individuals from being directors of corporations.

It remains to be seen how the Regulators will share and divide enforcement duties in practice. However, it is envisaged that the OAIC will be primarily responsible for providing remedies to aggrieved individuals and businesses with respect to the Privacy Safeguards, while the ACCC will focus on strategic enforcement (e.g. repeated or serious breaches). In the Policy, the Regulators have stressed their consumer-centric approach to enforcement (see below for the implications of this).

How will the Regulators foster compliance?

The Regulators have stated they will focus on preventing and addressing harm to consumers, using a 'risk-based approach' to monitor and assess compliance matters, and focus on circumstances that have the potential to cause significant harm or result in widespread consumer detriment. For the purposes of the Framework, the concept of a consumer is broad and includes small and medium-sized enterprises.

Compliance monitoring tools the Regulators' can use include:

- stakeholder intelligence and complaints: the Regulators will receive information (e.g. by complaints) from CDR consumers, businesses, consumer groups, government agencies, and intelligence/reports from certain external dispute resolution bodies, such as the Australian Financial Complaints Authority;
- business reporting: data holders and data recipients must submit reports every six months to the Regulators setting out information about their compliance with the Framework, including a summary of all complaints they receive. This information will help the Regulators track compliance and quickly address emerging issues and trends;
- audits and assessments: the Regulators may undertake audits and assessments of CDR Participants to ensure compliance with the Framework requirements. Where compliance gaps are identified (e.g. inadequate security controls or ineffective consents), the Regulators will seek to have the CDR Participants resolve them (likely with a follow-up confirmation audit); and
- information requests and compulsory notices: when the Regulators believe that a CDR Participant's conduct may be in breach of the Legislation, they may issue information requests to CDR Participants and may compel the provision of information, documents, or evidence using their information gathering powers under the Framework.

What the Regulators are trying to achieve

The Regulators see consumer trust as central to the successful roll-out of the CDR, with their stated overarching objective of 'ensuring that consumers can trust the security and integrity of the [Framework].' The Regulators want to instil confidence in the mechanics of the Framework, including the ongoing monitoring and enforcing of the compliance of all CDR Participants with the Framework.

In their enforcement role, the Regulators will be guided by the core principles of accountability, efficiency, fairness, proportionality, and transparency. In our view, periodic and pragmatic communications and targeted (i.e. 'biggest bang for their buck') enforcement actions from the Regulators will underpin the effectiveness of the Framework and ensure CDR participants comply with it.

What do I need to do now?

All potential CDR Participants in the banking sector should have finalised their preparations by now for the 1 July 2020 start. Banks (as data holders) should have implemented processes, technical controls, staff training, manuals/documentation, and customer support frequently asked questions to support their compliance with open banking under the Framework.

Future CDR Participants in other parts of the financial service sector, the retail, energy, and telecommunication sectors should have started their preparations. If not, conduct a preparedness review (which could be undertaken as part of your existing internal audit program) to identify those aspects of compliance that are the most likely problem areas for your organisation (with an eye on the 'priority conduct' specified by the Regulators).

Additional takeaways

Assuming (as we do) that the wording used in the Policy was carefully considered, the opening sentence of the Policy confirms what many of us have been thinking, that CDR will not be limited to the banking, retail, energy, and telecommunications sectors: '[CDR] is a [...] reform that will be rolled out economy-wide, sector-by-sector, starting with banking.'

Based on this, we expect that the CDR will be rolled out to the remainder of the consumer-focused economy over the next 12 to 48 months. Those outside of the initial sectors (banking, retail, energy, and telecommunications) should consider the issues raised by the Framework, institute necessary controls ahead of time (especially for any new IT projects/procurements) and, if possible, contribute to upcoming industry consultations around the development of Rules for your sector.

The fervent focus on and championing of the consumer and his/her interests may, at first glance, not seem out of place in something titled the CDR. However, we feel the rhetoric is actually a two-part warning or flagging of the intentions of the Regulators as follows:

- for those not used to dealing with the ACCC, it flags that the ACCC will bring its aggressive approach to enforcement under its other areas of responsibility (e.g. consumer law) into CDR enforcement; and
- for those used to dealing with the OAIC, it flags a more aggressive approach by the OAIC to enforcing the CDR (to keep in step with the ACCC), much more aggressive than we have seen to date from the OAIC in relation to privacy.

We expect that the OAIC's more aggressive approach to enforcing the CDR will ultimately be reflected in its approach to enforcing the Privacy Act too.

Where can I get more detail?

The Legislation and the Regulators make it clear that it is the responsibility of each CDR Participant to be fully aware of its obligations under the Framework. Ignorance will be no excuse. For more information, you may wish to review:

- the CDR legislation[2];
- the Consumer Data Standards[3]; and/or
- the OAIC's Privacy Safeguard Guidelines[4].

Also keep in mind that your obligations under the Privacy Act with respect to 'personal information' and, for entities regulated by the Australian Prudential Regulation Authority ('APRA'), the APRA information security requirements continue to apply in addition to/on top of all applicable CDR requirements.

Alec Christie Partner

achristie@millsoakley.com.au

James Wong Associate

jwong@millsoakley.com.au

Mills Oakley, Sydney

1. See: https://consumerdatastandards.gov.au/
2. See: https://www.legislation.gov.au/Latest/C2019A00063
3. See: https://consumerdatastandards.gov.au/
4. See: https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/

News in Brief

China: Civil Code introduces data protection and privacy rights

The Civil Code of the People's Republic of China ('the Civil Code') was adopted, on 28 May 2020, by the third session of the 13th National People's Congress.

In particular, the new provisions of the Civil Code ('the New Provisions') aim to enhance privacy rights as well as the protection of personal information in China by introducing obligations for information processors, including the adoption of security measures and requirements for the collection, usage, and processing of personal information.

Applicability

Manuel E. Maisog, Partner at Baker Botts LLP, told OneTrust DataGuidance, "The New Provisions apply broadly to businesses, [granting] a right of privacy to natural persons (though not to legal persons) and apply to any business whenever it deals with the private affairs or personal information of a natural person. '[P]ersonal information' includes the name, date of birth, ID number, biometric information, address, telephone number, email address, health information, and geolocational information of a natural person."

In addition, Dehao Zhang, Senior Associate at Fieldfisher, told OneTrust DataGuidance,"For businesses, the Civil Code doesn't distinguish [between] the controller and processor, and makes all businesses which process data, 'data processor[s],' the meaning of [which] is different from that under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') [...]. [However,] the word 'processing' has a similar meaning with that of the GDPR, referring to the collecting, using, processing, transferring, and providing of personal information, [as well as] making information public or [conducting] other operations."

Impact on businesses

The New Provisions introduce a number of obligations for information processors when processing personal information. In particular, the New Provisions provide that the processing of personal information shall follow the principles of lawfulness, justification, and necessity, and that personal information must not be excessively processed. In addition, the New Provisions require information processors to, among other things, obtain the consent of the natural person or his/her guardian, unless otherwise provided by laws and administrative regulations, comply with the rules for publicly processing information, and highlight the purpose, method, and scope when processing information.

Zhang highlighted, "Most Articles are similar [to] the content of the Cybersecurity Law of the People's Republic of China ('CSL') [and therefore] the obligations [in relation to] data protection do not change so much. However, the New Provisions differentiate [...] privacy and data protection, so businesses have to pay more attention to it. [In addition,] since privacy and data protection are [outlined] in the part [on] personality rights, [...] privacy and data protection can be regarded as personal rights and can be a reason of civil [litigation], especially when data breaches happen, individuals can raise claims for the compensation of mental and economic damages to the businesses who processed the data. [Furthermore,] the New Provisions have clarified that individuals have the right to access and get a copy of their data, which is not clearly stated under Article 43 of the CSL."

Ensuring compliance

Furthermore, the New Provisions require information processors to adopt technical and other necessary measures to ensure the security of the personal information they collect and store, to prevent information leakage, tampering, and loss.

Moreover, the New Provisions provide that information processors must in the event of a personal information leakage, tampering, and loss undertake remedial measures in a timely manner, including notification to natural persons and reporting to the relevant competent department.

In particular, Maisog further noted, "Businesses should take stock of their collection, storage, processing and use of private and personal information, and should both install a mechanism by which they obtain the data subject's consent and pair their collection and use of information so that they are using no unnecessary or extraneous information. It would also be a good idea to update and improve their information security systems. [Moreover,] businesses should adopt a policy of not indiscriminately collecting or processing private or personal information."

Correspondingly, Zhang outlined, "[B]usinesses should keep a blacklist or whitelist of marketing, since some businesses are keen to market individuals, especially the real state brokers, agents, micro-loan companies or the sports gyms, and other data driven companies. Before the businesses do marketing, they should consider if they have obtained prior consent, and [whether] the individuals have the options to opt out. [Moreover,] for legal basis of data processing, consent and legal requirements are the lawful bases, however, business can take a look at the new requirements under Article 1037 of the Civil Code."

> **The New Provisions provide that the processing of personal information shall follow the principles of lawfulness, justification, and necessity, and that personal information must not be excessively processed.**

Limitations

Zhang clarified,"[T]he Civil Code doesn't provide any rules [for] Data protection Impact Assessments, or Privacy Impact Assessments [, as well as] direct marketing [...]. [However,] we think this new legislation is really good for the legal statues of privacy and data protection [and] understand not all can be introduced [at] one time. [Furthermore,] since the Civil Code pays more attention to civil relationships, [...] obligations such as data transfers or data localisation are not introduced [...], and we expect that will be an important content of the Draft Personal Information Protection Law which is still on the way."

Furthermore, Maisog detailed, "The New Provisions do not impose liability for handling private and personal information if the individual's consent is obtained. Also, when personal information includes private information, rules regarding privacy rights will control, where there are no provisions regarding privacy rights, rules regarding personal information will control instead. [Moreover,] up [until] this time, personal information protection in China has proceeded as a patchwork affair, with each industry sector or regulatory body having its own particular set of rules.

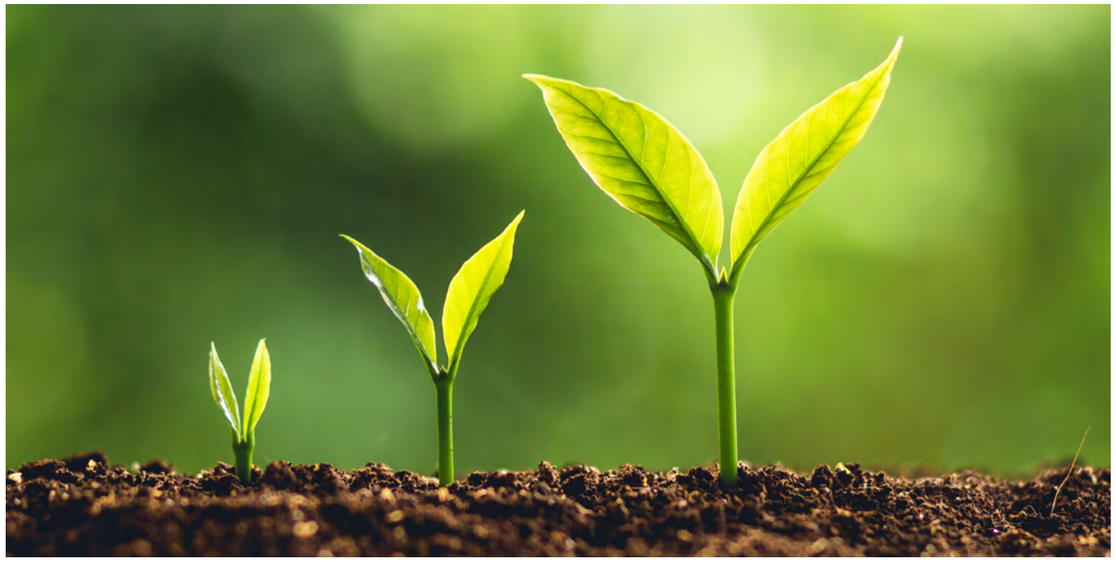
The expected promulgation this year of a new Personal Information Protection Law and Data Security Law appeared to be a step towards regularising this patchwork affair into an integrated, comprehensive framework. The appearance of these New Provisions in the Civil Code is puzzling because it appears contrary to that objective and appears to preserve and even extend the patchwork approach. The addition of a new 'privacy right' alongside personal information protection obligations further complicates the picture."

The Civil Code will enter into force on 1 January 2021.

Keshawna Campbell Privacy Analyst
kcampbell@onetrust.com

Comments provided by:
Dehao Zhang Senior Associate
dehao.zhang@fieldfisher.com
Fieldfisher

Manuel E. Maisog Partner
manuel.maisog@bakerbotts.com
Baker Botts LLP



South Africa: President announces commencement dates for certain sections of POPIA

The President of South Africa announced, on 22 June 2020, the commencement dates for certain remaining sections of the Protection of Personal Information Act, 2013 ('POPIA'). Such sections will commence on 1 July 2020 and 30 June 2021. Furthermore, following the 12-month transition period, organisations must be compliant with POPIA by 1 July 2021.

POPIA has been gradually entering into force since April 2014. The President outlined that a certain 'state of operational readiness for the Information Regulator' was required before all sections could come into force.

In light of this, on 11 April 2014, the President of South Africa announced the commencement of Section 1, Part A of Chapter 5 and Sections 112 and 113 of POPIA. These sections concern, among other things, definitions, the establishment of the Information Regulator, the Regulator's ability to make regulations relating to POPIA, and the procedure for making regulations.

On 22 June 2020, the President announced that Sections 2 to 38, 55 to 109, 111, and 114(1), (2) and (3) will commence on 1 July 2020. These sections are essential parts of POPIA relating to, among other things, the conditions for the lawful processing of personal information, the regulation of the processing of personal information, codes of conduct issued by the Information Regulator, procedures for dealing with complaints, provisions regulating direct marketing by means of unsolicited electronic communication, and the general enforcement of POPIA.

Furthermore, Sections 110 and 114(4) will commence on the later date of 30 June 2021. Sections 110 and 114(4) relate to the amendments of laws and the transfer the implementation of the Promotion of Access to Information Act, 2000 ('PAIA') from the South African Human Rights Commission to the Information Regulator.

Section 114(1), which commenced 1 July 2020, covers the 12-month transition period for all public and private bodies to ensure all processing of personal data complies with POPIA. As a result, organisations must be POPIA-compliant by 1 July 2021.

Purposes

POPIA aims to give effect to the constitutional right to privacy, balance it against other rights, especially the freedom to information, and regulate the processing of personal information in harmony with international standards.

More specifically, the sections of POPIA include the following.

Conditions for lawful processing of personal information

Chapter 3 (Sections 8 to 35) outlines the conditions for lawful processing of personal information, which include accountability, processing limitations, purpose specification, information quality, security safeguards, authorisations for processing of special personal information, and processing of children's data. The conditions for lawful processing of personal information form a crucial part of POPIA and compliance with its provisions.

Information Officer duties

Part B, Chapter 5(Sections 55 and 56) details the duties and responsibilities of the Information Officer where required. The Information Officer's role includes the encouragement of compliance with POPIA's provisions, especially the conditions for the lawful processing of personal information and dealing with requests. The responsible party must register the information officer before duties can commence.

Codes of conduct

Chapter 7 (Sections 60-68) provides for the Information Regulator to issue codes of conduct, which must include how the conditions for lawful processing are to be applied or complied with, specify appropriate measures for information matching programmes if used, and protect the legitimate interests of the data subject regarding automated decision making. Codes of conduct can apply to specified or classes of, among other things, bodies, information, activities, industries, professions, or vocations. The Regulator may review, amend, and revoke codes of conduct and provide written guidelines on the same. If a code of conduct is in force, failure to comply is deemed a breach of the conditions for lawful processing and dealt with under Chapter 10.

Direct marketing

Chapter 8 (Sections 69-71) covers the rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories, and automated decision making. In particular, Section 69 prohibits the processing of personal information for direct marketing purposes using electronic communication forms. However, it provides exceptions to this, which include where the data subject has consented to the processing or is a customer of the responsible party. Furthermore, any direct marketing communication must contain the details of the sender or representative, and the contact details where the data subject can request that communications cease.

International data transfers

Chapter 9 (Section 72) highlights provisions for transfers of personal information outside of South Africa, which are prohibited unless:

- the third party is subject to a law, Binding Corporate Rules ('BCRs'), or a binding agreement which provides an adequate level of protection of personal data, for example as specified in POPIA's conditions of lawful processing;
- the data subject has consented;
- the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the data subject's consent or the data subject would be likely to give it; or
- the transfer is necessary for:
  - the performance of a contract between the data subject and the responsible party, or the implementation of pre-contractual measures; or
  - the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

Enforcement procedure

Chapter 10 (Sections 73-99) is dedicated to the enforcement of POPIA. Any person may submit a complaint to the Regulator, which may or may not lead to the use of procedures as outlined in Chapter 10, for instance conducting a pre-investigation, acting as a conciliator, conducting a full investigation, and referring the complaint to the Enforcement Committee who must make a recommendation in respect thereof.

The Regulator can, at any time, choose to commence an investigation into the interference with the protection of personal information. Investigations may include summoning persons to give oral or written evidence or produce records, administering oaths, issuing warrants, searching premises, or conducting on-site investigations as the Regulator sees fit. Where settlements of complaints are possible, the Regulator may use its best endeavours to secure one between any concerned parties. Furthermore, the Regulator can, by choice or request from any party, make an assessment of whether an instance of processing of personal information complies with POPIA. The Regulator may make public the results of assessments, if it is deemed in the public interest to do so.

Following the recommendations of the Enforcement Committee, the Regulator may decide to make an enforcement notice if it is satisfied that a responsible party has interfered with the protection of personal information. The enforcement notice might require, among other things, specified steps to be taken or ceased within a particular timeframe (no less than three days) and certain processing activities to be ceased. Enforcement notices may be cancelled and appealed.

Fines and penalties

Chapter 11 (Sections 100-109) covers offences, penalties and administrative fines for violations of provisions of POPIA.

Any person convicted of violating Sections 100, 103(1), 104(2), 105(1), 106(1), (3), or (4) is liable to a fine or to imprisonment for a period not exceeding 10 years, or both. The relevant sections pertain to the following:

- Section 100: obstruction of the Information Regulator;
- Section 103(1): failure to comply with enforcement or information notices, where a responsible party fails to comply with an enforcement notice;
- Section 104(2): giving false evidence before the Information Regulator;
- Section 105(1): a responsible party who contravenes the provisions of Section 8 in relation to the processing of an account number of a data subject; and
- Section 106: unlawful acts by third parties in connection with the account number of a data subject.

POPIA aims to give effect to the constitutional right to privacy, balance it against other rights, especially the freedom to information, and regulate the processing of personal information in harmony with international standards

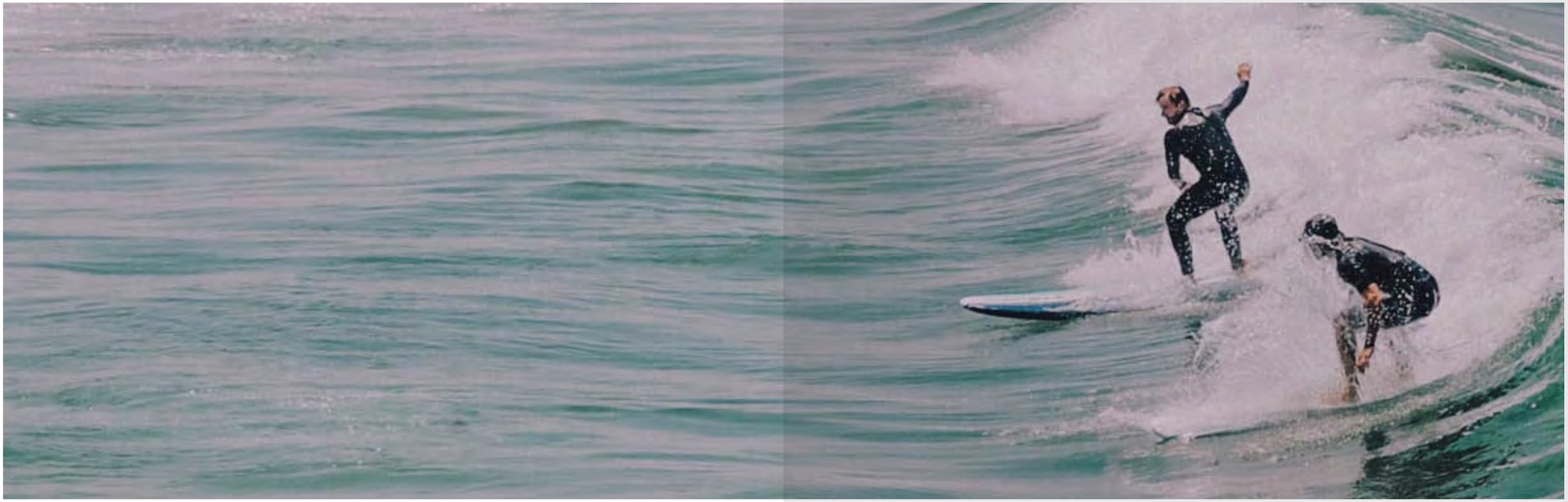
Any person convicted of violating Sections 59, 101, 102, 103(2), or 104(1) is liable to a fine or to imprisonment for a period not exceeding 12 months, or both. The relevant sections pertain to the following:

- Section 101: breach of confidentiality under Section 54;
- Section 102: obstruction of execution of a warrant;
- Section 103(3): a responsible party which, in purported compliance with an information notice, makes a false statement knowingly or recklessly makes a false statement; and
- Section 104(1): any person summoned to attend, give evidence, or produce any evidence who, among other things, who fails to:
  - attend at the specified time and place;
  - remain until the conclusion of proceedings or as excused;
  - be sworn in or make an affirmation as required;
  - answer fully and satisfactorily to any question lawfully put to them; or
  - produce any book, document, or object as summoned.

Administrative fines may not exceed R10 million (approx. €513,000), although the Regulator, by notice in the Gazette, may adjust this amount in accordance with the average of the consumer price index for the immediate period of 12 months multiplied by the number of years that the amount (R10 million) has remained the same. Such fines must be paid no later than 30 days after the date of service of the infringement notice.

Read our previous Insights on POPIA for further information on its progress and provisions, and how organisations can comply.

Amelia Williams Privacy Analyst
awilliams@onetrust.com



California: Status of CCPA and other privacy related bills in the State Legislature

The California Consumer Privacy Act of 2018 ('CCPA') was first signed into law, on 28 June 2018, by then California Governor Jerry Brown. In an unexpected turn of events and as a compromise between the Legislature and privacy rights advocate, Alastair McTaggart, who at the time had proposed an initiative for the November 2018 ballot, the CCPA was enacted to give California consumers unprecedented rights over their personal information, creating a myriad of obligations for businesses, who were expected to spend collectively more than $55 billion to comply.

Due to the urgency to pass the original CCPA bill (Assembly Bill ('AB') 325) in 2018, various ambiguities, confusing definitions, and technical errors ended up in the text. In order to make the CCPA functional and fix some of these errors, the Legislature had to discuss and pass a number of bills in 2018 and 2019, which, among others, dealt with enforcement, employee records, business to business marketing, and consumer requests for disclosure methods. This trend has continued in 2020; whilst no bills have been passed or signed into law at the time of writing, it seems that they still remain a main topic of discussion among the California Assembly and Senate members, who have continued their schedule mostly virtually during the pandemic. An overview of the bills is presented below along with their current status before various committees of the Assembly and Senate. Whilst some of them would amend the CCPA directly, others would create numerous consumer privacy provisions as part of the California Civil Code.

AB-713 was first introduced, on 19 February 2019, to the Assembly and was ordered to the Senate on 29 May 2019. However, AB-713, which seeks to exempt certain health information from the CCPA, has been heavily amended by the Senate so far.

In particular, AB-713 would add the following to the list of personal information that is exempt from the CCPA:

- information that is deidentified in accordance with the requirements for deidentification under the Privacy Rule of the Health Information Portability and Accountability Act of 1996 ('HIPAA') and is derived from patient information. However, deidentified information that meets these criteria and is subsequently reidentified would no longer be eligible for the exemption, and would be subject to applicable federal and state data privacy and security laws; and
- information that is collected, used, or disclosed in research, as defined in the HIPAA Privacy Rule, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of HIPAA, the Federal Policy for the Protection of Human Subjects, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the United States Food and Drug Administration.

In addition, AB-713 would prohibit reidentification, or any attempts to reidentify deidentified health information, except for certain purposes, including treatment, payment of health care operations conducted by a covered entity or business associate, public health activities, research, pursuant to a contract where the lawful holder of the deidentified information expressly engages a person or entity to attempt to reidentify the deidentified, or where otherwise required by law.

Finally, AB-713 contains a significant requirement for businesses dealing with deidentified health information – if it were to be signed into law, it would require businesses where one of the parties is a person residing or doing business in California, to include, from 1 January 2021, certain provisions within any contract for the sale or license of deidentified information:

- a statement that the deidentified information being sold or licensed includes deidentified patient information;
- a statement that reidentification, and attempted reidentification, of the deidentified information by the purchase or licensee of the information is prohibited pursuant to Section 1798.146 of the Civil Code; and
- a requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

AB-713 was last amended by the Senate on 11 June 2020 and was re-referred to the Senate Judiciary Committee.

AB-2280 was introduced, on 14 February 2020, to the Assembly and was ordered to the Senate on 10 June 2020. AB-2280 would amend the California Confidentiality of Medical Information Act, under Sections 56.05 and 56.06 of the Civil Code, and would add the definitions for 'personal health record' and 'personal health record information.' Furthermore, according to AB-2280, a business that offers personal health record software or hardware to a consumer, including a mobile application or other related device that is designed to maintain personal health record information in order to make information available to an individual or to a provider of health care at their request, for purposes of allowing the individual to manage their information, or for the diagnosis, treatment, or management of a medical condition of the individual, would be deemed to be a provider of health care subject to the requirements of this part. AB-2280 was read for the first time by the Senate, on 11 June 2020 and assigned to the Committee on Rules.

AB-2269 was introduced, on 14 February 2020, to the Assembly and seeks to create the Automated Decision Systems Accountability Act of 2020. According to Assembly Member Chau who introduced AB-2269, Big Data has raised concerns about the use of algorithmic or automated decision systems ('ADS') to make hiring and other workplace decisions, insurance eligibility, lending, and marketing decisions quickly, automatically, and fairly, however, if the underlying data used for an algorithm or ADS is biased, incomplete, or discriminatory, the decisions made by using such devices may result in massive inequality. AB-2269 would require businesses that provide a person with a program or device that uses an ADS to:

- take affirmative steps to ensure that there are processes in place to continually test for biases during the development and usage of the ADS;
- conduct an ADS impact assessment on its program or device to determine whether the ADS has a disproportionate adverse impact on a protected class;
- examine if the ADS in question serves reasonable

objectives and furthers a legitimate interest; and
- compare the ADS to alternatives or reasonable modifications that may be taken to limit adverse consequences on protected classes.

AB-2269 was referred, on 24 April 2020, to the Committee on Privacy and Consumer Protection.

AB-3119 was introduced, on 21 February 2020, to the Assembly and would create the Minimization of Consumer Data Processing Act. In particular, AB-3119 seeks to substitute the definition of a 'sale' under the CCPA with the term 'share' and would prohibit a business from collecting, sharing, retaining, or using a consumer's personal information if specified requirements are not met, including that such processing of the personal information is reasonably necessary to provide a service or conduct an activity that a consumer has requested. In addition, AB-3119 would prohibit a business from sharing personal information of a consumer unless such consumer has affirmatively consented to the sharing of information, and would also require a business to request a consumer's opt-in consent separately from any other permission or consent. AB-3119 was referred, on 5 May 2020, to the Assembly Committee on Privacy and Consumer Protection.

AB-2261 was introduced, on 14 February 2020, to the Assembly and refers to the use of facial recognition technology. In particular, AB-2261 would require from processors, defined to mean an agency or natural or legal person that processes personal data on behalf of a controller, that provides facial recognition services to make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations. In addition, processors would have to develop and implement a plan to mitigate the identified performance differences, if the results of an independent test identify material unfair performance differences across subpopulations, and those results are disclosed directly to the processor, who, acting reasonably, determines that the methodology and results of that testing are valid. AB-2261 defines 'subpopulation' as any of the following traits, race, skin tone, ethnicity, gender, age, disability status, or any other protected characteristic that is objectively determinable or self-identified by the individuals portrayed in the testing dataset. AB-2261 would also require a controller using a facial recognition service to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals to ensure that those decisions are subject to meaningful human review and would also grant various rights to individuals. AB-2261 was referred, on 2 June 2020, to the Assembly Committee on Appropriations and is currently held under submission.

SB-980 was introduced, on 11 February 2020, to the Senate and would create the Genetic Information Privacy Act. SB-980 would prohibit direct-to-consumer genetic or illness testing services companies from disclosing a person's genetic information to a third party without obtaining the person's prior written consent and it would also impose civil penalties for a violation of its provisions. In addition, SB-980 provides a written authorisation form that would be used by any person who obtains, analyses, retains, or discloses the genetic information of an individual. SB-980 was last amended by the Senate on 18 June 2020 and ordered to second reading.

AB-1281 was introduced, on 2 April 2019, to the Assembly but was amended heavily on 25 June 2020 by the Senate in order to extend the exemption of the CCPA in relation to employee information and business to business transactions until 1 January 2022. In particular, AB-1281 would exempt information collected by a business about a natural person in the course of such person acting as a job applicant, employee, owner, director, officer, medical staff member, or contractor. In addition, AB-1281 would provide an exemption for information reflecting a written or verbal communication or a transaction between the business and the consumer, if the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding a product or service.

AB 1281 would only become operative if the ballot initiative for the California Privacy Rights Act is not approved by voters at the November 2020 general election. AB-1281 was re-referred to the Committee on Judiciary on 1 July 2020.

Bill	Last Action	Does it amend the CCPA?
AB-713	11 June 2020, re-referred to Committee on Judiciary.	Yes.
AB-2280	1 July 2020, referred to Committee on Judiciary	No.
AB-2269	24 April 2020, referred to the Committee on Privacy and Consumer Protection.	No.
AB-3119	5 May 2020, referred to the Committee on Privacy and Consumer Protection.	Yes.
AB-2261	2 June 2020, referred to the Committee on Appropriations and is currently held under submission.	No.
SB-980	18 June 2020, ordered to second reading.	No.
AB-1281	1 July 2020, re-referred to Committee on Judiciary	Yes

Whilst not all of the above bills seek to amend the CCPA, they will certainly have an impact on operations of businesses in California, a state which has been a significant proponent of privacy rights in the US for a long time. More bills are expected to be introduced in 2020 and, at the same time, the Final Regulations proposed by the California Attorney General are before the Office of Administrative Law for final approval, and the California Privacy Rights Act, a new initiative proposed by MacTaggart looking to further amend the CCPA, is on its way to the November 2020 ballot.

Nikos Papageorgiou Lead Privacy Analyst
npapageorgiou@onetrust.com

New GDPR comparison reports available now

OneTrust DataGuidance is pleased to announce the release of the **GDPR v. PIPEDA** comparison report, which provides a means of analysing and comparing data protection requirements and recommendations under the GDPR and Canadian federal legislation.

The Report, produced in collaboration with Edwards, Kenny & Bray LLP, examines the protections afforded to individuals with respect to the protection of their data and privacy, comparing these guarantees to those afforded under the GDPR. More specifically, the Report details PIPEDA's scope of application, main definitions, controller and processor obligations, data subject rights, and enforcement matters, in comparison with those under the GDPR. The Report also highlights guidance issued by the Office of the Privacy Commissioner of Canada ('OPC'), which acts as non-binding legal interpretations to clarify certain nuances and aid in compliance with the law.

GDPR v. Singapore's PDPA comparison report, which highlights the similarities and differences between the two pieces of legislation in order to help organisations develop their compliance activities, is now available on the OneTrust DataGuidance platform.

The Personal Data Protection Act 2012 (No. 26 of 2012) was passed on 15 October 2012. The Report, produced in collaboration with Rajah & Tann Asia, explores further legislation behind the PDPA, including the Advisory Guidelines on Key Concepts in the PDPA, and explains where the GDPR and the PDPA differ and compare in areas such as cross-border data transfers, individual rights, non-compliance and penalties, and supervisory authorities.

Also available now is the **GDPR v. LPPD** comparison report, which provides a juxtaposition of the two pieces of legislation with a view to highlight the similarities and differences between the two pieces of legislation

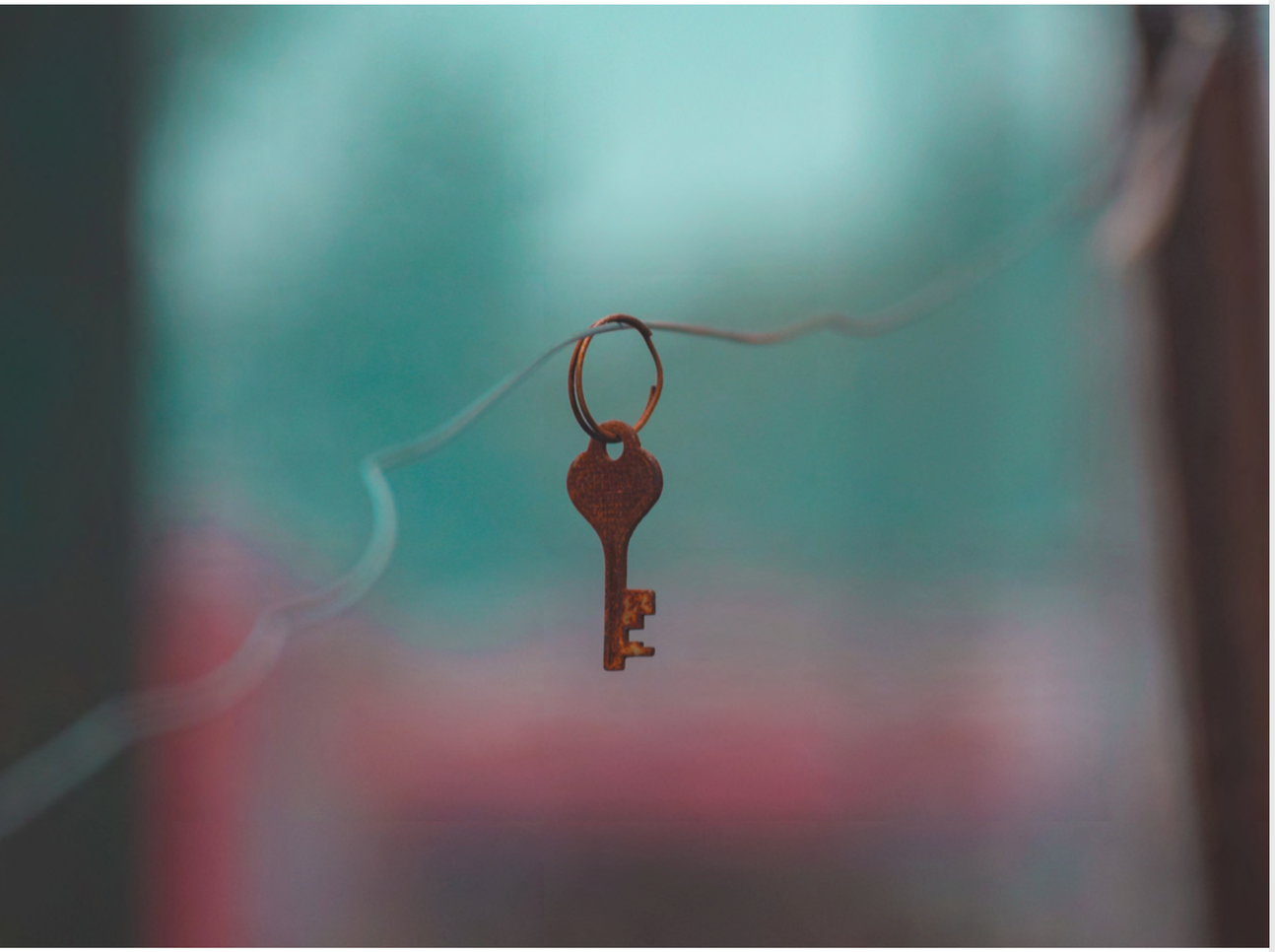
The LPPD is the first general data protection law in Turkey and is largely based on the former European Data Protection Directive. Secondary legislation introduced in Turkey in the form of regulations and communications have, though, led to a similar development as the changes in the EU brought about by the GDPR.The Report, produced in collaboration with Esin Attorney Partnership, scrutinizes areas of both legislations, such as the requirements of data processing records and data controllers.

*To read and download the latest copies of the GDPR comparison reports, go to the **OneTrust DataGuidance Regulatory Research platform**.*

www.dataguidance.com

Brazil: New open banking rules

While open banking is a key step towards providing data portability to customers, its execution may often prove challenging. Luis Fernando Prado Chaves and Beatriz Saboya, Partner and Attorney at Law respectively at Daniel Law, discuss open banking within the Brazilian context and related issues surrounding security, and the need for an effective regulator which may hinder its implementation.



In line with global trends, the Central Bank of Brazil ('the Central Bank') and the National Monetary Council ('the Monetary Council') issued, on 4 May 2020, Resolution 1 of 4 May 2020 and Circular No. 4.015 of 4 May 2020 ('the Resolutions'), which set forth the schedule and the relevant rules for the implementation of open banking in Brazil.

Generally speaking, open banking can be defined as the sharing of products, services, and data by financial and other licensed institutions through the integration of platforms and infrastructure of information systems ('APIs') in order to promote a safer, more efficient, and decentralised environment.

Nowadays, the banking industry faces a lot of difficulties to promote innovative and straight-to-the-point solutions, since financial institutions fail to access customer's financial data held by another financial institution in a secure fashion.

However, with the implementation of open banking, at the customer's discretion, financial institutions will be allowed to process personal and transactional data held by another financial institution, which benefits the market by promoting competition and providing more comfort and convenience to individuals. With a phased implementation approach, it is expected that by October 2021 the Brazilian financial market will have concluded the steps towards an interoperable and customer-centric ecosystem.

Since one of the main aspects of open banking is personal data sharing between financial institutions, it is inevitable to draw a parallel with 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'), which is not fully in force yet (date of coming into force is still under debate by the Congress, although an Executive Order from the President - which may not be definitive - postponed the effectiveness of LGPD until 3 May 2021).

In this sense, the recent regulation issued by the Central Bank and the Monetary Council establishes the lawful basis of consent as the unique legal ground to enact the data transferring within the scope of open banking.

Information that might be transferred upon a customer's request or consent include:

- the most updated data directly collected from customers plus those
- collected from public or private databases, except for sensitive data, credit scores and ratings, and login and access credentials; and
- data related to services used by the customer, with transactional and related registered information.

The aforementioned consent to enable such data transferring is broadly regulated by these new rules and cannot be obtained:

- through a subscription contract;
- by any sort of forms with pre-checked consent boxes; or
- in a presumed way (without customer's active expression).

> **Considering the high damages a data breach may cause in the context of customer's financial information, data security is a point of relevant concern**

In other words, the Resolutions set out a highly regulated and detailed data portability right for the benefit of customers from the main banking institutions in Brazil. Considering large-scale services, the establishment of open banking in Brazil is the second example of data portability that may be widely applied in order to facilitate service provision migration, the first one being the implementation of the phone number portability between telecom companies in the year of 2007 by National Telecommunications Agency.

There is no doubt regarding the benefits of open banking's implementation in terms of promotion of competition and empowerment of the customer's choice. On the other hand, however, considering the high damages a data breach may cause in the context of customer's financial information, data security is a point of relevant concern. Taking the European experience as an example, studies show that within less than a month before the deadline, none of the APIs were compliant with the Payment Services Directive ((EU) 2015/2366) ('PSD2') requirements and obligations[1].

Therefore, although information security in the banking context is highly regulated by the Central Bank and usually a strong point of the Brazilian banking system, the European experience shows us that ensuring high security standards on the essentials APIs may be a complex duty, as the privacy dilemma between security and portability this portends is not new.

Last but not least, the implementation of open banking must be celebrated by the privacy professionals in Brazil. The right of data portability is in fact provided by the LGPD (Article 18(V)), but cannot be fully effective without proper regulation, as it tends to become a merely 'right to access 2.0' if there is no definition of certain regulated standards.

Considering that the Brazilian data protection authority ('ANPD') has not yet been established (despite the fact that the part of LGPD that provides its creation is already in force and we should have been receiving its guidelines and complementary regulation during the readiness period), the Central Bank and the Monetary Council's initiative is remarkable and should guide other government-regulated and self-regulated sectors in Brazil.

The right of data portability is key for an open society, although its effectiveness is complex considering it depends on sectors' arrangements that should not be limited to telecom and banking services. In the absence of the ANPD, companies and regulators should take the example of the Central Bank and the Monetary Council to move forward in making data portability feasible in a modern and secure way as the information society demands.

Luis Fernando Prado Chaves Partner
luis.prado@daniel-ip.com
Beatriz Saboya Attorney at Law
beatriz.saboya@daniel-ip.com
Daniel Law, São Paulo

1. See: https://tink.com/blog/open-banking/psd2-status-update/

WEBINAR

Key Takeaways: A Global Perspective on the NIST Privacy Framework

The National Institute of Standards and Technology ('NIST') published, on 16 January 2020, Version 1.0 of its Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. The Privacy Framework is not legally binding. Instead, the Privacy Framework constitutes a voluntary tool which aims to help organisations protect individuals' privacy and enable better privacy engineering practices which support Privacy by Design, intended to be used in conjunction with the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, on which its structure was modelled. The Privacy Framework highlights the interaction between cybersecurity risks and privacy risks, creating the potential for cybersecurity-related privacy events.

On 25 June 2020, OneTrust DataGuidance presented a webinar with Ryan Burch, Global Legal Head of Privacy & Data Protection and Head of Legal for Latin America at PayPal, Andreea Lisievici, Head of Data Protection Compliance at Volvo Car Corporation, and Razvan Miutescu, Counsel at Whiteford, Taylor & Preston. The webinar covered a global perspective on the NIST Privacy Framework and the speakers discussed the privacy background, overview, and practical considerations.

Key takeaways

Privacy Framework overview

The Privacy Framework was published in its final form on 16 January 2020, and had just two months of life before the COVID-19 pandemic stopped a lot of activity around the world. The Framework is intended to help organizations answer, as outlined by NIST, the fundamental question of 'How are we considering the impact on individuals as we develop our systems and products. In other words, what are the privacy consequences of the operation?' The Framework is an entirely voluntary and non-binary tool to assist organizations with compliance with existing legal requirements, but it can also be used as the foundation to help draft new privacy laws. The Privacy Framework was built around the model of the NIST Cybersecurity Framework which was originally released in 2014. The Privacy Framework operates above and beyond legal requirements such as reputation, customer trust and adaption rate and nonetheless flexibility with multiple tiers which consists 4 Tiers: Partial, Risk Informed, Repeatable and Adaptive.

Practical considerations

The Framework is a compliance tool only and does not guarantee compliance. The Privacy Risk Management Practices under the Framework consist of risk management role assignments, enterprise risk management strategy, organizational-level privacy requirements, system/product/service design artifacts and data maps, whilst the Privacy Risk Assessments assist in prioritising risks and responding to risks.

Global context

A larger global context highlights the differences in scope and application of global regulations and highlight the diversities and complexities that privacy frameworks can struggle to accommodate for. The NIST Privacy Framework offers the benefit of being flexible to an organisation's structure and requirements, as well local regulatory and accountability requirements.

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 800 lawyers, 40 in-house legal researchers, and 14 full time in-house translators. OneTrust DataGuidance™ offers solutions for your research, planning, benchmarking, and training.

The NIST Privacy Framework and the NIST Cybersecurity Framework Guidance Notes are available on the OneTrust DataGuidance™ platform highlighting the structure and requirements of the latest versions of both frameworks.

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.

You can access key takeaways and watch all of our webinars in full via the Video Hub at dataguidance.com

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

Website: www.dataguidance.com