Volume 2, Issue 1

January 2020

dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

THE FUTURE OF UK DATA PROTECTION

Eduardo Ustaran discusses the UK's departure from the European Union and the potential for change 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.
eduardo.ustaran@hoganlovells.com

Gita Shivarattan, Ashurst
Gita Shivarattan is a Counsel in the Digital Economy Transactions group at Ashurst LLP. Gita specialises in UK data protection law, and has extensive experience on advising on a range of technology, commercial and data protection law matters including IT outsourcing, business process outsourcing, development and licensing arrangements, and IT-related issues in mergers and acquisitions. Gita also provides practical guidance on the legal and regulatory aspects of digital transformations and implementing dynamic technologies such as cloud, SaaS and automation. Gita has a wide range of experience in advising clients in relation to data protection compliance and has recently supported a number of clients on GDPR compliance projects.
gita.shivarattan@ashurst.com

Tom Brookes, Ashurst
Tom Brookes is a Solicitor in Ashurst's Digital Economy Transactions Group and is based in London. Tom has recently completed a six month secondment in the legal team of a global technology company, and has advised a number of multinational companies on data protection matters relating to data breach response, GDPR compliance projects and corporate acquisitions. He also has experience advising on the strategic issues relating to the adoption and use of emerging technologies, such as virtual shopping assistants. Prior to training as a solicitor, Tom was an Analyst at OneTrust DataGuidance, where he was responsible for managing content for Africa, Middle East and Asia Pacific.
tom.brookes@ashurst.com

Laura Flannery, Data Protection Commission, Ireland
Laura is an Assistant Commissioner in the Irish Data Protection Commission. She leads the DPC's work on International Affairs and One Stop Shop Operations. She also engages on a daily basis with counterparts at each of the other DPAs in the European Data Protection Board. As such, she's at the heart of the DPC's work on consistency of enforcement and cooperation, in the context of Ireland's Lead Supervisory Authority work. Laura also engages with DPAs from further afield.

Michelle Griffey, Communisis
Michelle Griffey is the Chief Risk Officer at Communisis, having been there since 2016. Michelle has over 30 years' experience across a wide range of areas, including risk and governance. Michelle initially built the risk function for the Customer Experience division at Communisis and is now responsible for managing risk across the group.

Stevan Stanojevic, Etihad Airways
Stevan Stanojevic is the Group Data Privacy Manager at Etihad Airways. Stevan oversees compliance with data privacy laws across six continents. In the past he has helped organizations establish compliance programs by increasing awareness, creating registers of processing activities, drafting privacy policies and notices.

Image production credits
Cover / page 4 image: Chalabala / envatoelements
Page 12 image: shulz / Signature collection / istockphoto.com
Page 20-21 image: SimonSkafar / Signature collection / istockphoto.com
Page 26-27 image: piccerella / Signature collection / istockphoto.com
Page 30-31 image: piranka / Signature collection / istockphoto.com
Page 32 image: merc67 / Essentials collection / istockphoto.com
Page 33 image: Pgiam / Signature collection / istockphoto.com
Page 34 image: scyther5 / Essentials collection / istockphoto.com

Data Protection Leader is published bi-monthly by OneTrust DataGuidance 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
Kotryna Kerpauskaite, Alexander Fetani, Lea Busch

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

EDITORIAL

"The UK cannot afford to go alone to achieve the best of all possible worlds: economic progress and protection for individuals. "

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

As with anything Brexit-related, the UK Government is facing a dilemma in relation to data protection law. Shall we follow the direction of travel of the past 25 years and opt for the continuity and certainty provided by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') or shall we use the departure from the EU to make radical changes to the regulation of data uses and privacy? On the one hand, it would be reassuring to know that despite Brexit's uncertainties, the current framework is here to stay and it will develop in a familiar way. On the other hand, it must be tempting to use this opportunity to completely re-think what is in the best national interest. For an area of law and policy that is so closely related to technological development and prosperity, it would be foolish not to consider whether a different formulation would lead to better outcomes. A dilemma indeed.

An important consideration to take into account in this process is what is happening across the rest of the planet. In today's uber-connected world, data is by definition global. So its regulation is spreading in consistent ways around the globe. Right now, the California Consumer Privacy Act of 2018 ('CCPA') is a huge focus of attention. The CCPA has a very different pedigree from the GDPR but it is essentially about giving people control over their data and the ways it is used by others. Looking at other countries that are actively developing new privacy legislation – from Brazil to India and from Bermuda to New Zealand – there is a visible thread towards strong accountability and powerful regulators. Each jurisdiction faces its own political nuances and social needs, but the emphasis is on comprehensive laws that follow a global trend.

If Brexit is about taking back control, in data protection terms, it must mean looking at where UK data protection law would likely be heading in the absence of any EU interference. In other words, if one looks at the history of UK data protection as a reflection of the country's ambitions and public policy goals, where would it make sense to be heading at this moment in time? Recalling 34 years of practice in this area, Jonathan Bamford, former Director of Strategic Policy at the Information Commissioner's Office, recently pointed out that data protection law was set up to encourage public trust and confidence, and that this objective is still alive today. As he put it, at the heart of all the legislation in this area are the same simple principles of looking after people's information properly and in ways they would understand. That was and will always be the British approach to practical and workable data protection.

Speaking of being practical, Brexit is also about departing from the EU in an orderly and non-chaotic fashion. The Political Declaration ('the Declaration') that accompanies the much-debated Withdrawal Agreement agreed between the UK Government and the European Council already confirms what the approach will be. According to the Declaration, both the UK and the EU are committed to ensuring a high level of personal data protection to facilitate data flows between them. The Declaration goes on to say that the European Commission will start the adequacy assessment with respect to the UK as soon as possible after the UK's withdrawal, endeavouring to adopt its decision by the end of 2020, if the applicable conditions are met.

So, what is the right way forward for the future? The UK cannot afford to go alone to achieve the best of all possible worlds: economic progress and protection for individuals. The UK must follow its instinct and lead the way by promoting progressive regulation that is in sync with a digitally borderless world. In doing so, it should look at what other leading democracies are doing and be prepared to be aligned in approach. In its relation with the EU, it should find a magical yet pragmatic way of achieving a mutual recognition of frameworks that paves the way for seamless data flows. With its mature law, robust individual rights, and influential regulator, the UK is in an extremely strong position to get there. The future of UK data protection law looks distinctively forward thinking, but above all, it should be anchored on responsibility and democratic values.

Updates to the GDPR v. CCPA report

*Download a copy of the latest edition of the GDPR v. CCPA comparison report, produced in collaboration with the Future of Privacy Forum, through the **OneTrust DataGuidance Regulatory Research platform**.*

www.platform.dataguidance.com

OneTrust DataGuidance released an update to its GDPR v. CCPA report in December 2019, ahead of the entry into force of the California Consumer Privacy Act of 2018. The updated report takes into account a series of bills, signed by the California Governor on 11 October 2019, amending the CCPA to exempt from its application certain categories of data and to provide different requirements for submission of consumer requests, among other things.

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the California Consumer Privacy Act of 2018 ('CCPA') (SB-1121 as amended at the time of this publication) both aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share personal data, whether the information was obtained online or offline.

The GDPR, which went into effect on 25 May 2018, is one of the most comprehensive data protection laws in the world to date. Absent a comprehensive federal privacy law in the U.S., the CCPA is considered to be one of the most significant legislative privacy developments in the country. Like the GDPR, the CCPA's impact is expected to be global, given California's status as the fifth largest global economy. The CCPA came into effect on 1 January 2020, but certain provisions under the CCPA required organisations to provide consumers with information regarding the preceding 12-month period.

As highlighted by this report, the two laws bear similarity in relation to their definition of certain terminology; the establishment of additional protections for individuals under 16 years of age; and the inclusion of rights to access and delete personal information.

David Longford, CEO at OneTrust DataGuidance, comments, "CCPA is already having a huge impact on organisations. Companies have been investing huge amounts of resources in preparing for its entry into effect as well as building new processes and procedures to monitor and maintain ongoing compliance. With questions still remaining regarding the finalised version of the Attorney General regulations under the CCPA, there is a need for organisations to stay up-to-date and understand any additional obligations as they are released.

At OneTrust DataGuidance, we have made assisting our clients with CCPA compliance a key priority since its initial introduction, and have continued to expand our dedicated CCPA tools around Research, Planning, Benchmarking and Training."

However, the CCPA differs from the GDPR in some significant ways, particularly with regard to the scope of application; the nature and extent of collection limitations; and rules concerning accountability. Regarding the latter for example, the GDPR provides for obligations in relation to the appointment of Data Protection Officers, the maintenance of a register of processing activities, and the need for Data Protection Impact Assessments in specified circumstances. Conversely, the CCPA does not specifically focus on accountability-related obligations, even though such provisions exist, such as the obligation for companies to train their staff that deal with requests from consumers.

It is also noteworthy that the core legal framework of the CCPA is quite different from the GDPR. A fundamental principle of the GDPR is the requirement to have a "legal basis" for all processing of personal data. That is not the case for the CCPA.

In addition, the CCPA excludes from its scope the processing of some categories of personal information altogether, such as medical data covered by other U.S. legal frameworks, including processing of personal information for clinical trials, and personal information processed by credit reporting agencies. Moreover, the CCPA focuses on transparency obligations and on provisions that limit selling of personal information, requiring a "Do Not Sell My Personal Information" link to be included by businesses on their homepage. In addition, the CCPA includes specific provisions in relation to data transferred as a consequence of mergers and acquisitions.

Finally, the California Attorney General issued, on 10 October 2019, Proposed Regulations under the CCPA which are intended to providepractical guidance to consumers and businesses. The Proposed Regulations were open for public consultation until 6 December 2019 and, when finalised, will provide an additional layer of regulatory requirements that companies will have to comply with.

OneTrust

PRIVACY, SECURITY & THIRD-PARTY RISK

CCPA is Here, Get Ready in 2020

FEELING THE PRESSURE TO BE CCPA READY?
WE'VE GOT YOU COVERED

- Same Day Implementation
- 7-Day Availability
- Manage Cookie Consent
- Prepare for Opt-Out
- Simplify Consumer Rights

Let us Help! Email

CCPAHelp@OneTrust.com

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

Emerging Tech

Episode 4

Gita Shivarattan Counsel
gita.shivarattan@ashurst.com

Tom Brookes Solicitor
tom.brookes@ashurst.com

Ashurst LLP, London

OneTrust DataGuidance have partnered with Ashurst LLP to present Emerging Tech, a four-part series of articles and videos on the data protection issues relating to novel forms of technology. Alexis Kateifides was joined by Gita Shivarattan and Tom Brookes, from Ashurst, for the fourth instalment of the series. They introduce some of the key issues users should consider within the ad tech industry in terms of data privacy law.

Fuelled by consumer expectations of receiving free services, information, and products, global digital advertising spend reportedly surpassed $100 billion dollars in 2018[1] with its revenue predominantly driven by 'ad tech.' At its core, ad tech refers to tools that analyse and manage information for online advertising companies and automated processing of advertising transactions.

Despite being a relatively mature industry, ad tech is one of the sectors to be hardest hit under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') because it is an industry powered by cookies, the use of which often involves the processing of personal data. The current lack of clarity in relation to the interplay between the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') and the GDPR has further had a disproportionately problematic impact on the industry.

Ad tech is in the regulatory spotlight as a result of several high-profile investigations into the technology, and the *Financial Times* reported that 12 data protection supervisory authorities are investigating complaints relating to ad tech. Earlier this year, the Information Commissioner's Office ('ICO') issued an updated report into ad tech and real-time bidding[2] ('RTB') ('the ICO Report') which has become a regulatory priority area for data protection, competition, and consumer protection.

In this fourth and final part of the Emerging Tech Series, we examine some of the main data protection challenges companies operating in the ad tech space are grappling with and look ahead to what the future may hold.

RTB – what is the big deal?

In its most basic form, advertising involves providing information about new products and services and digital advertising delivers this information through the medium of the internet. Whilst the first webpage banner advertisement was created back in 1994[3], the explosion of internet use due to increasingly ubiquitous connectivity has led to exponential growth in digital advertising.

RTB is an auction process that occurs in 'real-time' to sell visual advertising

***Figure 1**: Information included in bid request*

<table>
<tr><th colspan="4">RTB Participants</th></tr>
<tr><td>Publisher

Organisations who have advertising space (inventory) on their websites and platforms and apps to sell to Advertisers</td><td colspan="2">Advertising Exchanges and Severs

The location where bidding takes place. Mediates between Publishers and Advertisers and operates on both buy and sell sides.</td><td>Advertiser

Organisations who want to broadcast information on their products and services to consumers on a Publisher's advertisement space</td></tr>
<tr><td></td><td>Sell-side platform ('SSP')

Platform to help Publishers manage and sell their inventory</td><td>DSP

Platform used by Advertisers to place bids for inventory space on websites and platforms of Publishers</td><td></td></tr>
<tr><td colspan="4">DMP

Platform which analyses and combines data including personal data from multiple sources to facilitate targeted advertising personalised to an individual consumer</td></tr>
<tr><td colspan="4">Consent management platform ('CMP')

A tool which manages consents e.g. of individuals using a Publisher's website or platform</td></tr>
</table>

***Figure 2**: RTB Participants*

on websites and apps. Whilst there exist a variety of other forms of digital advertising and ad tech, this article focuses on programmatic advertising and RTB due to its widespread adoption[4] and the level of regulatory attention that RTB, in particular, has received to date.

In essence, RTB involves an operator of an online service (a 'Publisher') selling space on their website to be filled by the content of advertisers as a result of successful bids on a per end user basis.

The bid process relies on cookies or other technologies, such as pixels, that collect information from an end user's device when they visit a Publisher's website. This information is often enriched by a data management platform ('DMP'), which collates known information or infers additional information about the end user, thereby making the 'bid' more accurate, and therefore more valuable.

Multiple advertisers then place bids for the opportunity for their digital advertisement to be displayed to the end user in the advertisement inventory space on the Publisher's website.

Advertisers are aiming for their adverts to be displayed to individuals who are most likely to purchase their products, which is reliant on the information collected about the individual in the RTB process.

The information contained in the bid request may contain varying amounts of known and inferred personal data relating to the end user. According to the ICO Report[5], the categories of information included in **Figure 1** (above) can potentially be included in a bid request and will constitute personal data as defined under Article 4(1) of the GDPR, where they enable an individual to be identified either directly or indirectly.

The ad tech ecosystem

Set out in **Figure 2** (above) is an overview of the range of parties who are commonly involved in the RTB process ('RTB Participants'). The ad tech operating model is complicated by the fact that one organisation could potentially wear 'a number of hats' in the ad tech process, for example, having a demand-side platform ('DSP'), an Advertising Exchange, and a DMP.

Core data protection issues highlighted by the ICO Report

In the UK, there are two main data protection legislations which RTB Participants are required to adhere to, PECR and GDPR. PECR governs the use of cookies and other technologies on an end user's device, as this constitutes the use of an electronic communications network to store information. The GDPR governs personal data, and cookies will often involve the processing of personal data.

In July 2019, the ICO published Guidance on the Use of Cookies and Similar Technologies[6], which explains how PECR applies to the use of cookies and how PECR interacts with the GDPR. However, the EU data protection regulatory landscape is currently in a state of flux, with the underlying directive of PECR (Directive 2002/58/EC) set to be replaced by a new e-privacy regulation, once finalised by the EU institutions.

Lawful basis

Where personal data is processed, a lawful basis is required under the GDPR. In the context of RTB, the lawful bases

traditionally relied on are either consent of the individual whose personal data is being processed, or legitimate interests of the RTB Participant. However, the ICO Report noted there was a lack of clarity over which lawful basis many RTB Participants were relying on.

For any processing of special categories of personal data, such as information about an individual's political opinions, religion, health information, or ethnic group, the GDPR requires the explicit consent of the individual to be obtained, unless specific exemptions apply[7]. These exemptions are not applicable in the context of RTB. The ICO Report noted[8] that a proportion of RTB bid requests involve the processing of special categories of personal data, and found that consent requests which they had reviewed were not compliant with the GDPR, and needed to be modified to ensure explicit consent was collected prior to the processing of personal data.

In relation to non-special categories of personal data processed in the RTB process, the ICO stated that it believes the nature of the processing makes it impossible to meet the legitimate interests lawful basis requirements[9] for the main bid request processing[10].

This means that the lawful basis for processing involved in collecting personal data from an end user, and the onward transfer of that personal data in the bid request, is consent. In contrast with the GDPR, consent is required under PECR in order to drop cookies on the user's device, unless they are strictly necessary[11].

The consent requirements under both the GDPR and PECR are very specific and pose a number of challenges for RTB Participants. In particular, consent must be[12]:

- unambiguous, meaning pre-ticked boxes surfaced on a Publisher's website cannot be used;
- specific, meaning the consent must be obtained for each processing operation and be clearly distinguishable from other matters. Therefore one 'bundled' consent for each aspect of processing involved in the RTB process is not possible; and
- freely given, meaning that the individual must be given the choice of accessing a website or application without tracking cookies being dropped on their device.

It is common for CMPs to be used by RTB Participants, and in particular Publishers, to manage consents from users of their websites and applications. The Interactive Advertising Bureau's Transparency and Consent Framework[13], which is an industry initiative to assist RTB Participants in complying with the GDPR, relies on CMPs to obtain, store, and signal consents. However, RTB Participants need to carefully consider whether the consents obtained by CMPs meet the GDPR requirements discussed above if they are relying on these consents for their lawful basis to process personal data.

The ICO did not provide guidance regarding the lawful basis which could be relied on in relation to other aspects of processing which take place in the RTB process after a bid request is made, such as processing by advertisers, DSPs, and SSPs, who have no direct relationship with the end user whose personal data is being processed. Regardless of the lack of guidance, all RTB Participants need to undertake a careful assessment of the lawful basis they choose to rely on and ensure this is documented.

Transparency and fair processing notices

The GDPR requires transparency in relation to how personal data is processed and Articles 13 and 14 of the GDPR set out specific information which must be provided to individuals. PECR also requires clear and comprehensive information about the cookies and other technologies which are dropped on a device to be provided to the relevant individual[14]. In the context of RTB, the primary challenge faced by RTB Participants is being able to clearly describe to individuals, using clear and plain language, the complex processing operations and data flows which are taking place. These data flows often involve automated processing of large volumes of data for various purposes such as targeting, fraud prevention, analysis, and measurement, which requires both careful explanation and presentation in the privacy notice.

There is a tension between providing information which is either too granular or too high level, and in order to comply with these transparency requirements, it is essential that RTB Participants have clarity about:

- how their processing operations work, including what is the purpose for collecting each type of personal data;
- who they share any personal data with; and
- how they are enabling individuals to exercise their rights in relation to this processing.

Intrusive and unfair processing

The ICO Report also noted that during the RTB process, bid request information is often combined and enriched by creating a profile of an end-user using information gathered from other sources, such as DMPs.

The ICO's main concern with these activities is that this may constitute unfair and intrusive processing due to the quantity and nature of the personal data being processed, which appears to be disproportionate to the purpose of delivering targeted advertising[15]. Another key concern is the fact that individual users may not be aware that this combining and enrichment is taking place if fair processing notices do not clearly inform individuals what is happening.

Pursuant to Article 35(4) of the GDPR, the ICO has published a list of processing operations[16] likely to require a data protection impact assessment ('DPIA') to be undertaken, which includes data matching for the purposes of direct marketing. RTB Participants involved in information enrichment processes will need to conduct a DPIA in order to identify and minimise the data protection risks relating to this processing.

Other processing activities for which the ICO deems a DPIA mandatory include large scale profiling of

individuals, tracking of an individual's location and behaviour, and invisible processing where personal data which is being processed was not obtained directly from the individual and the organisation does not notify individuals of the processing due to a perceived disproportion effort[17].

Given the activities included on this mandatory list, all RTB Participants need to carefully consider whether they need to undertake DPIAs in relation to their processing of personal data.

Next steps

The ICO Report served notice on the ad tech industry that there are serious concerns about data protection compliance in relation to the RTB process, and highlights that the ICO wants the industry to take the initiative of reforming their activities. This raises difficult questions for each and every RTB Participant, such as how much personal data is actually necessary for the purposes in which they are using it, how can this personal data be collected and shared lawfully, and how can individuals be clearly informed about what is happening.

Conducting detailed DPIAs should form the starting point in assessing how to deal with these issues, however, time appears limited for the ad tech industry to come up with the answers. The ICO made it clear when the ICO Report was published in June 2019 that it would conduct a further industry review in six months' time. This could result in enforcement activity and potentially sanctions (including fines) given the nature of the non-compliance which was revealed in the ICO Report. Such a review could also focus on other aspects of non-compliance with the GDPR, which were referenced in the ICO Report but not considered in detail, such as data minimisation and data retention.

This is the final instalment of the Emerging Tech series in partnership with Ashurst LLP. To recap on previous episodes covering AI, Blockchain, and more, as well as additional video content visit the ***OneTrust DataGuidance Video Hub.***

1. Available at: https://www.iab.com/wp-content/uploads/2019/05/Full-Year-2018-IAB-Internet-Advertising-Revenue-Report.pdf
2. Available at: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf
3. Available at: https://www.wired.com/2010/10/1027hotwired-banner-ads/
4. Almost 90% of digital display advertising in the UK is programmatic according to emarketer, available at: https://www.emarketer.com/content/programmatic-ad-spending-in-the-uk-2019
5. Available at: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf (section 2.6 pages 12-13)
6. Available at: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/
7. Article 9 of the GDPR.
8. ICO Report page 16 section 3.2.
9. To rely on legitimate interests, organisations need to identify a legitimate interest, show that the processing is necessary to achieve that interest, and balance that interest against the individual's interests, rights, and freedoms.
10. ICO Report page 17 section 3.3.
11. Regulation 6 of PECR.
12. Article 7 and Recital 32 of the GDPR.
13. Available at: https://iabeurope.eu/transparency-consent-framework/
14. Regulation 6(2) of PECR.
15. ICO Report page 20 section 3.4.
16 ICO Examples of processing 'likely to result in a high risk,' available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/
17. Ibid.

Regulator Spotlight

OneTrust DataGuidance sat down with Laura Flannery, Assistant Commissioner at the Data Protection Commission, Ireland in October 2019 for our 'Regulator Spotlight' series. Laura shares her opinion on how the European Data Protection Board's ('EDPB') consistency mechanism has developed as well as discussing the key differences between the GDPR and Ireland's implementation law.

How has your work within the Irish Data Protection Commission been impacted by the entry into effect of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR')?

Obviously, with the GDPR it is great to have a harmonised law and have a better platform to work from because our laws in the past did not take into account the development of digital technology. In terms of our work, there has been an awful lot more awareness and, therefore, there has been a huge increase in complaints from data subjects. I think we have had over 10,000 since the GDPR entered into force, and we have also had quite a huge increase in data breach notifications. So, for ourselves, we have expanded unbelievably in the last couple of years, and we have had to deal with that and deal with the challenges and the opportunities that brings as well. We have had some major recruitments, we have hired a lot of legal and technical expertise, as well as investigators to cope with that. So, it has been a time of growing and a time of learning so far.

How has the EDPB's consistency mechanism developed in the management of cross-border cases?

The development in terms of the mechanism has not really been tested as of yet, particularly in relation to complaints, but there have been a number of consistency opinions in relation to data protection impact assessments. There have been a few Article 64 of the GDPR opinions as well. But, the role of the EDPB has not really been tested for consistency in terms of dispute resolution between an elite supervisory authority and a concerned supervisory authority that has not really been fully tested yet. So, we have a bit of a learning curve and we have a bit of a way to go with the consistency mechanism. But on the other hand, we actually, in terms of cooperation, we have been sharing our experiences across all of the data protection authorities and using expertise from other data protection authorities and feeding into that. So, it has actually been quite beneficial already without the mechanism being tested yet, and we can see the benefits that we will have in the future.

How do you see the future development of mechanisms for the transfer of data?

There has actually been a lot of focus on this and a lot of discussion about this at the moment because of Brexit, and particularly, as you are aware, if there is a no deal Brexit, all of a sudden Great Britain becomes a third country. And so, there would be a lot of small and medium-sized enterprises and an awful lot of data controllers in Ireland who, by nature of our closeness with the UK, would be transferring personal data to the UK. So, we advise, at the moment, that Standard Contractual Clauses ('SCCs') are actually one of the most convenient methods to transfer personal data. Until there is a decision on Brexit, we do not know what way the Court of Justice is going to go in their decision. They may find the SCCs are actually perfectly valid and legal. There are other mechanisms, in the GDPR, providing for these, such as adequacy decisions and binding corporate rules.

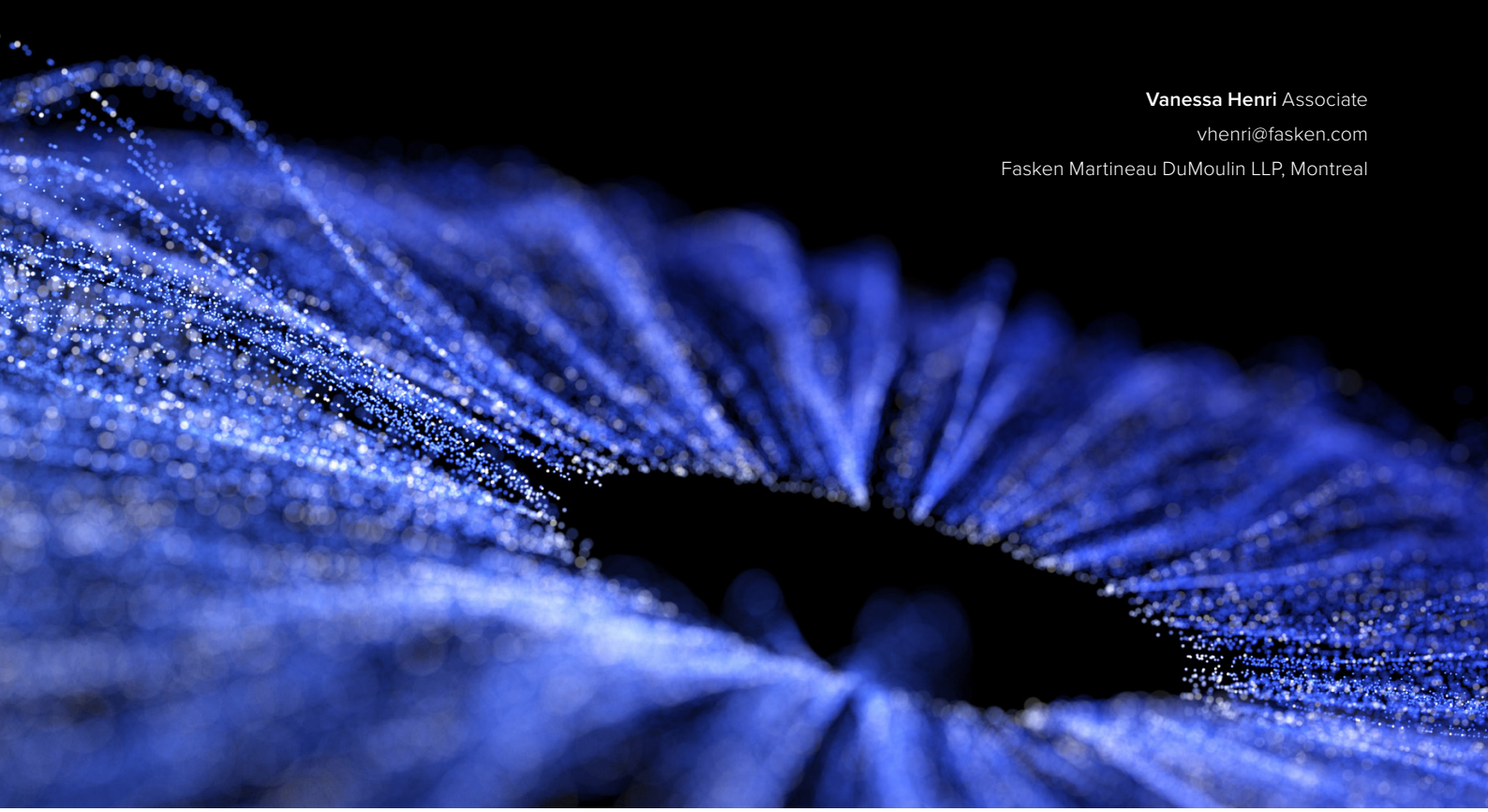
There is also a lot of potential for a code of conduct and certification mechanisms. Again, this has not been tested, but in the EDPB, one of the working groups is actually looking at providing guidance in terms of using codes of conduct and certification mechanisms as tools for international transfers. But there are other ways. and we are positive that there will be ways there, but again, it is a learning curve and there will be quite a way to go for the future landscape of data transfers.

What are some of the key differences between the GDPR and Ireland's implementation law?

So, while the GDPR has tried to harmonise as far as possible, there are differences in each member state at the moment that still need to be worked on and defined. For ourselves in particular, Article 80 is one whereby a mandated body, the legislator decided not to allow a body to bring a complaint to us without a data subject mandate behind it. And that is something that is different from some of our colleagues, which is causing a little bit of difference in the application of the GDPR. Legally, in Ireland we would be under the common law system, which is quite a bit of different to the civil law system. So, as part of our process in terms of dealing with complaints, we have a separate investigation and decision-making process, and there would be quite a lot of engagement with data controllers giving them the right to be heard and due process in our procedures. This would be slightly different from some of the other supervisory authorities who, under the civil law system, have a very different mentality in terms of enforcement and wouldn't engage quite as much as we would engage at times. That is one of the differences. But again, there are improvements. The GDPR is due to be reviewed by the commission and these matters will be discussed then. There are differences in our systems, but we are working our way through them to ensure the most important thing, which is the data subject at the end of the day, and ensuring that their rights are vindicated.

Laura Flannery
Assistant Commissioner at the Data Protection Commission, Ireland

*Laura's interview is part of OneTrust DataGuidance's '**Regulator Spotlight**' series which features over 20 new interviews with a range of regulators and commissioners from across the world, including the European Data Protection Supervisor and the Privacy Commissioner for Personal Data, Hong Kong.*



Vanessa Henri Associate
vhenri@fasken.com
Fasken Martineau DuMoulin LLP, Montreal

International: Deepfakes and their risks to society

'Deepfakes' is an infamous buzzword initially made popular through somewhat benign manipulation of celebrities' pictures and videos. However, it is a lot more than that. Artificial intelligence ('AI') applications, such as machine learning, work to create deepfakes, which the creation of have led to certain privacy implications. Vanessa Henri, Associate at Fasken Martineau DuMoulin LLP, discusses the main impacts and concerns surrounding deepfakes, and whether the regulation of deepfakes is possible.

From a technical standpoint, deepfakes are made using artificial neural networks that aggregate existing media through machine learning and there are many techniques that can be used, such as generative adversarial networks ('GANs'). GANs are able to generate new faces that have never existed before through machine learning[1], many of which are already being used for fake social media accounts. While this is problematic enough, deepfakes impersonate living individuals, and their identity. For many, this is just fun and games, but for others, the consequences are real.

As a starter, deepfakes are predominantly used against women. 'The State of deepfakes 2019[2],' is a study by Deeptrace Labs from October 2019, and it reported that nearly 96% of the deepfakes on the internet are used in non-consensual porn involving women, 41% of which are British or American actresses and 25% of which are from South Korean descend. This is not only an invasion of these women's privacy, but also a discriminatory practice that sexualizes women and directly attacks their dignity. It is a processing of biometric personal information that results in discrimination, and as a result, is not a licit processing of personal information under many privacy legislations. This is acerbated when used in the context of revenge porn, which has implications beyond privacy, and directly to the core of human rights framework.

Deepfakes can also be used in politics to misrepresent what the politicians and other public officials have said or done. A report by researchers at New York University[3], published 3 September 2019, identified deepfakes as one of eight factors that may contribute to disinformation during the 2020 US presidential election. Concerns about misinformation resulting from such technologies are very present in Canadian news outlets, and many news outlets concerned with impacts on democracy have joined forces with organisations such as the Trusted News Charter, an initiative to strengthen measures to protect audiences from disinformation, led by the British Broadcasting Corporation.

In the same line of thoughts, Canadian Prime Minister Justin Trudeau introduced a Digital Charter ('the Charter') to combat hate speech, misinformation, and online electoral interference. While there are some innovative concepts in there, such as algorithmic transparency and impact assessments, as well as much needed improvements to the Personal Information Protection and Electronic Documents Act, 2000, what is striking is the recognition

of the role of trust in the digital world, and of the fact that it can be easily eroded through misinformation. While the Charter is not a law, but rather an approach to modifying current law, the role of trust in the digital economy should be a guiding principle for judges to interpret any existing or upcoming legislations in our modern data-driven economy.

Following the elections, Mr. Trudeau mandated the Honorable Mr. Bains, Minister of Innovation, Science and Industry to work with the Minister of Justice and Attorney General of Canada to advance the Charter, including 'the ability to be free from online discrimination including bias and harassment,' and 'with the support of the Minister of Digital Government, continue work on the ethical use of data and digital tools like AI for better government.'

Indeed, a more pervasive impact of deepfakes is the erosion of trust within society. Trust is so critical to Western societies that many of our laws are built upon this concept, even in the corporate world, directors are bound by a fiduciary duty to a corporation. In fact, the crime of treason is so important that in the US, it has been incorporated directly within the Constitution, the most fundamental law of a country. Deepfakes attack the very foundation of society through integrity and trust, and have become a source of considerable reputational damages for both private and public institutions.

Should deepfakes be banned altogether then?

The Chinese Government responded swiftly, making the spread of fake news and misleading videos using AI entirely illegal as of 1 January 2020. The Cyberspace Administration of China will be enforcing this new policy, and will likely lead to prosecution of users, and possibly, video hosting websites. So, what are we waiting for in Canada?

Of course, the need to regulate deepfakes is emerging as a central point for regulators, shown by the several pending bills establishing a private right of action against creators and distributors in the US.

Nonetheless, there are many issues with regulating deepfakes:

- how can deepfakes be identified and recognised, ideally in real-time;
- how can culprits be identified, and how can attribution be proved;
- how is it ensured that the trouble does not outweigh the benefits for the victims that would have to go through these lawsuits;
- how is it ensured that these lawsuits are actually affordable and do not end up as a David against Goliath situation, where the average joe must sue a BigTech;
- how can the inherent rhythm of courts and lawsuits be reconciled with the urgent need to control and mitigate the effects of deepfakes;
- how is it ensured that police departments are equipped to conduct investigations relating to deepfakes;
- how is it ensured that crown attorneys have the technical knowledge required to conduct these types of criminal accusations; and
- even if a deepfake is identified, how can it be removed from the Internet in a timely manner, and is that even possible?

Many of these questions are not specific to deepfakes, but to articulating legal frameworks in technological context and within IT architectures often owned by private parties and located in various jurisdictions around the world. These questions have been long-debated, such as in the context of cybersecurity.

This reality means that governments are ill-equipped to address modern technology-related issues on their own, and that they must collaborate with private companies. For instance, platforms such as social media websites, are likely best equipped to address the deepfakes issue resulting from content shared through their infrastructure. With the right technologies, they are more likely to identify in real-time the user's IP, trace the origins of the posts, and remove these posts almost immediately.

Doing this from the outside would require extensive resources, such as filling injunctions to ask these platforms to remove the content and sending subpoenas to obtain data on the crime, etc. In addition, allowing governments broad powers to intervene would likely breach many constitutional principles protecting private assets from arbitrary interventions. In the long term, it may lead to unintended consequences that have not been assessed, which means that relying on governments to fix the deepfakes issue is delusional. At best, they can drive a public-private partnership requiring private companies to implement some measures to identify, contain, and eradicate deepfakes.

This raises the issue of determining who will be liable if deepfakes are to be regulated. Identifying the users behind deepfakes can be difficult and proving attribution even more difficult. In a criminal context, the *mens rea*, ie. the malicious intent as defined in the criminal provision, would need to be proven. Users may share deepfakes without knowing or may create deepfakes for benevolent reasons that may be acceptable, such as if they are identified as deepfakes. There are many grey areas in terms of what is malicious intent with deepfakes. Prosecuting users will likely turn out to be a difficult task. Even if not impossible, this would mean that only a small percentage of deepfakes scam artists would be prosecuted, and that prosecution would not be an effective deterrent.

Another option, therefore, is to hold platform owners liable, which is a highly debated topic in the field of technology law. Whether a platform should be held liable for the content posted or shared through their platform, and whether it should be required to deploy certain measures to prevent deepfakes or similar fake news, is a cultural question that depends, at least partially, on how individual rights are articulated and balanced in a legal system. For instance, in the US, the protection against free speech is 'broader' than in Canada, where hate speech is not considered free speech. Both legal systems have exceptions regarding freedom of speech, but only Canada has anti-hate propaganda statutes.

In the US, §230 of the Communications Decency Act of 1996 provides immunity for internet service providers ('ISPs'), in addition to specific immunity in State laws, for instance the Code of Virginia 1950 Annotated §18.2-386.2 on unlawful dissemination or sale of images of another. By contrast, the Supreme Court of Canada has established in two landmark decisions that ISPs can become liable if they fail to act once given notice of infringement.

This distinction between both legal systems regarding intermediaries' liability has been weakened by the North America Free Trade Agreement ('NAFTA'), since Article 19.17 states that, 'other than as provided in paragraph 4, no party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information".

Paragraph 4 provides an exception regarding the enforcement of criminal law, or the obligation of an interactive computer service from complying with a specific, lawful order of a law enforcement authority. All this legal and cultural context must be considered when regulating

deepfakes in Canada, and as a result, it raises some very delicate questions.

Regulating technologies is not easy. It requires drafting laws that can evolve over time. This often calls for expressions such as 'reasonable' or 'adequate' which must be operationalised by private organisations, leading to much uncertainty. These laws also face strong lobbyism from various industries, as they are often perceived as an obstacle to innovation. In a knowledge-based economy like Canada, regulating innovation such as AI can be an economic suicide if ill-redacted. Of course, regulating deepfakes does not amount to regulating AI, but there can be unintended consequences and impacts. In addition, regulating at the state or country-level has become an issue in a world of international technologies and global trade. Small and medium-sized enterprises are often unable to monitor the vast arrays of legal obligations with the same capabilities than Big Tech can afford, resulting in inadvertent impacts on free competition in an industry that is already perceived as overly monopolistic.

Most importantly, in many cases, the actual legislations are perfectly fine, and can be interpreted to cover a new technological context. When cryptocurrencies gained popularity, many regulators raced to draft the first regulation and set the tone. Nonetheless, a close study of the cryptocurrencies' ecosystem demonstrates that most of the elements that were perceived as unregulated could be regulated under existing laws, or under existing laws with new guidance. This is largely a result of the opaque nature of information technologies that is maintained through buzzwords such as 'dark net,' 'deepfake,' 'AI,' and 'cyberspace.' These do nothing to help regulators, they only paint technologies as incomprehensible and in need of being controlled, while in the end, there are much more cables and physical structures than the buzzwords would let you think.

For instance, the Copyright Act of Canada may be used by video and pictures owners to claim copyright infringements of their videos and pictures that are used for deepfakes, and courts may order copies of modified videos and photos to be destroyed. These rights are extended through international treaties, such as the Agreement on Trade-Related Aspects of IP Rights. The Canada Elections Act also contains provisions to address situations when technology is used to influence or disrupt a Canadian election, such as §480.1 introduced through the Fair Elections Act of 2014, which addresses impersonation directly. An Act to amend the Canada Elections Act and other Acts and the make certain consequential amendments (the Elections Modernization Act) also covers the publication, distribution, transmission, and publishing of misleading or false statements. While there are exceptions applicable to parody and satire, this should not prevent malicious actors to be targeted where there are impacts on democracy. It is also noteworthy that that the Canadian Centre for Cyber Security updated its report 'Cyber Threats to Canada's Democratic Process' in June 2017 to touch on deepfake technology.

Other legal grounds already existing in Canadian law may include defamation, if there is no disclaimer that the media is manufactured, and privacy-related torts or legal actions, in Quebec, privacy is a right subject to punitive damages in addition to compensation. Canadian common law also includes a tort of appropriation of personality. Finally, there are several articles that can be leveraged in the Criminal Code of Canada, RSC 1985 c 46, including the recent amendments on revenge porn.

We are far from a legal void, as clearly, the issue does not lie within the law or the lack of awareness of concerned entities and individuals, but rather within the capacity to enforce the legal remedies online. It's not obvious that spending more resources on legislations will actually address deepfakes.

Therefore, initiatives around technologies to identify and tag deepfakes in real time, such as the Defense Advanced Research Projects Agency's Media Forensics Program[4], are needed more than any additional legislations. These initiatives are increasingly common in the private and non-for-profit sector.

As with cybersecurity, a private-public partnership is likely the right approach.

The Deepfake Report Act of 2019 (S. 2065), is one of the bills in the US which would require the Department of Homeland Security to:

- issue an initial report within 200 days and then every 18 months;
- assess the AI technologies used to create and detect deepfakes; and
- make suggestions on changes needed in legislation.

To the same effect, in the above cited mandate letter to the Minister of Innovation, Science and Industry, Mr. Trudeau requested to support the Chief Science Advisor to ensure that the government's pure and applied science is fully available to the public. While this lacks the specificity and maturity of the proposals currently on the table in the United States to address deepfakes, the commitment to work with the private sector remains critical.

With accurate data, companies would be in a better position to keep up with new deepfakes technologies and adjust, but with what incentives? What's in it for companies to remove deepfakes? The Federal government would have to create a clear system of incentives within its already bloomy cybersecurity ecosystem to work hand in hand with the private sector on these critical issues that will shape the future.

This private-public partnership is likely more useful than a legislation, but this approach continues to put us in a position where we react to threats rather than anticipate them. Would it be possible that we are thinking within the box created by deepfakes scam artists? Maybe detecting fake media is not the right approach, and perhaps, certifying the authenticity of the original media through new technologies is worth exploring.

Innovation is disruptive, and sometimes that means more than just re-inventing some features of a game to score better points, but rather reinventing how the game must be played. Blockchain technologies and cryptographic signing remain marginally used, notwithstanding a clear and demonstrable use. Energy would be better spent exploring safer ways to manage our identities and content media than legislating regulations that cannot be enforced properly just to gain political points. We need to have a plan, not to respond to threat, but to mitigate them and eradicate them through a new system that is less vulnerable. In the future, we will need to be much more agile, and that's our biggest challenge.

1. Available at: https://thispersondoesnotexist.com/
2. Available at: https://deeptracelabs.com/mapping-the-deepfake-landscape/
3. Available at: https://www.stern.nyu.edu/experience-stern/faculty-research/disinformation-and-2020-election-how-social-media-industry-should-prepare
4. Available at: https://www.darpa.mil/program/media-forensics

WEBINAR

Key takeaways: Cookies and the German approach

On 26 November 2019, OneTrust DataGuidance hosted a webinar covering important decisions, developments, and the salient points regarding organisations' utilisation of cookies in Germany and their compliance obligations. Particular topics discussed include recent guidance from data protection authorities in Germany and across Europe and the changing legal landscape pre- and post-General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').

Changes to the legal framework on cookie-rules

While under the Section 15(3)(1) of the Telemedia Act 2007 ('TMG') and former jurisprudence, implied consent with an option to opt-out was considered sufficient for the use of cookies, the German Federal Data Protection Conference ('DSK') now takes the position that the GDPR is directly applicable instead of the TMG. In particular, it states that cookie practices must be based on explicit consent, a contract or legitimate interests (Articles 6(1)(a), (b) and (f) of the GDPR). However, the speakers note that the exact scope of the legal bases remains unclear in the cookie-context and the ePrivacy Regulation, which was expected to be adopted in 2020, would bring more certainty on the matter.

Requirements for cookies

According to the DSK Cookie Guidance and the CJEU Planet49 Decision, pre-ticked checkboxes on websites do not constitute explicit consent to cookies and website providers must inform website visitors about the life span of cookies and access by third parties. Moreover, continued browsing is no longer considered valid. In addition, data processing requiring consent is only allowed to take place after consent has been obtained.

It may be argued that, functional and essential cookies may be used without consent, based on legitimate interests (Article 6(1)(f) of the GDPR), in particular in the light of Recital 47 of the GDPR, providing that direct marketing could be considered to be a legitimate interest. Whether this basis also covers analytic and marketing cookies remains unclear. Businesses should document their legitimate interest and the legitimate interest assessment in detail, particularly if cookies are used on a large scale.

Cookie banners

The DSK Guidance states that cookie banners are only required if consent is required, thus excluding the category of strictly functional cookies. It is not sufficient if the website provider only provides information on the setting of cookies, together with and “OK” button. Cookie banners should include a selection menu with the names of the parties involved and cookie functions. Moreover, the DSK Cookie Guidance states that information on the possibility to withdraw consent is required and that visiting a website must also be possible if cookies are rejected by the user. The webinar also contains a summary on a study analysing the best positions and techniques to increase website users’ engagement with cookie banners.

Third party content and Google Analytics

On 14 November 2019, seven German DPAs issued statements regarding third party content and tracking mechanisms. In particular, they agree that consent is also required for the integration of third-party services whose providers use personal data for their own purposes. In this regard, they state that Google Analytics has been developed in recent years in such a way that it no longer constitutes an order processing tool but now uses the collected data for its own purposes. In this case, specific consent has to be sought and cookie banner and pre-filled checkboxes do not constitute sufficient consent. The DPAs announced that they will start targeted website inspections and called upon data controllers to immediately check their websites for third party content and tracking mechanisms to avoid fines.

Consequences of non-compliance and GDPR fine calculation

Consequences of non-compliance with data protection law can take the form of criminal sanctions to administrative orders to comply or stop processing, and cease-and desist injunctions. Moreover, data subjects may claim for material and immaterial damages under Article 82 of the GDPR and increasingly make use of it.

On 16 October 2019, the DSK issued a new GDPR fine calculation model based on four different sections: light, medium, severe and very severe. DPAs must be expected to use this fine calculation model in the future, although it is likely that it will be reviewed by the German courts. German courts are not bound by this calculation and may issue higher or lower fines.

A European view of cookies

The UK's Information Commissioner’s Office ('ICO'), the French data protection authority ('CNIL'), and the Spanish data protection authority ('AEPD') have all issued guidance on the use of cookies. In particular, the ICO has noted that cookie banners should not 'nudge' users towards consent. Moreover, CNIL'' guidance notes that global opt-in is permissible, as long as users are offered the option to specifically opt-in for each purpose.

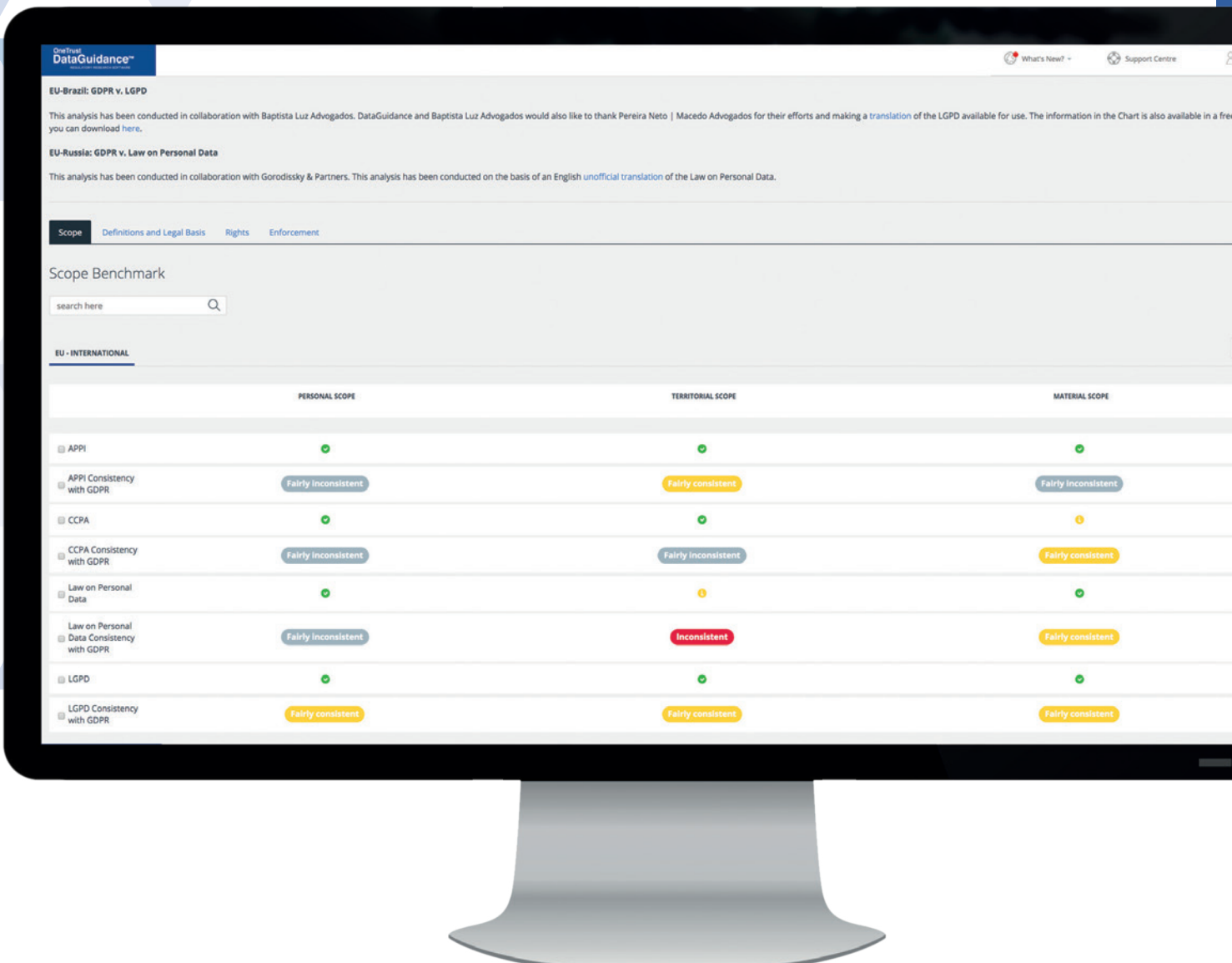
OneTrust DataGuidance™

REGULATORY RESEARCH SOFTWARE

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers
Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk
and achieve global compliance.

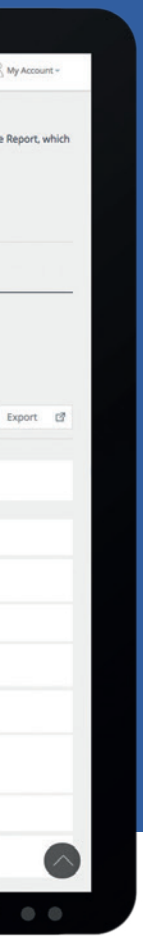


Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan

Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe.

The GDPR Benchmarking tool provides a comparison of the various pieces of legislation on the following key provisions.



- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

Start your **free trial** today at **dataguidance.com**

Privacy Talks

Michelle Griffey is the Chief Risk Officer at Communisis. OneTrust DataGuidance spoke with Michelle regarding the key controls she implements in order to protect customer privacy, third party risk mitigation, and the future of managing risk around communications.

Customer privacy

This is absolutely key and critical, and a lot of the things we do relate to the individual on the street and what they are doing day in, day out. So, your bank statement, maybe a tax return, or something of that nature, that is key. If you then go into the marketing world, historically, it might be a, 'Dear Mrs. so-and-so,' or something coming through the door, and people were not really that interested in whether it mattered if something was slightly wrong. I think that focus has become much more prominent now, and everybody wants to make sure that nobody is getting their information.

We might do something online and we might go on social media and put lots of things out like that, however, in our world that is coming into us, we very much feel that somebody should not invade our privacy and should not take that information or give it to someone else. So, reconciliation in our world is around making sure that if we have had one hundred documents in, one hundred letters that our client wants to send to individuals, we know that one hundred letters have gone out and they have all gone to the right individual. That is one of the key controls that we have to make sure happens. We have got lots and lots of other controls across our organisation, and here we are probably talking more the big printed things, perhaps stuff going out on digital as well. So, we send an email out, and again, it is critical because once you have pressed that button on the email, it is gone. You may have a chance of getting it back if you put it in the post, but once it is gone into email, you can not.

Again, you have just got to make sure at all times in your process that you are checking that what you have got coming in, and what you are sending out to individuals, is right and that you are testing that and it is all happening in the way that it should.

Third party risk

Our clients are asking more of us because of regulation and because they need their supply chain to be safe and secure and to do what it needs. Now that extends out from us all the way down our supply chain. So, our clients that come to us are asking us to do more, to check more, but also to make sure our supply chain is as secure as we are. So, we are trying to ask our clients not to just do a tick box exercise, because it does not help anyone, and we actually try and prove back to them that we are doing the right thing. We are trying to amalgamate things, and if one client needs to see evidence of whatever policy it is they need to see, why can we not put that all in one place for several clients to see, because it is the same thing, or audit at the same time. But, we also flow our processes down our supply chain, so we want to make sure that people are looking after data in our supply chain as securely as we would expect them to. I think there is a general misconception that actually your supply chain, maybe a license for software or a piece of paper you are buying or whatever it is, is not a part of your business and therefore does that privacy matter. But I think where it starts to come into focus in the trends we are seeing is that, actually, this is more about if something happens that is a bad thing down there. For example, maybe one of our suppliers gets compromised, you have got to have in place the right processes. So, you need to ensure that it feeds back up and they say to you immediately, 'we have got an issue,' and then you can say 'let's work together on solving this so that it does not flow all the way back up that supply chain.' Therefore, we keep everyone safe and secure all the way through.

Risk management

I think that there has always been a traditional view that risk sits in the centre, and it is very ivory towered. You sit there and you say to people, 'this is what you have got to do.' And, generally, risk, data protection, information security, all of those disciplines historically do not actually go and engage with people, they do not really understand that you tend to mandate what is going to happen through policy generally, and no one wants to read hundreds and hundreds of policies, particularly if you have got to do your work.

So, what we have tried to do is bring those different disciplines together and almost cross fertilize the ideas, and what you do when you do that is you start to see the overlaps almost like it is a Venn diagram. So, you start to see those overlaps and you start to challenge each other within the team, but also go out and you do not put so much pressure on the wider teams. You will go out with three or four key messages, but through one person, rather than hitting them several times. And we bring people in and try and make it real. So, anything that we are doing is also related to us, we are the person on the street, we are the people that need to be kept private or helped, we try and make these things come to life really. So, it could be somebody's mortgage it could be your mortgage that we're mucking up with somebody else's potentially, if you are doing something wrong. And by doing that, people start to understand it is not just an email going out, it is not just a piece of paper, it is something that means something to somebody.

We believe fully that people probably are your greatest risk, but also your greatest protection. If people do not know what they need to do, how are they ever going to get it right. You cannot expect someone to get it right without knowing what they need to do, but also they will spot things. So, the more we put out just little snippets of information, for example, on phishing emails, that is really helpful at home, but also people start to spot things and they get quite proud of going, 'I found this,' or 'I have seen this,' and reporting it, and so you can stop things. But also, probably more mundane, is just explaining why the controls are there. Sometimes it might feel that actually checking this document, or checking this and that, is time consuming, do people really want to do it, but actually, if we know it is there to protect something at the end of it, the end person, then I think people start to add value to that.

Future of risk

I think it will continue to become more and more regulated on one hand, because you have got different types of communications on the marketing front. People have got, and do get, very fed up with seeing more and more that they do not want. But I think people start to also get fed up with seeing more and more of what they have actually had before because of all the algorithms that are saying, 'if you have been interested in that, then you must be interested in more of that moving down the line.' So, I think communications from our clients perspective on a marketing front are going to have to become much more understood in terms of what the customer wants.

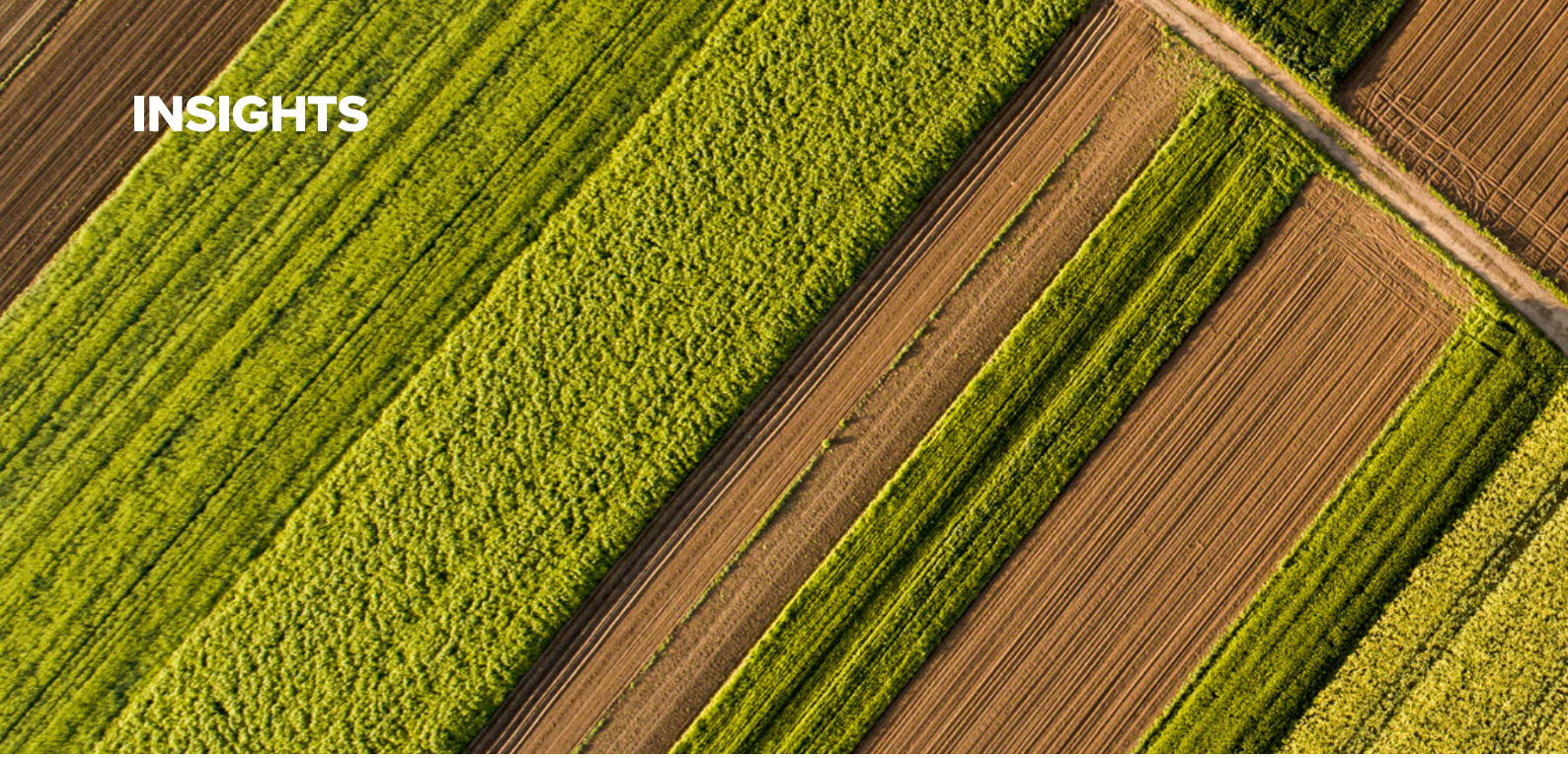
On a transactional front, the regulators want people to get the right documents at the right time and it has all got to be correct. It becomes much more difficult to navigate and I think the other thing is making sure that people get things in the right way, at the right time. And if more and more people, or channels, are opening up, and print is not going away, if you can send out something it has got to be right. So, it is going to be squeezed at both ends, I think.

Michelle Griffey
Chief Risk Officer
at Communisis

Michelle's interview was filmed as part of OneTrust DataGuidance's 'Privacy In Motion' series which covers topics and industries including Brexit, the financial sector and emerging technologies.

*Why not try **OneTrust DataGuidance Privacy Core® Awareness Training** which offers more than 30 specialized, role-based courses to drive a privacy first culture in your organisation.*

For more information, visit onetrust.com/privacy-core



Kenya: Overview of the Data Protection Act, 2019

On 8 November 2019, President Uhuru Kenyatta signed the Data Protection Bill, 2019 into law ('the Act'), establishing requirements for the protection of personal data. The Act is Kenya's first data protection law, which came into force on 25 November 2019. Francis Monyango, Law and Policy Associate at Kenya ICT Action Network (KICTANet), provides an overview of the privacy law and discusses the conditions set out regarding data transfers, data processing, and data subject rights.

Short overview of the right to privacy in Kenya

The Act was preceded by the Privacy and Data Protection Policy 2018. The Act gives effect to Article 31(c) and (d) of the Constitution of Kenya, 2010 which enshrines the right to privacy.

Despite a lack of data protection law, Kenyans with grievances have not hesitated to use judicial means to get declarations on what they felt were breaches of their right to privacy.

Outside the corridors of justice, privacy concerns among Kenyans include the arbitrary use and misuse of personal information, unsolicited marketing messages by entities, and the need for identification at entrances of buildings.

Business entities, on the other hand, have been concerned about how they can comply with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). The Act borrows heavily from the GDPR, something that eases the compliance burden.

Overview of the text of the Act

The Act's objectives and scope are to regulate the processing of personal data and to ensure that the processing of personal data is guided by the legislated data protection principles. Other objectives are to protect the privacy of individuals and to establish the legal and institutional mechanism to protect personal data by providing data subjects with rights and remedies.

The Act establishes the Data Protection Commissioner ('the Commissioner'). The role of the Commissioner will be to oversee the implementation and the enforcement of the Act. The other role will be to establish and maintain a register of all the data controllers and data processors in Kenya. This seems to be inspired by the UK's Data Protection (Charges and Information) Regulations 2018, which require every organisation or sole trader that controls the processing of personal data to register with the Information Commissioner's Office ('ICO'), unless all the processing they carry out is exempt. While Kenyan data processors and data controllers will be required to register, in the UK only data controllers register with the ICO. This also means that no person is allowed to act as a data controller or data processor unless they have registered with the Commissioner. The Commissioner is expected to prescribe thresholds required for mandatory registration of data controllers and data processors.

The Commissioner will also be able to exercise oversight over all data processing operations in the country, promote self-regulation among data controllers and data processors, and to conduct data processing assessments on its own initiative or upon request. The Commissioner will also be expected to promote international cooperation in data protection issues while ensuring

that Kenya complies with data protection obligations under international conventions and agreements.

The Act contains data protection principles that require data processing to be lawful, fair, and transparent. Data collection should be for a specified and legitimate purpose, relevant, and limited to what is necessary. Data should not be kept for longer than is necessary. It should also not be transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

The rights of a data subject are also stated in Section 26 of the Act. A data subject has the right to be informed of the use of their personal data, the right to access their personal data, the right to object to the processing of all or part of their personal data, and the right to correct and even delete false data about them. The recurring message in Sections 26, 27, 29, and 30 of the Act is the need for informed consent before data processing. A data subject will have to be informed that their data is being collected, the purpose for which the data is being collected, and the third parties which the personal data has been or will be transferred to, including details of safeguards adopted before they consent to data processing. The Act also empowers the data subject to request a stop to or a restriction of the data processing.

Regarding children's data, parental consent is required and the processing should be in the best interest of the child. In terms of automated individual decision making, the Act states that every data subject has the right not to be subject to a decision based solely on automated processing where the decision produces legal effects that affect the data subject. The Act stipulates that processing for direct marketing may not be done unless the data processor or data controller has express consent from a data subject, or is authorised under any other law which the data subject has been informed of. The Act also empowers a data subject to receive, upon request, personal data concerning them in a structured, commonly used, and machine-readable format. The data subject has the right to transmit this data to another data controller or data processor without any hindrance.

Just like the GDPR, the Act has provisions that require the data processor and data controller to practice Privacy by Design. Data processors and data controllers will have to implement technical and organisational measures which will have all the necessary data processing safeguards. Data Protection Impact Assessments ('DPIAs') are also made mandatory prior to commencement of data processing activities. DPIAs should enable entities that process data to determine organisational measures, such as ensuring all those who act under the authority of the data controller or processor, comply with the relevant security measures.

In the event of a data breach, the Act requires a data controller to notify the Commissioner within 72 hours of becoming aware of such a breach. Upon the occurrence of a data breach, the data controller is also required to communicate to the data subject, in writing, within a reasonably practical period. Processing of sensitive personal data is permitted after consent is granted by the data subject and there are appropriate safeguards. Personal data relating to health may be processed under the responsibility of a healthcare provider.

The Act sets the conditions for the transfer of data out of Kenya. The transfer is allowed where the data controller or data processor has given proof to the Commissioner that the destination jurisdiction has similar data protection laws and that the transfer is necessary. Despite all the restrictions on data processing, the Act has exemptions. Some of the exemptions are based on national security, journalism, literature and art, research, history, and statistics. The Commissioner may legislate more exemptions. Other than dealing with complaints, the Commissioner is also empowered to issue enforcement notices, penalty notices, and administrative fines. The Act provides compensation for the data subject in the event that their privacy rights are breached.

The enactment of the Act is a step in the right direction and it provides Kenyans with legal recourse for privacy violations. However, it is too early to draw any final conclusions about its impact as the Act has not yet been implemented.

Francis Monyango Law and Policy Associate

monyango93@gmail.com

Kenya ICT Action Network (KICTANet), Nairobi

Key differences between the 2018 and 2019 Indian personal data protection bill

In July 2018, the Committee of Experts on Data Protection submitted a draft Personal Data Protection Bill, 2018 to the Government of India. On the basis of recommendations made by the Committee, and suggestions from various stakeholders, on 11 December 2019, the revised Personal Data Protection Bill, 2019 was introduced to the lower house of the Indian Parliament, Lok Sabha.

Definition of personal data and sensitive data

- Section 3(28) of the 2019 Bill expands the definition of 'personal data' to include a reference to online or offline characteristics, traits, attributes or any other feature of the identity of a natural person, as well as 'any inference drawn from such data for the purpose of profiling'.
- The 2019 Bill excludes passwords from the definition of sensitive data.

Right to erasure

- The 2018 Bill and the 2019 Bill both include a right to be forgotten i.e. data subjects can restrict or prevent the continuing disclosure of their personal data, section 27 and Section 20 respectively.
- In addition to this, Section 18 of the 2019 Bill includes a right to erasure for data subjects with regards to personal data which is no longer necessary for the purpose for which it was processed.

Reasonable purposes for processing

- Section 14(2)(h) of the 2019 Bill includes the 'operation of search engines' as a possible reasonable purpose to process personal data without obtaining consent from the data subject.
- The 2018 Bill does not include this provision.

Data localisation and transfer requirements

- Section 40 of the 2018 Bill required data fiduciaries i.e. data controllers, to store a copy of all personal data on a server or data centre located in India.
- Section 33(1) of the 2019 Bill limits this requirement to sensitive personal data.
- Section 34 of the 2019 Bill introduces a mandatory requirement to obtain consent from the data subject for cross-border transfer of sensitive personal data, which was not present in the 2018 Bill.

Social media intermediaries ('SMIs')

- Section 30 of the 2019 Bill lays down norms for SMIs. An intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.
- The 2019 Bill notes that SMIs who have users above a certain threshold and whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order, or the sovereignty and integrity of India would be classified as 'significant data fiduciaries', and would be subject to the obligations under Sections 27-30 of the 2019 Bill.

- Section 93(1)(d) of the 2019 Bill outlines that the Central Government may make rules for the methods of voluntary identification to identify users of social media.
- The 2018 Bill does not contain any reference to SMIs.

Anonymised data

- Section 91(2) of the 2019 Bill introduces powers for the Central Government, in consultation with the DPA, to direct any data fiduciary or data processor to provide any anonymised personal data, or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government.
- The 2018 Bill does not contain any similar provision.

Data Protection Authority selection committee

- The 2018 Bill and the 2019 Bill state that the chairperson and members of the DPA shall be appointed by the Central Government on the recommendation of a selection committee, (Sections 50(2) and 42(2) respectively).
- The 2018 Bill's selection committee consisted of the Chief Justice of India or a Supreme Court judge as the chairperson of the committee, the Cabinet Secretary, and an expert nominated by the Chief Justice or Supreme Court judge.
- The 2019 Bill's selection committee is composed of the Cabinet Secretary as the chairperson, and the Secretaries to the Government in the Ministry/Departments dealing with legal affairs, and electronics and IT.

Exemption of government agencies

- Section 35 of the 2019 Bill introduces a power for the Central Government to exempt any government agency from the application of all or any provisions of the Bill with respect to processing personal data, and for preventing incitement to the commission of any cognisable offence relating to the sovereignty and integrity of India.
- The 2018 Bill does not contain this provision.

Penalties

- The 2018 Bill included imprisonment penalties for three instances (Sections 90-92 of the 2018 Bill):

- Data fiduciaries who violate the provisions on obtaining, transferring, or selling personal data;
- Data fiduciaries who violate the provisions on obtaining, transferring, or selling sensitive personal data; and
- Re-identification and processing of de-identified personal data.

- Section 82 of the 2019 Bill only imposes a penalty of imprisonment for the offence of re-identifying and processing de-identified personal data.

INTERVIEW

OneTrust DataGuidance spoke with Stevan Stanojevic, Group Data Privacy Manager at Etihad Airways in September 2019. Stevan shares his personal views on the challenges of maintaining an effective privacy program, as well as how to measure and report on the program's performance.

How did you create and implement a global privacy program?

In my experience, when you want to create and implement a privacy program, the first thing is to get a leadership buy in. Once you get leadership buy in, you can think about other steps, such as having your team properly resourced, because if you are a privacy professional sitting within the compliance function, or even legal, you might not have the required project management skills, for instance. That is why you need a team of project or program managers, business analysts, and depending on the size of the project, organisation, and the demand for business, you might need to consider a few more privacy advisors. Once you have that in place, you can proceed further, and you should conduct a gap analysis. When it comes to the gap analysis, it really depends on your organisation, what are your operations, and in which countries you are operating in.

If we look at an organisation with a global footprint, they will need to consider all of the legislation and whether they apply or not, whether you are established in those countries, whether you process personal data for individuals, residents, or citizens. Once you know what you have to deal with in terms of legal requirements, you need to develop a central register of processing activities, internal policies and procedures, publish privacy notices, consider notification requirements and notifying regulators about the identity of your data protection officer representative in that country, the localisation requirements and if you need to notify a regulator if you are exporting data or if you need permission for that. Of course, in the case of a data breach, you would have to notify regulators of that as well.

If you are doing some marketing activities, such as sending emails, calls, SMS, and similar things, you want to have a proper understanding of what the requirements are in those countries, such as having appropriate consent for instance in certain jurisdictions. You need to ensure that you have a proper cross-organisational collaboration, which means you need to have on board your information security, legal corporate affairs, insurance departments, human resources, marketing, IT, and other departments involved in processing personal data.

Often people tend to forget how they should manage vendors, so when you select a vendor, you need to assess your relationship properly. You need to understand whether they are your processors, or whether there is a controller-controller relationship. Based on that, you have to enter into appropriate agreements.

Privacy by Design is required by some of the laws. Companies should really think about how they can embed privacy within their processors. It can be done through Privacy Impact Assessments, in which you can assess risks and work with businesses in order to implement action plans so as to mitigate those risks successfully.

Also, whenever doing a privacy program, it should always be assessed what the risk of a processing activity is, against what the cost of the implementation of a certain technology, because if there is not a risk, you do not need to employ the most sophisticated piece of technology you can find on the market.

What are the challenges in maintaining a privacy program?

When trying to be compliant with multiple jurisdictions, you have to consider what the requirements in each jurisdiction are first. If they are similar to each other, then it is an easy job, and you can have a certain standard and apply that across the organisation. However, if the requirements in some jurisdictions are different, then you have to consider if you are going to apply a higher standard, even in those jurisdictions which do not require it, or you are going to have a different approach when processing personal data or people in certain countries.

I think if you go down the second route and you decide to have a differential approach, then you might face challenges such as having appropriate procedures in place because you need to explain your actions. How are you going to apply certain laws on certain occasions in certain jurisdictions? You have to also find a way to segregate that data successfully which is a challenge. Finally, it will require more resources when it comes to privacy, so you need to strengthen the team by having fresh people to help you carry on with that activity.

How do you measure and report on the program's performance?

A privacy program is similar to any other program or project. Once you have developed your strategy, you need to consider what are your milestones. If you are hitting them, it means you are staying on track, however if you are missing

"When trying to be compliant with multiple jurisdictions, you have to consider what the requirements in each jurisdiction are first."

those milestones, you will need to revisit what went wrong. Sometimes this is a case of dependency on some other project that is running independently, because let's say when you were starting your project there was a certain IT system in your company, in the meantime the system got replaced, now you have to deal with that change so you might miss some of your milestones. You can use milestones to see whether a project is running in a timely manner or not.

Then, the budget is another thing to consider. When running a program, it is assumed that nobody has an unlimited budget. If you are staying within the budget, it means that you are doing well. If you are exceeding the budget, then you have to revisit your program and you have to justify why you are going above the agreed budget scope.

The views and opinions expressed in this interview are those of the Author's and do not necessarily represent the official Policy or Position of the Author's company.

Mexico: Comparing GDPR and CCPA with Mexican data protection law

The Federal Law on the Protection of Personal Data Held by Private Parties 2010 ('the Data Protection Law') and the Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties 2011, were seen as modern data privacy laws when they were first published. With recent privacy legislation, such as the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the California Consumer Privacy Act of 2018 ('CCPA'), alongside the development of new technologies, it is possible that the Data Protection Law may require an update. Daniel Villanueva and Karla Guerrero, from Baker McKenzie, compare and contrast the GDPR and the CCPA with the Data Protection Law.

The Data Protection Law included most of the best practices found in European and North American regulations, including many of the standards in the Madrid Resolution: International Standard on the Protection of Personal Data and Privacy ('the Madrid Resolution'). In a way, the Data Protection Law served as a reference for other countries in Latin America, and different rules have been published in order to complement the Data Protection Law and to follow international correlative laws, directives, and statutes, such as the Guidelines on Privacy Notices 2013 and the Parameters of Self-Regulation Regarding the Protection of Personal Data 2014, among others. It is important to state that the principles and provisions in this large regulatory framework has permitted Mexico to share similar principles, regulatory scope, and provisions with international frameworks.

The Data Protection Directive 95/46/EC, issued by the European Parliament and the Council of the European Union in 1995, and the Madrid Resolution in 2009, inspired the creation of the Data Protection Law. From its publication, the Data Protection Law has always considered the legality, consent, quality, purpose limitation, proportionality, loyalty, transparency, and accountability principles. Further, it establishes an obligation on data controllers to implement appropriate administrative, technical, and physical security measures to protect personal data against unauthorised damage, loss, modification, destruction, access, and/or processing.

It also recognises data subject rights to access, rectification, cancellation, and opposition ('ARCO rights'), in which a data subject is entitled to:

- access their personal data;
- rectify their personal data when it is inaccurate or incomplete;
- cancel their personal data if they do not fall under the clear exceptions stated; and
- oppose, with legal cause, the processing of their data.

Data subjects also have the right to withdraw their consent, completely or in part, and to opt out of receiving marketing communications. The Data Protection Law also establishes rules for national and international data transfers, self-regulatory frameworks, and different proceedings before the National Institute for

Transparency, Access to Information and Personal Data Protection ('INAI').

Mexico has been on its way to establish itself as a strong defender of the protection of personal information and, in 2018, Mexico joined the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108'), which may help Mexico to be recognised as a country offering an adequate level of protection.

When the GDPR came into play, it gave rise to much discussion and controversy in Mexico. At first it was not clear whether companies and individuals in Mexico were obliged to abide by the GDPR, but it was clear that in order to comply with its provisions, companies would require additional investment. Large companies would have to invest time, money, and effort, while smaller businesses and startup companies would probably not have enough financial resources to comply. Nonetheless, the Data Protection Law is similar to the GDPR in some parts, for example the accountability principle and the Data Protection Impact Assessment, for which Mexico has a similar procedure. Also, the GDPR and the Data Protection Law both share the notion of self-regulation. In this regard, in 2013 and 2014, INAI issued its Guide on Self-Regulation Regarding Personal Data Protection.

Nonetheless, there are also clear differences between the regulatory bodies, such as the right to erasure (right to be forgotten), which permits the data subject to obtain from the controller the erasure of personal data when legitimate grounds apply. While the Data Protection Law at the time that it was issued did not consider the right to be forgotten, certain principles and provisions might be adapted in order to provide the same protection to data subjects. In general, while the GDPR might be more pragmatic and broader in its definitions and applicability, the Data Protection Law shares many similar obligations within its catalogue.

The CCPA, on the other hand, was created in order to enhance privacy and consumer protection rights of residents of California in the United States and was published in 2018 and came into force on 1 January 2020. Similarly to the Data Protection Law and the GDPR, the CCPA's main focus is to provide individual rights to data subjects, such as the right to know what personal data is being collected about them, the transfers that are made with their personal data, and the ability to oppose certain processing, as well as the right to the deletion of the data. While the general purpose is quite similar between the GDPR, the Data Protection Law, and the CCPA, there are key differences between each of them, such as the territorial scope, definitions, levels of specificity, opt-out rights, and sales of personal information, among others.

For example, the Data Protection Law identifies the right to rectification in Article 24 and Article 103 as the right to request the rectification or correction of personal data that is inaccurate or incomplete. However, the CPPA does not include such a right. Also, the CPPA identifies the right to data portability, which states that the information provided electronically shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. In this regard, while both the GDPR and CCPA have recognised this right, the Data Protection Law has not, probably because at the time it was written, data portability was not an issue as it is today.

Every new legal instrument that comes into force, regardless of where, will include certain rights or legal figures that were not considered in previous regulations due to the ever-changing technology and environment. The demand for the GDPR and the CPPA proved that privacy regulation was needed in order to contend with increasing technological changes and their impact on human rights. However, in taking a closer look at certain regulations, principles can be identified that could apply to this new technological environment. It may be more advisable to adapt a broad interpretation of principles already stated in legal instruments that are in force, than to publish new ones that could be considered obsolete after just a few years.

It is important, when it comes to data protection, privacy, and similar rights, to be aware of new key elements that might be a hindrance to such rights and, if considered necessary, to issue effective tools in order to provide enough protection to data subjects. This can be accomplished by taking into account already established principles.

Today the Data Protection Law has enough legal ground to comply with most of the provisions stated in new international legal instruments such as the CCPA and the GDPR, however, there is definitely room for improvement.

Daniel Villanueva Associate

daniel.villanueva-plasencia@bakermckenzie.com

Karla Guerrero Associate

karla.guerrero@bakermckenzie.com

Baker McKenzie, Guadalajara

UK: Data trusts and the data economy

Data trusts are a relatively new idea in the data world. They combine governance and stewardship to increase trust when sharing personal data. Jamal Ahmed, Director at Kazient Privacy Experts, provides an overview of what a data trust is and how companies may benefit from their use.

Typically, trusts are a way of managing assets such as investments, land, and money by holding these assets and making decisions on them. Data trusts work in the same way, but instead of a tangible asset, data is used. Trusts are a legal concept which provide independent regulation on the way data is used and stored. In this current climate of leaks and data breaches, could independent data trusts be the answer to better outcomes for clients and businesses?

Research has stated that in the UK, 44% of consumers would hesitate to do business with a company for a few months if they had suffered a data breach, and 41% of customers would never return to the business[1]. If companies are serious about keeping clients' data and business, then a data trust, where the data is used responsibly and safely held, could be mutually beneficial. This is because data trusts encourage individuals to become trustees of these trusts to make decisions about, and have a say in, what happens to their data.

The Centre for Data Ethics and Innovation, and the Competition and Markets Authority, are completing further research on how data trusts can be used in a commercial setting to help both consumers and businesses make informative choices on data protection. Information is collected by organisations on current and potential customers to increase revenue by knowing what consumers actually want from a business. This goes beyond simply keeping data for the purpose of a single transaction. On the one hand, it may make many customers feel uneasy that they do not know how or why their data is being used, or, knowing their data is being used for purely monetary gains which they may not have a say in. On the other hand, data trusts can let customers decide what they feel is appropriate for their personal information, with customers helping to regulate trusts from within.

The value of data to the UK economy is increasing in this technological era. In simple terms, data equals money. The more data you can extract from someone, the more targeted and personal you can make adverts and sales pitches, and companies may often sell this data to third parties to increase

Jamal Ahmed FIP Director
jamal@kazient.co.uk
Kazient Privacy Experts, London

their revenue. From a company's point of view, gaining data means business growth and increased value. However, from a consumer point of view, although targeted adverts and deals may prove useful, the selling and profiting off of personal information is a thought which unsettles many. Data trusts can therefore make these processes more transparent and enable businesses and customers to work together.

Along with data trusts, another new technological innovation in recent years has been artificial intelligence ('AI'). AI is used to examine data and quickly create patterns and filter it into data sets. With the growth of data trusts, AI developers could use this new information for a common interest or shared belief, and to help people make informed choices. Using data trusts, where relevant data is all in one place, could streamline processes for AI innovators when developing solutions for the world's problems. In 2018, the Secretary of State for Health and Social Care spoke of the importance of using AI, and compiling AI with National Health Service data could save lives. The benefits of AI developers working with data trusts may be the good publicity that the data world needs, showing consumers the wider gains that can be made from sharing data.

In reality however, how practical will businesses find using data trusts? Would they be willing to give up their data to a trust when they know how valuable data is and how important it is to the economy? Large companies, which have the financial proficiency, business knowledge, and a vast consumer spread, would be able to offset any immediate pitfalls of using a data trust. The repercussions of not using one may not show immediately, but it could cost businesses more in lost consumers than it would in time or resources to initially set up with a data trust. For large businesses, using a data trust is completely practical, and smaller companies need to weigh up short term efforts to work with data trusts for long-term gains, which may enable a bigger customer base and an increase in returning consumers.

Keep up to date with enforcement and breach news through the OneTrust DataGuidance 'Enforcement and Breach Tracker' which now includes a downloadable version of the ***'Global Privacy Enforcement: Highlights and Trends' summary report.***

1. Available at: https://www.pcipal.com/en/knowledge-centre/news/it-toolbox-feature-pci-pal-survey-examines-data-breach-repercussions-for-organizations/

News in Brief

California: CCPA entry into force brings "significant impact on future state and federal legislation"

The California Consumer Privacy Act of 2018 ('CCPA') entered into effect on 1 January 2020. In particular, the CCPA provides certain rights to consumers, such as the rights of access and portability, to deletion, to opt-out, and to seek relief for breaches that involved their personal information. It was signed into law on 28 June 2018, after efforts by Alastair MacTaggart who was the main supporter of the ballot initiative which then led the CCPA to be passed unanimously by both houses of the California State Legislature. In addition, the CCPA was further amended in October 2019 by various bills which corrected technical details and implemented certain exemptions. The CCPA will be enforced by the California Attorney General ('AG') who will be able to bring civil actions for alleged violations.

"Without the final regulations companies continue to be in limbo [...] "

Lisa J. Sotto, Partner at Hunton Andrews Kurth told OneTrust DataGuidance that, "There is no question that the CCPA will have a significant impact on future state and federal legislation. The CCPA has set the bar. While future laws might deviate from the CCPA, every provision of the law will be debated and considered in any new U.S. privacy legislation. Companies in the U.S. have spent months preparing for the January 1st compliance deadline. There is a rush to the finish and a number of the behind-the-scenes compliance processes will continue to be refined over the next few months. But there is a serious and earnest effort by most companies to comply." Alongside the CCPA, the AG has also released draft Regulations ('the Regulations) which are to aid with the interpretation and implementation of the CCPA. The Regulations provide for clarity on how notice is to be given to consumers when collecting personal information as well as how businesses should handle consumer requests and the verification of said requests. However, this is currently in a draft form with the deadline for comments only recently ending.

Sotto further noted, "We are eagerly awaiting the final regulations. There are portions of the draft regulations that deserve to be reconsidered and rewritten (or dropped entirely). Without the final regulations, companies continue to be in limbo and compliance across U.S. companies will vary depending on whether companies are choosing to comply with the draft regs or just the law [...] We have entered into a new era in privacy in the United States. We have been out of step with the rest of the world in sticking with our sectoral regime and the CCPA brings us one step closer to global alignment."

OneTrust DataGuidance produced, in collaboration, with the Future of Privacy Forum, a report comparing the CCPA with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which was last updated in December 2019 to take into account the bills that amended the CCPA.

Alexander Fetani Privacy Analyst

afetani@onetrust.com

OneTrust DataGuidance

Russia: New fines for violations of localisation requirement "increase risk for companies"

The President of the Russian Federation, Vladimir Putin, signed, on 2 December 2019, Federal Law of 2 December 2019 No. 405-FZ on Amending Certain Legislative Acts of the Russian Federation ('the Law'), which increases the fines for violations of data localisation and processing requirements.

Vyacheslav Khayryuzov, Counsel and Head of Digital Business and Data Privacy at Noerr LLP, told OneTrust DataGuidance, "The authors of the Law believe that non-compliance with the data localisation requirement threatens the safety of Russian citizens and important informational infrastructure, as well as impedes the fight against terrorism. The key take-away would be the increasing risk for companies which are trying to avoid or minimise their efforts in terms of compliance with the data localisation requirement. [In addition, the data protection authority] is expected to run more audits, and now they have a new tool to force the companies to comply."

The Law supplements Article 13.11 of the Code of Administrative Offenses of the Russian Federation with parts 8 and 9, which establish administrative responsibility for the operator's failure to ensure that the personal data of Russian citizens is collected, recorded, systematised, accumulated, stored, updated, changed or extracted using databases located within the territory of the Russian Federation. In particular, a fine of up to RUB 6 million (approx. €85,000) for a first offence, and RUB 18 million (approx. €255,000) for repeat offences may be imposed on a legal entity failing to meet the said requirement.

Khayryuzov continued, "The localisation requirement, which has existed in Russian law since 1 September 2015, can be complied with, for instance, by placing a database with personal data of Russian citizens in a Russia-based data centre or server [that] needs to be 'primary'.

> *"Companies working in Russia are encouraged to revisit the topic of data localisation and to have a closer look at their compliance measures"*

This means that all initial recording and modification of data has to be made to the Russian database first, [while] further mirroring to foreign databases can be made only afterwards. This topic is becoming much more serious [and] therefore companies working in Russia are encouraged to revisit the topic of data localisation and to have a closer look at their compliance measures."

Kotryna Kerpauskaite Privacy Analyst
kkerpauskaite@onetrust.com
OneTrust DataGuidance

Rhineland-Palatinate: Taking pictures without consent permissible when "necessary for the purposes of the legitimate interests"

The Rhineland-Palatinate data protection authority ('LfDI Rhineland-Palatinate') published, on 13 December 2019, its guidance on legal requirements for photography ('the Guidance') under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which aims to reduce uncertainty on the topic at a corporate and private level.

In particular, the LfDI Rhineland-Palatinate highlights that photographs of living people, regardless of whether they are analogue or digital, always contain personal data if the person can be identified under Article 4(1) of the GDPR because the image of a person conveys physical and psychological features, and the taking of pictures, therefore, needs a legal basis as provided under Article 6 of the GDPR.

"Freely given consent can usually be assumed if a legal or economic advantage is achieved for the employee"

Dr. Carlo Piltz, Attorney at Law at reuschlaw Legal Consultants, told OneTrust DataGuidance, "One must note that all legal possibilities to process personal data under Article 6(1) of the GDPR stand equal beside each other. [...] According to the LfDI Rhineland-Palatinate, the production of pictures is also permissible without specific consent pursuant to Article 6(1)(b) of the GDPR, if this is necessary for the performance of a contract. Under certain circumstances, the production of photos may be justified under Article 6(1)(f) of the GDPR. This would be the case if the data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. The reasonable expectations of the person depicted must be taken into account, such as whether he or she must expect to be photographed in a specific situation. Transparency is a very important principle here. Data subjects need to know that pictures are being taken and for what purpose."

Moreover, the Guidance states that specific duties of information and documentation apply in the context of photography and that Article 17(1) of the GDPR lists, among other things, that a picture must be erased when the purpose for which it was taken no longer exists or the person depicted asks for the deletion and no overriding legitimate reasons of the photographer prevail. In addition, the Guidance highlights that particularly on a corporate level, the taking and publishing of pictures is subjected to special rules and restrictions. In particular, Section 26(1) of the Federal Data Protection Act ('BDSG') provides that employee data may only be processed if this is necessary for the employment relationship, which, according to the Guidance, could be the case for positions that are particularly exposed to the public, such as models or TV hosts. However, the Guidance states that in most cases the taking and publication of pictures of employees is not necessary for the fulfilment of an employment contract and the employee's consent is required.

Piltz further noted that, "Freely given consent can usually be assumed if a legal or economic advantage is achieved for the employee or if the employer and the person employed pursue similar interests. In this context, however, the employee must also have a genuine right to choose whether or not to have a picture taken and published. [...]. Thus, good data protection management can distinguish a company as an attractive employer and lead to a competitive advantage, as the LfDI Rhineland-Palatinate said in its own Guidance. [...] For practical reasons, written documentation of consent is advisable. However, it must also be said that Article 24 of the GDPR per se does not prescribe any particular form of documentation. [...] Consent can also be obtained by the employer in an electronic form according to Section 26(2) of the BDSG. It should be noted, however, that in the event of a subsequent change to the purposes of data processing, renewed consent must be obtained."

Lea Busch Privacy Analyst
lbusch@onetrust.com

OneTrust DataGuidance

Announcing OneTrust Cookie Auto-Blocking™

Zero Code Implementations, Same-Day Deployment

- Scan Site for Cookies & Tracking Technology
- Auto-Categorize Cookies
- Customize your Consent Model
- Immediately Block All Cookies
- No Tag Manager Integration Required

Get Started Today

OneTrust.com/CCPA-Compliance/Cookie-Blocking/

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

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

Website: www.dataguidance.com