Volume 1, Issue 4

September 2019

dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

MAKING FACIAL RECOGNITION GDPR-COMPLIANT

Eduardo Ustaran provides insight on how to ensure using facial recognition technology is compatible with the GDPR 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

Sophie Kwasny, Council of Europe
Sophie Kwasny is the Head of the Data Protection Unit of the Council of Europe and is responsible for standard-setting (notably the current modernisation exercise of Convention 108) and policy on data protection and privacy. She is a graduate of the Strasbourg Law University and has been working for the Council of Europe for over 20 years on a variety of topics ranging from prisons' reforms to medical insurance, or from the independence of the judiciary to nationality law.
sophie.kwasny@coe.int

Mark Reynolds, HSBC
Mark Reynolds is Group Head of Data Privacy Advice & Risk Management at HSBC. He is an English qualified lawyer and advocate specialising in privacy, technology and information law with particular expertise in advising clients in the financial services sector, both from an in-house and private practice perspective. His areas of practice include banking, commercial litigation and information technology.
mark.reynolds@hsbc.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

David Hoffman, Intel Corporation
David A. Hoffman is Director of Security Policy and Global Privacy Officer at Intel Corporation, in which capacity he heads the organization that oversees Intel's privacy compliance activities, legal support for privacy and security, and all external privacy/security engagements. He is currently a member of the advisory Board for the Future of Privacy Forum and the Board of the Information Accountability Foundation. David is the co-chair of the International Chamber of Commerce's Task Force on Data Protection and Privacy and is a Senior Lecturing Fellow at the Duke University School of Law.
david.legal.hoffman@intel.com

Image production credits
Cover / page 4 image: Mihai Maxim / Essentials collection / istockphoto.com
Page 6-7 image: MATJAZ SLANIC / Signature collection / istockphoto.com
Page 18 image: phototechno / Essentials collection / istockphoto.com
Page 24 image: metamorworks / Essentials collection / istockphoto.com
Page 30-31 image: patpitchaya/Essentials collection/istockphoto.com
Page 32 image: DmitrySteshenko / envato.elements.com
Page 33 image: McDobbie Hu/Unsplash
Page 34 image: RakicN/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
alexis.kateifides@dataguidance.com

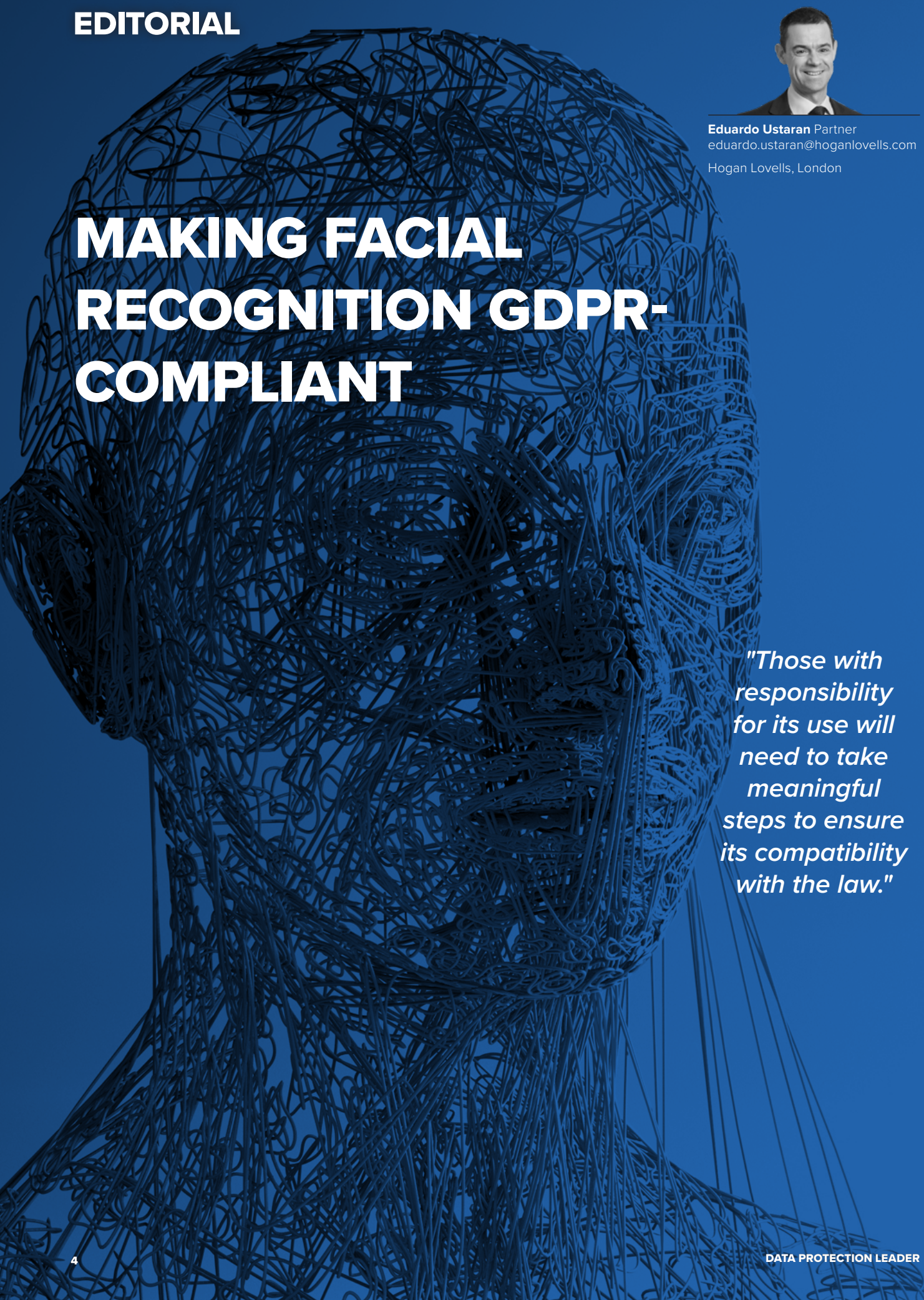
Editorial Assistant Victoria Ashcroft
victoria.ashcroft@dataguidance.com

OneTrust DataGuidance™ Content Team
Lea Busch, Matteo Quartieri, Tooba Kazmi

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

EDITORIAL



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

MAKING FACIAL RECOGNITION GDPR-COMPLIANT

"Those with responsibility for its use will need to take meaningful steps to ensure its compatibility with the law."

Facial recognition is not science fiction. Facial recognition is not next year's big technological wonder (or threat). Facial recognition technology is a reality today and a logical evolution of our infatuation with ever-present cameras and CCTV systems. Like most technological developments, facial recognition can be used for good or evil, but it would be disingenuous to ignore its implications for our privacy. Across the world, attempts to bring facial recognition into the mainstream have been met by public outcry, but whether the deployment of this technology can be lawful is a valid question. In other words, could the use of facial recognition technology ever be compatible with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR')?

To start with the basics, data captured through facial recognition technology that enables organisations to identify specific individuals in a crowd will always be personal data. What complicates things from a GDPR perspective is that the same data qualifies as biometric data used for the purpose of 'uniquely identifying a natural person.' As a result, by its very nature, facial recognition will always attract the application of the tighter regime that applies to special categories of personal data.

This means that under the European data protection framework, the use of facial recognition can only be lawful where at least one of the available legal bases is met, and one of the exemptions to the blanket prohibition affecting the processing of special categories of personal data applies. As with the vast majority of situations where the use of personal data does not involve direct interaction with the individual, the most relevant legal basis to rely on in this context will be the legitimate interest ground. In other words, unless the use of facial recognition is to interact directly with an individual with their knowledge - such as to provide access to premises or enable some sort of action - neither consent, nor contractual necessity, will be suitable legal bases.

In order to rely on the legitimate interest ground, a controller must carefully assess what an individual would reasonably expect at the time of the collection of their personal data. At a more technical level, this involves carrying out a legitimate interests assessment, which will look not only at how necessary the use of facial recognition is to achieve the desired purpose, but also what can possibly be done to minimise the inherent privacy intrusion that this technology involves. Expect regulators to set a reasonably high bar which focuses on the deployment of the whole range of accountability measures envisaged by the GDPR.

Something to bear in mind is that public authorities, such as the police and other law enforcement bodies, cannot rely on the legitimate interest ground at all for any of their data processing. In fact, law enforcement is subject to a different regime altogether under its own data protection directive, which gives the responsibility for establishing the relevant conditions to each Member State. In the UK, for example, police forces seeking to use facial recognition for law enforcement would need to demonstrate the necessity of the technology for the performance of a task carried out for that purpose.

As far as the processing of biometric data as a special category of personal data is concerned, the availability of exceptions to the general prohibition is very limited in practice. In the context of the use of facial recognition as a public safety measure, the only available exception will be the fact that the processing is necessary for reasons of substantial public interest. If the legitimate interests bar is already high, the substantial public interest bar is undoubtedly higher because it must stem from a law that is proportionate, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard individuals' rights.

Looking at how the GDPR applies to facial recognition, it is clear that this technology is very strictly regulated, but it would be wrong to say that its deployment is entirely unlawful. One of the aims of the GDPR is precisely to address the most privacy-sensitive technological developments in a constructive way. Facial recognition is very unlikely to disappear from our devices and cities altogether. Those with responsibility for its use will need to take meaningful steps to ensure its compatibility with the law. Carrying out thorough Data Protection Impact Assessments and ensuring that the voices of data protection officers are truly influential will be essential. Putting into practice the principles of data minimisation and purpose limitation will be equally crucial. Additionally, deploying effective practical measures to achieve the highest possible degree of transparency, storage limitation and data security will be key. Facial recognition is compatible with the GDPR, but focusing on achieving this in practice is as important as ensuring the technology's correct functionality.

OPINION

Gabriel Voisin Partner
gabriel.voisin@twobirds.com
James Fenelon Associate
james.fenelon@twobirds.com
Bird & Bird LLP, London

UK: ICO publishes new Guidance on cookies and similar technologies

On 3 July 2019, the Information Commissioner's Office ('ICO') published its revised Guidance on the use of cookies and similar technologies[1] ('the Guidance'). The Guidance updates the ICO's previous guidance on this topic, in particular to take into account the provisions of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), and organisations are expected to comply with immediate effect. Gabriel Voisin and James Fenelon, of Bird & Bird LLP, provide insight into the key aspects of the Guidance.

Interaction between the GDPR and PECR

In the Guidance, the ICO clarifies that the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') sit alongside the Data Protection Act 2018 and the GDPR. However, where PECR rules apply, they take precedence over the GDPR. According to the ICO, organisations should look at PECR first in relation to cookies and ensure they comply with its consent requirements, before moving on to consider the GDPR.

Specifically, Regulation 6 of PECR requires that users or subscribers consent to cookies being placed or used on their device. As the ICO notes, '[i]f the cookies you set aren't exempt from Regulation 6 [of PECR], then you can only use consent - and this must be of the GDPR standard. This is also the case whether or not personal data is involved.'

Functionally equivalent technologies to cookies are also caught by Regulation 6 of PECR, including pixels, tags, software development kits, and device fingerprinting techniques, among others.

The end of implied consent

The ICO is clear that consent requires some clear and positive action. An 'implied' consent to cookies will not constitute valid consent. In the ICO's view, 'users who fail to engage with the consent box cannot be said to consent to the setting of [...] cookies.'

This is an important change for the many organisations that use implied consent for cookies, and will not be welcomed by companies that rely on online advertising for revenue, given the decrease in acceptance rates that will flow from the change.

Interestingly, the ICO's views on this point are arguably narrower than those taken by the European Data Protection Board ('EDPB') in its Guidance on Consent[2]. According to the EDPB, while merely continuing the ordinary use of a website is not conduct from which one can infer consent, other specific actions, such as swiping a bar on screen, turning a smartphone clockwise, etc., **could** [emphasis added] be action used to signify agreement.

The ICO also reminds organisations of the importance of clear and informed consent. In particular, ambiguous or unclear references to 'partners' or 'third parties' will be invalid. Third parties need to be named.

Don't blame the technology

The Guidance acknowledges that not all cookie consent management platforms ('CMP') on the market enable users to disable third party cookies.

However, it is the website publisher that determines what cookies are set on its website, and employing a tool that technically does not give a user the ability to control all cookies will not be a defence. It is, according to the ICO, the publisher's job to ensure a compliant CMP is therefore in place.

Placing non-essential cookies before the user consents

It can be technically challenging to prevent cookies being placed prior to the user consenting. In its previous pre-GDPR guidance on cookies, the ICO acknowledged these challenges and showed some flexibility on the point. In the post-GDPR world, the ICO has, unsurprisingly, toughened its stance on this issue. According to the Guidance, '[e]nabling a non-essential cookie without the user taking a positive action before it is set on their device does not represent valid consent. By doing this you are taking the choice away from the user.' This principle applies across the board to all non-essential cookies, including

analytics cookies which are routinely set by many publishers prior to the user consenting, as analytic cookies have generally been viewed as low risk.

User interfaces and nudging techniques

A user needs to be given a fair choice between accepting and rejecting cookies.

The ICO warns controllers that user interfaces should not be designed to nudge individuals into non-privacy protective choices. In particular, a consent mechanism that emphasises 'agree' or 'allow' over 'reject' or 'block' would be non-compliant.

The implementation of consent mechanisms should also be carefully considered, having regard to the user experience. For example, while long lists of checkboxes might seem to be offering individuals a high degree of choice, according to the ICO, they risk overwhelming users, leading to poor engagement and consent fatigue.

Lawful basis for processing of personal data obtained via cookies

While consent is always required under PECR for the placing of non-essential cookies, the ICO does not rule out that an alternative lawful basis may apply for the subsequent processing of personal data obtained via cookies.

However, most organisations will want to use cookie-derived data for the purposes of profiling and marketing, and in the ICO's view, in most circumstances, consent is likely to be the most appropriate lawful basis for '[a]nalysing or predicting preferences or behaviour' and 'tracking and profiling for direct marketing and advertising.'

This is broadly in line with the ICO's recent Update report into adtech and real time bidding (20 June 2019)[3], and represents a significant reading down of legitimate interest for the subsequent processing of cookie data.

Cookie walls

According to the ICO, a full cookie wall, i.e., requiring users to 'agree' or 'accept' the setting of cookies before they can access an online service's content, is unlikely to be valid. The ICO, however, acknowledges that partial cookie walls that restrict access to certain content that requires the use of cookies **could** [emphasis added] be valid.

Overall, the ICO's views on cookie walls are less than definitive. While the ICO clearly does not like the idea of cookie walls, the uncertainty in the Guidance reflects the fact that this is a difficult area given the policy considerations, notably the fact that many publishers rely on targeted advertising to monetise otherwise free content.

Use of third party cookies

Where third party cookies are being set, both the website publisher and the third party have a responsibility to obtain consent. The fact the third party does not have a direct relationship with the end-user does not relieve them of the obligation to obtain consent.

According to the Guidance, the third party wanting to set the cookies must place contractual obligations on publishers to ensure the rules in PECR relating to notice and consent are met. However, a contract alone may not suffice, and the third party adtech company may need, in line with previous guidance from the ICO, to take further compliance steps, such as undertaking due diligence that consents are being obtained in practice.

Analytics cookies

Analytics cookies, whether first or third party, are not exempt from the notice and consent requirements under PECR.

In addition, if the information collected via the analytics cookies is passed to third parties, this should be made absolutely clear to users.

Nevertheless, the ICO acknowledges that first party analytics with low levels of intrusiveness and harm to individuals are unlikely to be a regulatory priority for the ICO.

In addition, the Proposal for a Regulation of the European Parliament and of the Council on Privacy and Electronic Communications ('the ePrivacy Regulation') **may** [emphasis added] introduce some further flexibility for analytics technologies, as it is expected that first party cookies used for web audience measurement will be exempt.

Consequences of failure

The ICO makes clear that the enforcement regime for PECR remains what was in effect under the Data Protection Act 1998, i.e., maximum fines of £500,000. However, importantly, this limit only applies to the PECR requirements relating to the placing of cookies. Where personal data derived from the cookie is subsequently processed, the higher fines under the GDPR, up to a maximum of €20 million or 4% of annual worldwide turnover, will apply.

While historically cookies have not been an enforcement focus for the ICO, organisations should not treat this as the benchmark for things to come. Web and cross device-tracking are a regulatory priority for the ICO for 2018-2021.

This article was published in the Opinion section of the OneTrust DataGuidance Platform.

To see more articles like this, request free trial access or sign-in to the OneTrust DataGuidance platform today.

1. Available at: https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf
2. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guideline/consent_en
3. Available at: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

INTERVIEW

MARK REYNOLDS

" One of the great things that the GDPR has done is brought data privacy a lot more into the public awareness. There's clearly a lot of greater media attention and a lot more media focus on data privacy and privacy rights. "

Mark Reynolds is the Head of Data Privacy Advice & Risk Management at HSBC. He is a specialist in privacy, technology and information law, with particular expertise in advising clients in the financial services sector, both from an in-house and private practice perspective.

OneTrust DataGuidance spoke with Mark about the cross-over between data protection and financial regulations, and the impact of investigations in the financial services sector.

What was your experience in working towards compliance with regulations such as Market in Financial Instruments Directive (Directive 2014/65/EU) ('MiFID II'), and subsequently the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR')? Were there any particular challenges or areas of intersection between these regulatory frameworks?
There was an approach from some parts of the industry that said that the requirements that you have in the MiFID II, the requirements you have in the Payment Services Directive ((EU) 2015/2366) ('PSD2'), they are not compatible with the GDPR, and I don't think that's the case. It's true that MiFID II has specific requirements that apply to specific outcomes, same for PSD2, but the GDPR is not a sector-specific piece of legislation, it encompasses everything but it is much more outcomes focussed, and I think it is adaptable to actually meet those outcomes. It's just the fact that as new laws come into place, as new regulations apply, of course you will have those scenarios where you have questions about how do you actually combine the two, where do you come to? There may be difficult questions, but I don't think ultimately privacy legislation is in conflict with those.

What have you seen from the likes of the FCA with regard to investigations into data protection practices? Has the regulator been particularly active in this area?
The Financial Conduct Authority ('FCA') is very interested in this area. I think the FCA really does recognise the fact that data protection is not an island, data protection overlaps with other areas of legislation and other regulatory requirements. So they recognise the fact that the GDPR is a piece of legislation within the UK, your appropriate regulator for that is the Information Commissioner's Office ('ICO'), but at the same point, if you have a data breach that results in you making a notification to the ICO, if you are a regulated firm then you may very well at the same time have other issues, for example system issues, other compliance issues that you would need to report to the FCA. So there is a link between the FCA and the ICO, and the FCA has also issued guidance on its expectations as regards to the GDPR, but again I think we are in a position where we're in, not a honeymoon period, but we are at the beginning of the enforcement of the GDPR. It has not become clear how that may change perhaps positions that have been held, but again certainly, the FCA and other regulators are very interested, and also very keen to make sure that they form part of that larger privacy environment as well.

How far has the financial services sector been impacted by enforcement and penalties? Are there any trends or unique aspects of note?
I think it is too early to say. We have had a handful of public fines issued so far. Obviously one the most public one of that was the Google fine of €50 million but as things stand, I think it is difficult to assess enforcement because we have not built up that back book yet. You have to remember of course under the data protection directive that we pretty much had 20 years' worth of enforcement activity and enforcement action which allows you to build up some trends, bearing in mind that a lot of this is specific to the case in hand, so it can be quite difficult actually, and dangerous at times, to assume that you can rely on a trend. Clearly the potential under the GDPR is that we are going to see larger fines. We may also see more fines because of points like mandatory breach reporting, but I think at this stage it is possibly too early to say.

How do you see the impact of data privacy in the financial services industry developing in the future?
There is definitely an impact in terms of legislation. I think that there is also more of a philosophical shift in terms of data privacy. One of the great things that the GDPR has done is brought data privacy a lot more into the public awareness. There's clearly a lot of greater media attention and a lot more media focus on data privacy and privacy rights. There's also just that shift from perhaps an older school privacy perspective of your data controller, so an organization holding data about you and them controlling, to its being more of a dialogue between the individual and the organization about what that data can be used for, and more of a shift of it going back to an individual's data. I think with things like open banking, with developments in that area, the rights afforded to individuals under the GDPR, I think we are just going to see more of that going forward. I also think technology, and the ability to provide people with insights into their data, access to their data, the potential that you can use multiple sources and multiple providers to actually help you drill down further into your information is going to see a lot more availability of information for individuals, but also in new and interesting ways. I think privacy is an enabler for individuals rather than a blocker, and I also think it's an enabler for organisations as well.

PRIVACY IN MOTION
FINANCIAL

Mark's interview is a part of OneTrust DataGuidance 'Privacy in Motion: Financial' video series.

To compare requirements from 20+ jurisdictions try using the OneTrust DataGuidance Financial Sector Cross-Border Chart.

For Access, request a free trial or sign-in to the OneTrust DataGuidance platform today.

Emerging Tech

Episode 2

Gita Shivarattan Counsel
gita.shivarattan@ashurst.com

Tom Brookes Solicitor
tom.brookes@ashurst.com

Ashurst LLP, London

OneTrust DataGuidance are delighted to partner with Ashurst 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, Counsel at Ashurst LLP, for the second instalment of the series. Gita introduces some of the key issues clients should consider when incorporating artificial intelligence ('AI') technology solutions, such as lawful bases, data minimisation, data subject right's, and Privacy by Design, alongside discussing some uses and applications of AI technologies.

Introduction

AI is emerging in its own right as a nascent industry with the potential to raise the productivity of a diverse range of sectors and create entirely new jobs. PWC estimates that 'AI could contribute up to $15.7 trillion to the global economy in 2030, more than the current output of China and India combined. Of this, $6.6 trillion is likely to come from increase productivity and $9.1 trillion is likely to come from consumption side effects.'[1]

The growth and adoption of this technology is inevitable. As a technology, albeit at an embryonic stage, AI has already proven that when strategically deployed it drives operational efficiencies and can lower costs. For example, chatbots, smart reply and predictive technologies being used as a first response customer service tool and warehouse and distribution analytics for network optimisation.

AI solutions are dependent on access to large and diverse datasets. These datasets are required to shape, train and direct AI towards the required outcomes. It follows that employing these technologies requires an understanding of data licensing, data sharing, and digital trust models, as well as inherent data protection challenges. In the second part of the Emerging Tech Series, we look at AI and related data protection considerations.

What is AI?

AI is a form of computing that allows machines to perform cognitive functions, such as reacting to input, in a similar way to humans. This is different to traditional computing functions, which also react to data, as in traditional computing all the responses are hand coded meaning that there is a finite set of responses, and unexpected inputs cannot be computed. In comparison, current AI enabled technologies are able to modify the response based on an analysis and interpretation of data. This is known as 'machine learning,' the capacity for machines to learn and take independent decisions. Before we delve into the data protection considerations, for context we have set out some AI applications and examples of use cases in which are already present in our everyday lives (see **Figure 1**).

There are other legal challenges around AI which need to be grappled with, including:

- potential discrimination or bias;
- the impact on resourcing and labour markets; or
- antitrust issues.

Each of these important issues requires thoughtful consideration, but they are beyond the scope of this article which focuses exclusively on data protection legal issues and AI.

AI and data protection

Personal data

Data protection laws govern the use of personal data. The definition of personal data can vary by jurisdiction and by statute, therefore ascertaining whether personal data is involved is not a simple task. The line between what is 'personal' and what is not has been blurred by the correlations and inferences that can be made from aggregated data sets. Today, information that once seemed to be non-personal now has the potential to be personal data, particularly where distinct data elements are joined together. The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') defines personal data as:

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

The very nature of AI, including the variety of data sets on which it often depends to expand the capability for linking data or recognising patterns of data that may render non-personal data identifiable, seems to be in constant

Technology Process	Description	Use Case
Data mining	Discovering patterns or extrapolating trends from data	• Anomaly detection, identifying fraudulent entries or transactions; • association rules, detecting supermarket purchasing habits by looking at a shopper's typical shopping basket; and • predictions, predicting a variable from a set of other variables to extrapolate for example a credit score.
Image processing and tagging	Analyse images to get data or to perform transformations	• Identification/image tagging. Algorithms learn facial recognition in photos on social media to unlock smartphones and search images. This leads to the ability to ascertain other data from a visual scan, such as health of an individual or location recognition for geodata; and • optical character recognition. Algorithms learn to read handwritten text and convert documents into digital versions.
Text analysis	Extract information or apply a classification to items of text-based data	• Filtering, used in email exchanges to identify spam; • information extraction, for example to pull out particular pieces of data such as names and addresses; • sentiment analysis to identify the mood of the person writing, as Facebook has recently implemented in relation to postings which are potentially suicidal; and • chatbot technology allowing for interaction on line with customer service messaging services.
3D environment processing	An extension of the image processing and tagging skill where analysis is carried out on images presented in the real world to create spatial and relational images	• The learned skill required by an algorithm in 'Connected and Autonomous' vehicles to understand its location and driving environment; and • free roaming robot devices including pilotless drones.
Speech analysis	Equivalent skills to those used for textual documents and applies them to the spoken word	• Personal digital home assistants from the likes of Amazon's Echo device, Microsoft's Cortana, Google's Home device and Apple's Siri.

Figure 1: Key applications of AI technologies in everyday uses

tension with the challenge of determining when data protection laws apply.

Businesses looking at investing in or developing AI solutions will need to ensure that they are able to clearly define the scope of any personal data that is collected by and processed through the proposed solution. In addition, businesses should consider whether personal data is in fact necessary for the purpose of processing, or if anonymised data sets can achieve the same outcome.

Fairness and transparency

Under Article 5(1)(a) of the GDPR, the processing of personal data must be fair and lawful. Fairness is a fluid concept which is determined through several elements:

- transparency, i.e. that individuals are presented with information about the processing;
- the effect of the processing on individuals, i.e. does the processing determine an outcome; and
- what the expectations of the individuals are regarding how their data is used, i.e. is the intended processing in the 'reasonable expectations' of the individual.

The effect of processing the individual's data should be built into the design and implementation phases of AI solution deployment. At the design phase, datasets and any inferred data should be clearly defined and tested to ascertain any biases created by the algorithm. Often, AI results in a form of profiling or automated decisioning which, subject to the circumstance, can have a more intrusive effect on individuals. An everyday example of this is credit scoring algorithms used to determine credit limits. Credit applicants are likely to be aware that an online application with 'instant credit decisions' will be processed through automated means, however, what they may not be aware of is that the decision to provide credit will be based on their assignment to a 'group' and the factors identified by the analytics, which are common to that group. It is this potential bias or discrimination, which is a result of inferred data, that individuals are often unaware of.

Under Article 22 of the GDPR, individuals have a right not to be subject to decisions carried out purely by automated profiling or decision making. If AI solutions are being relied on to solely determine a decision, that is without human interference, which will have an impact on an individual, under the GDPR the individual has a right to:

- object to the processing;
- request that a human carries out the analysis; and
- request further information about the way the automated decision was arrived at.

From a practical perspective, businesses should review the organisational measures implemented to ensure a request for information about the AI decision process, or a review of the AI decision, is adequately handled. As AI solutions should be a more efficient and accurate method of arriving at a response, businesses should regularly spot check outputs against human decisioning on the same input in order to test whether the outcomes are aligned with a human review, and if any bias has been created through the learned data. This regular review should be built into the governance process for the technology.

The right to be informed and the principle of transparency require that businesses are able to clearly, and using plain language, describe:

- how the personal data is processed;
- any other sources of personal data used in the processing;
- the lawful condition of processing;
- retention periods; and
- the details of any automated decisioning, including a description of the algorithm etc.

In order to effectively discharge this obligation, businesses will need to have fully considered the privacy impact of employing the AI solution.

Lawful basis

In order for processing to be 'lawful' under the GDPR, it will need to satisfy one of the conditions for processing in Article 6 of the GDPR. The most likely conditions to be relevant to processing through AI are:

- consent;
- legitimate interest; or
- performance of a contract.

The standard of consent under the GDPR requires that it is 'freely given, specific, and informed.' In addition, consent needs to be able to be withdrawn. Businesses will need to assess whether this threshold can be met given the opaque nature of AI technologies. 'Just in time' notices and consents may be a practical way in which businesses can employ consent to ensure that consents are tailored to specific processing activities.

Legitimate interest is often lauded as the most flexible lawful basis, however the onus is on the businesses to consider any unwarranted impact on the rights and freedoms of individuals, and that the required safeguards and governance have been implemented to meet the GDPR obligations. Furthermore, in order to satisfy this condition, the processing is to be 'necessary' for the stated legitimate interest, meaning that if there is another way to process the personal data to meet the stated legitimate interest, which is less intrusive into people's privacy, the method of processing will not be considered necessary. A decision to rely on legitimate interest will need to be documented in a legitimate interest assessment.

Whilst legitimate interest is an alternative to seeking consent, individuals will have a qualified right to object to processing based on legitimate interest, and therefore businesses will be responsible for implementing appropriate processes and procedures to handle such requests.

The performance of a contract condition is of more limited applicability with regards to processing through AI solutions, and requires a case by case analysis. In general, the processing carried out by AI often goes beyond what is required in order to sell or deliver a product or service and therefore it may be difficult to evidence that the processing is strictly necessary in order to 'perform the contract.'

Purpose limitation

The purpose limitation, i.e. personal data that is only used for the purpose as notified to the individual when the data is initially collected, with certain exceptions, is a central tenant of the GDPR and transparency principle. However, the enhancement of AI solutions entail a material issue with reference to the purposes of data processing, such as:

- the ability of an AI solution to interact with the surrounding environment;
- to learn from the experience; and
- to address future behaviours based on such interactions and learnings.

Whilst the GDPR does not prohibit the use of personal data for an additional purpose, the secondary purpose must not be incompatible with the original purpose. This is a further assessment of fairness. Guidance from the Article 29 Working Party's opinion on purpose limitation states that where processing is carried out for a secondary purpose which involves making a decision which affects the individual, 'free, specific, informed and unambiguous consent would almost always be required, otherwise further use cannot be considered compatible[2].'

AI and machine learning features may cause the processing of personal data to be carried out in different ways and for different purposes than those for which it was originally set. Businesses will need to constantly review the potential outputs and use cases for derived and inferred data, ensuring that the way the data is used is consistent with the original purpose, or carrying out further analysis to determine related use cases, their related lawful basis and consider whether additional notifications, and related consents, are required.

Data minimisation

Data minimisation is the principle that '[p]ersonal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed' and 'personal data should not be kept for longer than is necessary for that purpose.' This stands in tension with developing AI technologies, as it is difficult to know in advance 'what is necessary' in a world of 'surprising correlations' and computer-generated discoveries. The challenges of defining a purpose for processing and only keeping data for that purpose are exacerbated because the nature of machine learning and AI means businesses are not able to predict what the algorithm will learn and secondly, the purpose may also be changed through advances in the algorithm.

AI also challenges retention limits because deleting or restricting the use of data after its original purpose has been fulfilled, or upon request by an individual, could strip businesses of the potential benefits of using that data for AI development, deployment, and oversight. Data is essential if these models are to perform optimally. Yet, keeping data for longer periods, or indefinitely, may fall foul of current data protection laws.

There is clearly no hard and fast rule as to how to apply the data minimisation principles to this evolving technology, but businesses will need implement appropriate controls to ensure that data used to teach these models are up-to-date and accurate, as well as reviewing processes for deletion, where technically possible, as appropriate.

Accuracy

Data quality plays a central role in the effectiveness, or ineffectiveness, of AI technologies. Data quality is relevant at all stages of the processing cycle, collection, analysis and application. Under the GDPR, businesses have an obligation to ensure that data is accurate and up-to date. Businesses employing AI will need to consider not only data accuracy on initial collection, but also the possibility that collected data may become out of date or be inaccurate. Predefining a process for how such inputs can be corrected, and considering the implication of correcting data on previous outcomes, will be crucial to ensuring that results are not tainted by inaccurate data.

Further considerations relating to the training datasets should also be carried out to ensure that the 'sample data' is representative of the population as a whole. This is particularly important where AI is used to perform a level of profiling or automated decisioning.

Finally, businesses should also assess and test any hidden biases contained in datasets which, subject to the purpose of the technology, may lead to inaccurate predictions based on inferred or derived data.

Data subjects' rights

The GDPR introduces a number of enhanced rights for individuals with regards to their personal data, such as the right of access to processed personal data, the right to be informed about the processing, the right to restrict the processing, the right to erase the personal data concerning the data subject, the right to object to the processing of personal data and the right to data portability. In practice, employing new AI technologies, are likely to require that processes relating to handling data subject requests will need to be reviewed and amended to take into account the new method of processing. It is critical that such processes are clearly defined and documented before new technologies are deployed to ensure that businesses do not fall foul of the mandated response periods as set out in the GDPR.

Privacy by Design and Privacy by Default

The GDPR codifies the concept of Privacy by Design and Privacy by Default (Article 25). Businesses looking to implement AI solutions should carefully consider how to adhere to these principles, which may not naturally fit with the nature of data processing by AI systems. The concept of Privacy by Design is important to ensure that data protection principles, such as minimisation, proportionality, etc., are considered at the design phase of AI solutions. It requires that businesses carefully consider and integrate available safeguards into the processing to

ensure that the requirements of the GDPR are adhered to. It follows that under the Privacy by Default, businesses should set technical and organisational measures which typically only permit the processing of what is necessary for each specific purpose.

Data Protection Impact Assessment

Under Article 35(3) of GDPR, the Data Protection Impact Assessment ('DPIA') is required, in case of 'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.' Accordingly, most AI solutions would require a DPIA before carrying out any personal data processing. This will require a detailed assessment of AI solution from a data protection perspective, and an assessment of the relevant security measures which are applied. The Information Commissioner's Office Privacy Impact Assessment Code of Practice sets out the requirements and practical steps on how to complete a DPIA.

Prior consultation of the supervisory authority

In addition, 'where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk,' the controller shall consult the relevant data protection supervisory authority under Article 36 of the GDPR. Open engagement and fluid dialogue with data protection supervisory authorities is key to ensuring that businesses and regulators are informed about any challenges being faced when employing new technologies and determining how the legal obligations can be met.

AI and ethics

There is also a trend towards developing ethical frameworks, i.e. beyond legal compliance, to govern the use of data in AI and other data analytics technologies. This ethical approach addresses the concern that whilst use cases may be legal, is the use case 'responsible.' Currently there is no widely adopted ethics framework or harmonised set of principles for the ethical approach to AI and data, however, if businesses are looking to leverage emerging technologies which are more opaque regarding the way data is used and the outcome, they should be cognisant of the ethical considerations which are typically fairness and transparency.

Conclusion

AI technologies have great potential to offer insights to businesses and the public sector, however, these technologies need to be designed and tested to ensure that they adhere to the data protection legal framework. It is evident that the challenge will be applying the framework in the face of rapidly changing AI solutions and businesses should implement appropriate data protection governance frameworks to meet this challenge. In our next article in the Emerging Tech Series, we will consider the data issues surrounding blockchain.

1. PWC: sizing the prize: what the real value of AI for your business and how can you capitalise? June 2017. Available at: http://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf
2. Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation, European Commission, 2 April 2013, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/p03_en.pdf (pg. 46)

Watch Episode 2 of the Emerging Tech series with Gita and Alexis in full, on the OneTrust DataGuidance Platform.

ashurst

For further video content produced by OneTrust DataGuidance, request a free trial or sign-in to the OneTrust DataGuidance Video Hub today.

REGULATOR SPOTLIGHT

SOPHIE KWASNY

Regulator Spotlight

EUROPE

At the International Association of Privacy Professionals ('IAPP') Global Privacy Summit 2019 in Washington DC, OneTrust DataGuidance spoke with Sophie Kwasny, Head of the Data Protection Unit at the Council of Europe. Sophie discussed what challenges the Data Protection Convention is considering over the next two years, and the relevance of Convention 108+ on the global scale.

How are changing regulations and attitudes around data protection impacting digitalised environments?

Firstly, let's talk about changing regulations before we get to changing attitudes and their impact. I think changing regulations are something that have been quite important in the last decade and we have seen this effect. We now see that there is continuous discussion about the need for regulation, which is globally acknowledged, for instance here in the US. We see that increasing numbers of countries around the globe are moving towards strong data protection laws, so that is something that has to be acknowledged as it has not always been the case. I can remember ten years ago we had discussions on self-regulation, and now it is general knowledge that we need strong data protection laws. That is a way to efficiently protect us individuals. In terms of changing attitudes, I think we have to focus on individuals as users and the fact that users' awareness, especially with all the big scandals that we have seen recently, is key in having an impact on the technologies and how the technologies are developed. In addition, there is a change in attitude not only from the user's perspective, but from the designer and the manufacturer of technologies' perspective. There is now a Center for Humane Technology, which was created in 2013, now trying to put our best interest first. I think that's very significant and it's a virtual circle; it means by design there is this awareness of the need to embed data protection, and with a strong legal framework, I think it these are all a convergence of elements towards respecting our right, our fundamental right, to data protection, so I think that it is fantastic to see this evolution.

What is on the agenda of this year's Data Protection Convention, and why?

The Data Protection Convention meets twice a year in Strasburg for a Plenary session. The Consultative Committee, established by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) ('Convention 108'), is a group of 70 plus countries, which is very significant. They do not all participate as parties to Convention 108, there are only 54 countries that are legally bound. It is a very rich mix of data protection experts that come to Strasburg and they come to discuss topical questions to see how the core provisions of Convention 108 can be articulated and interpreted on various topics. For instance, one of the latest documents that was adopted by Committee 108 in January 2019, was Guidelines on Artificial Intelligence and Data Protection.

In the June 2019 Plenary session, the agenda for the next two years of Committee 108 was discussed. One of the topics was facial recognition. We have seen an absolute deployment of this technology everywhere for various purposes and we have also, once again, seen a call from the makers of the technology for regulation on that topic. Some might say it is already too late, but it is never too late. The Plenary sessions are good, as it is 70 countries coming together and agreeing on standards, soft law, and guidance that they will then take back home for their data protection authority's to try and implement, or try to push their own legislator to get those guidelines in. We thought facial recognition would be a great topic for countries to work together on, considering the challenges that are at stake.

Another topic we would like to work on is completely different, which is the beauty of data protection in that you deal with so many topics. The other topic is individualised education and processing of pupils and student's data by the education system. Here again, we've seen a huge development. We see technologies penetrating the field of education with tools and kits that are proposed to schools that involve data processing, but not that much of an awareness of the fact that its actually quite sensitive data sometimes that is processed, so there is a need to act. It is not too late from a European perspective, as I would say it is not that developed yet, so we are at the beginning, contrary to other countries in the world. It is a very interesting topic, and also it is linked to an award that Committee 108 launched this year for the first time, the Stefano Rodotà Award. The awardees of the prize this year are Ingrida Milkaite and Eva Lievens from Ghent University in Belgium. The prize is for their research concerning children's

"[...] there is this awareness of the need to embed data protection, and with a strong legal framework I think it is all a convergence of elements towards respecting our right, our fundamental right, to data protection."

rights and data protection, so there is a link between the Stefano Rodotà award, the research they awardees are carrying out and the work that Committee 108 will be taking over.

The last topic we are working on is a revision of a text, which was already adopted by the Committee of Ministers of the Council of Europe in 2010, on profiling. This was a really important document nine years ago. We wanted to re-examine it from the point of view of new technologies as there is also a link with artificial intelligence. The evolution in terms of public sector processing/profiling has been taken up quite broadly, so we wanted to address that as well. It was necessary to examine what needs to be reviewed, and then to agree on whether or not the 2010 text needs to be altered.

How is Convention 108+ relevant in a global context?

Although supposedly a European initiative to start with in 1981, already in the drafting phase of Convention 108, the drafters were not only Europeans, but Americans and Canadians, and I think Japan was participating 40 years ago in the work too. So, there was already a willingness of the drafters to go beyond the borders of Europe, because it was about facilitating data. Clearly, we did not have the view of what it would become, with the internet and with the technologies we are now using, but they really had in mind the need to create a harmonised space where the legal protection of our personal data is ensured, so that the data could circulate freely. So that was 40 years ago, and the relevance and the potential of Convention 108 is only now really coming to life. That is why it is absolutely unique at a global level as there is no equivalent, and it is essential to have a text by which governments commit to:

- respecting the provisions commonly agreed so that they will apply the same definitions;
- following the same bases, for instance legitimate bases for processing; and
- the rights of the data subjects so everybody agrees those are the rights we should grant to the data subjects.

So, making the link with this normative development you have worldwide, it is good to have a reference that everybody can follow, and more and more countries are joining from outside of Europe which is highly significant. With the modernised version of Convention 108 that we have delivered (referred to as Convention 108+) what I think is very important in the global context is an incentive and a facilitation of cooperation between the data protection authorities. That is also something that is provided by Convention 108+, that is one of the big issues we need to insist on in this globalised environment we are dealing with.

What data protection issues do you think will arise in the near future?

What is amazing with data protection is that it is constantly evolving, and new challenges emerge that you have to address with core provisions and principles that date back from decades, so how do you continue to adapt them? Something I really see coming is not necessarily concerning the technological core developments, but I think looking at data governance and how an increasing volume of data is produced, that this can actually be used for the greater good. However, how can we ensure that? Therefore, this would be one of the key topics for the future because we definitely need to seize the potential for the information that is there and can help us for public good.

Sophie's interview is a part of OneTrust DataGuidance 'Thought Leaders in Privacy' video series.

For daily updates regarding regulatory developments, such as Convention 108+, as well as news from over 300 jurisdictions visit the News Tracker on the OneTrust DataGuidance Platform.

Request free trial access or sign in today.

OneTrust

Privacy Management Software

World's #1 Most Widely Used Privacy Management Software

For Privacy, Security & Third-Party Compliance

Solutions to Comply with the CCPA, GDPR & Global Privacy Laws & Security Frameworks

Privacy Program Management:

- **Maturity & Planning:** Compliance Reporting Scorecard
- **Program Benchmarking:** Comparison Against Peers
- **DataGuidance Research:** Regulatory Tracking Portal
- **Assessment Automation:** PIAs, DPIAs & Info Security

Marketing & Privacy UX

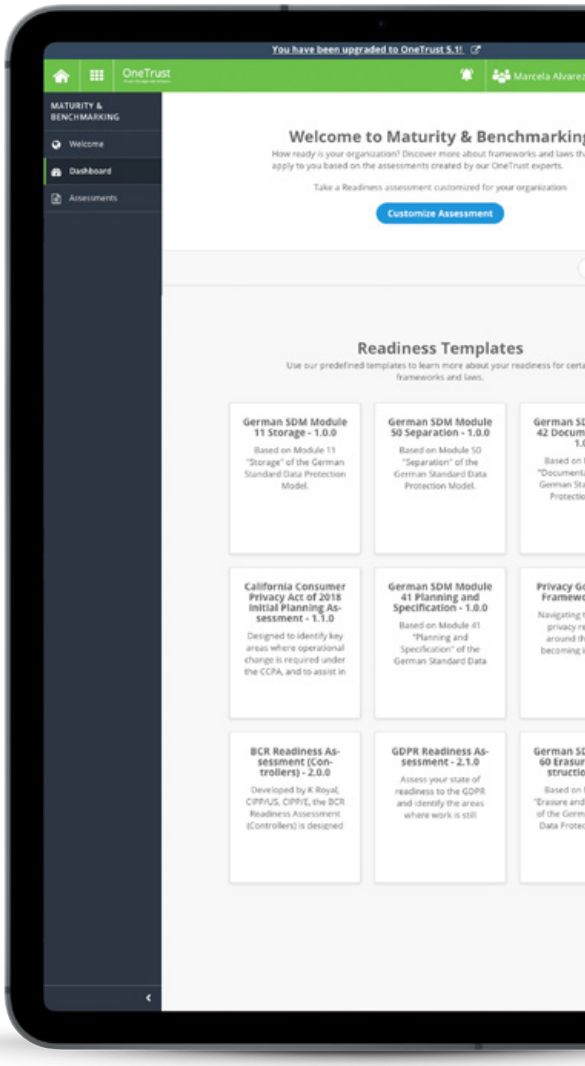
- **Cookie Compliance:** Website Scanning & Consent
- **Mobile App Compliance:** App Scanning & Consent
- **Universal Consent:** Consent Receipts & Analytics
- **Preference Management:** End User Preference Center
- **Consumer & Subject Requests:** Intake to Fulfillment
- **Policy & Notice:** Centrally Host, Track & Update

Third-Party Risk Management

- **Vendorpedia Management:** Assessment & Lifecycle
- **Vendorpedia Risk Exchange:** Security & Privacy Risks
- **Vendorpedia Contracts:** Contract Scanning & Analytics
- **Vendorpedia Monitoring:** Privacy & Security Threats
- **Vendor Chasing Services:** Managed Chasing Services

Incident & Breach Response

- **Incident & Breach Response:** Intake & Lifecycle Management
- **DatabreachPedia Guidance:** Built-in guidance from 300 laws



GET STARTED TODAY | ONETRUST.COM/FREE-EDITION

LEARN MORE ABOUT ONETRUST | REQUEST A DEMO | ONETRUST.COM

OPINION

Senator Iyere Ihenyen Lead Partner
senator@infusionlawyers.com
Infusion Lawyers, Lagos

Nigeria: New regulation demonstrates a serious approach to data protection

On 25 January 2019, the National Information Technology Development Agency ('NITDA') issued the Nigeria Data Protection Regulation 2019 ('the Regulation'). Although it is a subsidiary legislation, the Regulation has the force of law, having been issued in accordance with the mandate of the National Information Technology Development Agency Act 2007 ('NITDA Act'). Senator Iyere Ihenyen, of Infusion Lawyers, provides insight into how the Regulation will work, and comments on the impact it will have on data protection within Nigeria.

In today's data-driven global economy, Nigeria clearly wants to safeguard the personal data of Nigerians wherever they are, regardless of the means of data processing, or the location of the data controller or processor.

Before the Regulation, Nigeria had the Guidelines on Data Protection 2013 ('NITDA Guidelines'). However, right from the inception of the NITDA Guidelines until the time they were repealed, there were doubts over their status, coupled with a lack of enforcement of them. The NITDA Guidelines were also not as comprehensive as the Regulation.

By having a stronger protective regime for data privacy, in tune with global best practices, Nigeria hopes to help boost international trade and commerce. At a time when transactions increasingly involve personal data processing, one of the objectives of the Regulation is to ensure that there are adequate safeguards in place. Also, the economic advantage to data protection is not lost on the makers of the Regulation. The scope of the Regulation and its penalties demonstrate this consciousness.

Scope of the Regulation

The Regulation brings all data processing transactions involving data subjects who are Nigerians, anywhere in the world, under the Regulation, regardless of where the data controller or processor is located. Considering the huge and ever-growing population of the Nigerian people, home and abroad, applying protection to the personal data of natural persons residing in Nigeria, and natural persons residing outside of Nigeria but who are of Nigerian descent, is a welcome development. No data controller or data processor anywhere in the world should be under any mistaken impression that the Regulation does not apply to it. Similarly to how the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') deals with the personal data of EU citizens, the Regulation will also work to protect the personal data of Nigerians globally. Data controllers and data processors involved in any data breach affecting the personal data of Nigerians are liable to the penalties set out by the Regulation.

Of course, the universal scope of the Regulation will certainly be a tall enforcement hurdle for NITDA, and for the various relevant authorities

in Nigeria whose responsibility it is to regulate personal data in various sectors. International cooperation must be vigorously pursued, otherwise the success of enforcement would be significantly affected.

Data protection authority in Nigeria

The Regulation does not recognise NITDA as the sole data protection authority ('DPA') in Nigeria, and rightly so. This is because apart from NITDA, there are other relevant authorities, or statutory bodies, mandated by law to deal with matters relating to personal data in Nigeria. Therefore, under every act, regulation, and guideline that relates to personal data protection, various government agencies are typically designated as the DPA in their relevant sectors. For example, in Nigeria's financial services industry, where the Consumer Protection Framework 2016 and the Credit Reporting Act 2017 apply, the Central Bank of Nigeria is the DPA. Similarly, in the telecommunications industry, the Nigerian Communications Commission is the DPA.

There have been calls for the establishment of an overarching DPA in Nigeria, but there are administrative and political concerns. A Data Commission Bill was passed 16 May 2019 by the National Assembly, which was forwarded to the President for assent. If assented to by the President, the Data Commission Bill will establish Nigeria's Data Commission. The Data Commission will be responsible for protecting personal data and regulating the processing of personal data, and other related matters.

Procuring consent of a data subject

Considering the high rate at which data controllers process personal data without first obtaining the data subject's consent, it is good to see that processing personal data without the data subject's consent is prohibited. Subject to legitimate purposes, such as for the prevention of crime, to aid an investigation, or for a court order, the Regulation prohibits the processing of personal data without first obtaining the data subject's consent. Before transferring personal data to a third party for any reason, the data subject's consent must also be obtained. Also, seeking, giving, or accepting consent in order to directly or indirectly propagate anti-social conducts, atrocities, children's rights violations, criminal acts, and hate, is prohibited by the Regulation. This will impact mainly on Nigeria's telecommunications industry, where subscriber's personal data is often subject to daily abuse.

Due diligence by data controllers

It is good to note that data controllers and data processors are now liable for the actions or inactions of third parties who handle the personal data of data subjects protected under the Regulation. This will minimise negligence and recklessness on the part of a data controller and processor. As a party to a contract, a data controller or processor is required to take reasonable measures to ensure that the other party does not violate the data processing principles under the Regulation. It must ensure that the other party is either accountable to NITDA or a regulatory authority for data protection within or outside of Nigeria. As NITDA does not have power over data controllers and processors outside of Nigeria, under the Regulation, regulatory authorities who exercise control over data controllers and processors outside Nigeria will provide enforcement assistance to NITDA, or the relevant regulatory authority in Nigeria. Enforcing this will definitely be a major challenge for regulators.

If NITDA does succeed in developing international cooperation and mutual assistance towards effective enforcement of personal data protection legislation, the magnitude of this task would be minimised. The Regulation contemplates information exchange, complaint referral, and investigative assistance amongst DPAs across jurisdictions. Whether NITDA can pull this off is debatable. So far, we are not seeing those international co-operations happening. Even locally, we are yet to start witnessing enforcement.

Privacy policies and data security for protection of personal data

Data controllers are now mandated to have a privacy policy published on their website or any medium through which they collect or process personal data. This is good, but even better is the requirement that data controllers or processors must put data security measures in place to ensure data protection. Beyond policy statements, data controllers must put measures in place to protect the personal data they collect, process, store, or transfer. Though the Regulation does not stipulate penalties for failing to have these data security measures, should a data breach result from this failure, data controllers and processors will be liable to the same penalties stipulated for data breaches.

Rights of a data subject under the Regulation

The Regulation does a good job guaranteeing privacy rights, such as:

- right to access;
- right to object;
- right to withdraw consent;
- right to deletion or right to be forgotten, and;
- right to data portability.

However, it does not adequately provide remedial procedures to data subjects. Merely listing these privacy rights without detailing the redress that must be made available by data controllers, to an aggrieved person for certain data breaches, creates uncertainty. This uncertainty may affect the extent to which data subjects are able to enforce their rights. Particularly in a jurisdiction where enforcing rights is a major challenge, ensuring easily accessible and free, or cheap, administrative enforcement mechanisms at the level of data controllers, and then at the level of relevant DPAs, should have been given better attention. For example, the Regulation gives data subjects the right to submit complaints to a DPA, but it is silent about applicable remedial procedures, administrative timelines, and specific remedies for redress. Establishment of the administrative redress panel ('the Panel') is a good idea, but this is a quasi-judicial process that typically applies after pursuing redress with data controllers has already failed.

Restrictions on and exceptions to international data transfer

While the administrative and supervisory roles given to NITDA and the Accountant General of the Federation ('the AGF') are understandable, given how sensitive international data transfer generally is, they are bound to create a serious bureaucracy inconsistent with global competitiveness. It is a relief therefore that the Regulation contains certain exceptions to NITDA's or the AGF's supervision. By obtaining the data subject's consent by virtue of necessity, such as contract performance, implementation of precontractual measures, public interest, etc., data controllers effectively avoid the requirement of obtaining approval from NITDA and the AGF.

Penalty for data breach

Unlike the NITDA Guidelines, which did not contain any penalties apart from the general penalties stipulated under the NITDA Act, the penalties stipulated under the Regulation demonstrate that Nigeria is taking data protection more seriously. Under the Regulation, a data controller who deals with more than 10,000 data subjects shall be liable to pay a fine of 2% of its annual gross revenue ('AGR') of the preceding year, or pay NGN 10 million (approx. €25,000), whichever is greater. Similarly, for a data controller

who deals with less than 10,000 data subjects, the data controller is liable to pay the fine of 1% of the AGR of the preceding year, or pay NGN 2 million (approx. €5000), whichever is greater. Apart from the nationality issue, adopting a GDPR approach to both the scope and the penalties for data breaches is quite commendable, particularly when one considers Nigeria's huge and growing population, home and abroad. If efficiently and effectively enforced, this will certainly set Nigeria up as a leader within Africa in terms of data protection, but this won't be a walk in the park. NITDA must be prepared to effectively enforce penalties against data controllers and data processors who breach the privacy rights of data subjects under the Regulation. This is particularly so with organisations that process the personal data of Nigerians on global platforms. NITDA will definitely need international co-operation. The provisions of the Regulation are quite inadequate in this regard, as it expects NITDA to drive that process and put cross-border enforcement mechanisms in place.

Third-party violations and the data controller's liability to data subjects

By impinging liability on a data controller, the Regulation protects a data subject against third party violations. This will have a direct effect upon data controllers, as the excuse that the data subject's personal data is out of the data controller's control, will no longer be tenable. This is why the Regulation requires third party data processing contracts between data controllers and the partners they engage. Consequently, data controllers must now keep processors that they can trust as partners. By way of improvement, I think the Regulation should have listed certain exceptions in order to limit the data controller's liability to events where the data controller may have failed to take reasonable steps to ensure compliance by third parties.

Data protection officers and data protection compliance organisations

The Regulation makes it a requirement for a data controller to appoint a data protection officer ('DPO'). This is necessary, and also consistent with global best practices. DPOs are expected to make NITDA's, or the relevant authority's, regulatory role less difficult, since DPOs are better positioned to handle administrative inquiries. The Regulation introduces data protection compliance organisations ('DPCOs') with whom DPOs are expected to closely work. Registered and licensed by NITDA, DPCO's responsibilities include data monitoring and auditing, conducting data protection training, and consulting on data protection compliance. For transparency, the Regulation should have stated the qualification requirements for DPCOs, and the procedure for application. Since DPCOs are independent of NITDA or any relevant DPA, it will be interesting to see how DPCOs carry out their mandate in NITDA's or the relevant DPA's interest.

Establishment of the Panel as an enforcement mechanism

The introduction of the Panel, charged with the responsibility of providing redress to data subjects under the Regulation, is commendable. The Panel is required to:

- investigate allegations of data breach under the Regulations;
- invite affected parties to respond;
- make necessary orders; and
- provide redress all within 28 days.

However, it remains to be seen how the Panel will implement this provision in a country where rights enforcement remains a major challenge, mainly due to a lack of rights awareness, a generally inefficient justice system, weak capacity building, and poor funding. Data breach-related dispute resolution will increasingly become a serious affair in Nigeria, with state and non-state actors. To ensure that the Panel carries out its duties efficiently without fear, favour, or undue influence, its independence should have been secured, and a fund established for its operations.

Beyond establishing a Panel for enforcement of data privacy rights, the Regulation fails to stipulate modern enforcement mechanisms for data protection. In today's technologically advanced world where large-scale data breach is most likely, many data protection regulations now require data processors to implement Privacy by Design principles and carry out periodical Privacy Impact Assessments. These mechanisms boost prevention of data breaches.

Nigeria needs a data protection act, not subsidiary legislation

Nigeria needs a principal legislation on data protection. After the ghostly existence of the NITDA Guidelines for up to six silent years, one would have expected that Nigeria would enact a more comprehensive data protection legislation. For more efficient and effective administration, regulation, and supervision, new legislation should establish an overarching DPA in Nigeria. The establishment of this would not necessarily mean that relevant authorities under the various laws, regulations, and directives would no longer have roles to play in data protection within their sectors and industries, but, by having an overarching DPA, there would be more efficient and effective coordination.

In a GDPR era where every country is putting the power of data back in the hands of its people, I think a more comprehensive data protection regime would have been more appropriate. Particularly in the areas of definite procedures for adequate redress against data breaches, the Regulation is a far cry. While Nigeria may not enact a comprehensive data protection law anytime soon, hopefully all relevant authorities in Nigeria will at least use the Regulation as a general basis for adopting a sector-specific approach to data protection and privacy in their various sectors.

Final words

Though the Regulation does not have all the answers to data protection, by issuing the Regulation less than a year after the GDPR was introduced in the global data protection landscape, Nigeria is demonstrating that it realises how critical the protection of personal data has become in today's data-driven global economy. So, should we be expecting global platforms such as Facebook and Google, for example, to pay as much as NGN 10 million, or 2% of their annual gross revenue of the preceding year, in cases involving more than 10,000 data subjects protected under the Regulation? The answer is **yes** [emphasis added].

In the data game, with both local and global players in an increasingly competitive digital economy where data is 'the new oil,' Nigeria is saying it is ready to play. By the Regulation, Nigeria is taking data protection more seriously. But how NITDA will handle enforcement with other relevant authorities is another kettle of fish.

This article was published in the Opinion section of the OneTrust DataGuidance Platform.

Request a free trial or sign-in to the OneTrust DataGuidance platform today to access more than 50 Guidance Notes and 390 pieces of Legal Research from 37 jurisdictions across Africa

PrivacyConnect

CCPA & GDPR Community by OneTrust

NEW DATES ANNOUNCED!

125+ FREE WORKSHOPS

100+ GLOBAL CITIES

CCPA, GDPR & LGPD
Dive into regulatory requirements
and how to implement in practice

INTERACTIVE ACTIVITIES
Gain practical implementation tips
through activities and group discussions

WEBINAR SERIES
Hear from distinguished privacy innovators
on top-of-mind regulatory topics

REGISTER FOR A LOCAL WORKSHOP TODAY: PRIVACYCONNECT.COM

Privacy Talks

David Hoffman
Global Privacy
Officer at Intel

David Hoffman is Global Privacy Officer at Intel, and has led the first comprehensive cybersecurity review of Intel. At the International Association of Privacy Professionals Global Privacy Summit in Washington in 2019, OneTrust DataGuidance spoke with David about his experiences of the existing privacy bills in the U.S. and what the likelihood of their being a federal privacy bill is.

How do some of the recently introduced state-level privacy bills compare to the CCPA?

I think we now have this recognition that individuals are concerned about privacy and they are searching for ways to have their privacy risks mitigated. For the ballot initiative to be started by Alistair Mactaggart, and then for that to result in the California Consumer Privacy Act of 2018 ('CCPA') is a visible result for everybody who is involved in the privacy environment. It shows that something needs to be done because individuals are really crying out saying that both the current situation and environment are unacceptable. So now we have a situation where legislation is popping up all over the country. Actually, by our count, over 20 pieces of legislation that are at some point in the judicial process in individual states, and those are only the comprehensive bills which are similar to CCPA. For targeted pieces of legislation, we would say there's probably over 90 pieces of legislation. So, the issue when looking at all of them in total is that they are not harmonised in their requirements in any way.

They take certain different approaches, and many of them have learnt from the CCPA and therefore take that particular approach. However, it is that diversity that the economy cannot handle, especially in terms of regulatory requirements for things like the successful processing of personal data when each individual state is going to have a different way at setting out their own different requirements. I think this is bad for individuals because they are going to have differing rights depending on what state they are in, and I think it is going to be bad for companies that are trying to figure out how to put compliance operations in place.

What prompted Intel to draft a proposal for a federal privacy bill?

After the CCPA had come into force, what we realised was that having a patchwork of state legislation really wasn't going to work, and that what we really needed to be able to articulate is a way to regulate privacy that would actually still allow for the innovative use of data. At Intel, we believe that technology is going to help solve some of the biggest social problems that we have, whether that is improving the efficacy and reducing the cost of healthcare, or whether that is improving environmental issues, or whether its improving the way cities work and transportation systems function. All of that is going to require a lot of data to be used in an ethical and appropriate way, so how do you create the right legislative structure to allow people to use data in appropriate ways, but to also ensure that there are limitations on that use so the data is not going to be used to harm them.

Intel was involved in several efforts, alongside other companies, in trying to create legislation, but we kept feeling like at the end of the day the bills that we were talking about in those processes were not really optimising both innovative data use, and protecting individuals.' We also got a bit discouraged that all of these legislative processes were happening behind closed doors, and they'd always be under Chatham House Rules. Nobody could talk about this externally, and we finally said, "Look, we are creating public policy for the future of technology, we are not even using the technology that we have today to create public policy." So, what we decided to do was to write the bill we believed was going to be the best for individuals privacy and the use of data, which would be good for Intel in the end because we make money and our business succeeds when people can have trust and confidence in the use of technology. So, we thought if we could accomplish this, we knew it was going to be good for our business, and we said, "Let's just do this in an open and transparent way, we are talking about transparency with privacy, let's just create a website."

It ended up being USprivacybill.intel.com. We decided to put our legislation up there, and to contact a whole

"I'm incredibly hopeful that we are going to see federal privacy legislation by the end of this Congress, so I think the reasonable timeline is the end of 2020."

bunch of leading experts in privacy law in order to have an expert section. I told them that we were going to give them password access, that we would not edit anything they write, that they could tell us what they liked and what they did not like about our law, and then we would take those comments, and any comments we get from the general public, into consideration. We would then come out with a second draft, which we launched in November 2018. I was really excited about the content, but I knew there was hard issues that I was not confident that we had gotten right. However, we got tremendous feedback and people were really happy with the opportunity to engage, it was a sort of online participatory democracy. We also got a lot of comments from the general public that came flooding in. We took all of those comments from the experts and from the general public, we did a second draft that we released on Data Privacy Day on 28 January 2019, and we also took the feedback that we got from that. All of that was loaded up on the website and we released a third draft on 25 May 2019, one year on since the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into force.

Do you see potential in a federal privacy law passing in the US in the near future?

I am incredibly hopeful that we are going to see federal privacy legislation by the end of this Congress, so I think the reasonable timeline is the end of 2020. I have been spending an awful lot of time in Washington and talking with other stakeholders. I am really encouraged that it is truly a bipartisan issue, and that both sides of the aisle are really engaged on needing to protect individuals' and still provide for the innovative use of data to drive our economy.

What I see is an agreement converging in a number of areas, and so now it is about the process, and we are going to do it. There are going to be some hard questions and pre-emption is really hard. There are a lot of issues around how much authority to give to the Federal Trade Commission ('FTC') and how many additional staff the FTC needs, but those are all issues we can work through, and from everything I hear, I think the momentum is going in the right direction and I am incredibly hopeful that we are going to get it done.

What is your view on how facial recognition technology is regulated in the US?

There are a lot of appropriate concerns around facial recognition technology, particularly around bias and whether the data that was used to train the algorithms that are being used for facial recognition are robust and diverse enough so that different populations are treated appropriately.

Our view at Intel is that those issues are not unique to facial recognition, those issues happen anytime you are using data to train algorithms that are going to make decisions about people. Whether it is facial recognition, or gate recognition, or speech recognition, or another type of biometric identification, or whether it is just sort of general data mining or data broker activity, we think the right way to handle this is as part of a comprehensive federal privacy bill, like the one we put forward.

David's interview is a part of OneTrust DataGuidance 'Thought Leaders in Privacy' video series.

Compare privacy legislation, including the CCPA, from across U.S. jurisdictions with the brand-new U.S. State Law Tracker on the OneTrust DataGuidance Platform.

To access the OneTrust DataGuidance Platform, request a free trial or sign-in today

Claire Walsh Director of Global Privacy and Data Protection
claire.walsh@marshalldenning.com
Marshall Denning, London

EU: DPO - how far can you go?

The requirement to appoint a data protection officer ('DPO') if you carry out certain types of data processing, is one of the many changes that was ushered in with the implementation of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') in May 2018. Claire Walsh, Director of Global Privacy and Data Protection at Marshall Denning, examines the scope of the DPO role and its potential evolution.

DPO job description

Article 37 of the GDPR requires private organizations to appoint a DPO if their business involves 'regular and systematic monitoring of data subjects on a large scale or when the organization processes special categories (as defined by Article 9) of personal data 'on a large scale.' Organisations that do not meet the criteria in Article 37 may still opt to appoint a DPO but are not required to do so. Organisations that have elected to appoint a DPO based on the criteria set out under Article 37 of the GDPR are either confident that their processing activities mean that they are legally required to do so, are unsure whether or not they need a DPO and have decided to appoint one, or have determined that a DPO is not mandatory but nevertheless have decided that designating a DPO will be beneficial.

Whether the DPO's appointment is mandatory or voluntary will not change its fundamental job description, which is laid out under Articles 37, 38 and 39 of the GDPR. This was confirmed in the most recent Article 29 Working Party ('WP29') Guidelines on DPOs[1] ('WP29 Guidelines'). Although introduced prior to the effective date of the GDPR, the WP29 Guidelines have been endorsed by the European Data Protection Board ('EDPB'), and to date the EDPB has not issued any further guidelines to supplant them. Organisations that are designating a DPO on a voluntary basis may want to consider the alternatives available, such as appointing a data protection manager, who can perform many of the same functions but will not be burdened by the various DPO obligations set forth in the GDPR. According to the GDPR, the DPO role encompasses 'at least' the following skills and tasks:

- having 'professional qualities' that include expert knowledge of data protection law and practices[2];
- being involved in all issues relating to the protection of personal data[3];
- reporting directly to the highest level of management in the business[4];
- informing the organisation and its employees of their data protection obligations under

the GDPR and local laws[5];
- monitoring compliance with the GDPR, local data protection laws and internal policies, including staff training and audits[6];
- providing advice and support with data protection impact assessments[7]; and
- cooperating with and being a contact point for the regulator[8]. (Article 39(1)(d) and (e).

The WP29 Guidelines elaborate on these and make the following notable observations:

- the DPO should be invited to participate regularly in meetings of senior and middle management;
- the opinion of the DPO must always be given due weight (in case of disagreement, the WP29 recommends that the reasons for not following the DPO's advice are documented); and
- although it is the organisation that is required to maintain a record of processing under Article 30 of the GDPR, in practice this may fall to the DPO to manage under the responsibility of the controller or the processor.

DPO candidates

Although the DPO is required to have an expert knowledge of applicable data protection laws, there is nothing in the GDPR requiring them to be a qualified lawyer. The reference to 'professional qualities' is a little ambiguous, but the WP29 Guidelines relate this back to expertise in privacy laws and the ability to fulfil the DPO tasks.

The WP29 Guidelines include a non-exhaustive list of relevant skills and experience, which include understanding information technologies and data security, as well as knowledge of the business sector and organisation.

Being a technologist and industry expert appear then to be as important as having the requisite legal knowledge.

Take the recent ICO enforcement action against British Airways: this related to a cyber incident where customer details were harvested by attackers. The ICO investigation found that poor security arrangements had led to customer personal data being compromised in this way. A DPO assisting with a similar breach and/or regulatory investigation would need to appreciate the adequacy or otherwise of the businesses technical and organisational measures, which calls upon expertise beyond a legal qualification.

Carrying out a straw poll of advertised DPO vacancies in May 2019, not all list a legal qualification as being essential, although several ask for a recognised privacy or security certification. These include the International Association of Privacy Professionals (IAPP) Certified Information Privacy Professional (Europe) (CIPP/E), Certified Information Privacy Manager (CIPM) or Certified Information Privacy Technologist (CIPT), or the British Computer Society (BCS) training courses for IT professionals.

More guidance on DPO qualifications is expected from supervisory authorities. In July 2019, the French data protection authority approved the first DPO certification and accreditation body. Earlier in the same month, the Spanish data protection authority announced that it had issued a DPO certification scheme.

DPO options

Before organisations despair of being able to find and fund the DPO role, it is worth noting that the GDPR caters for a number of options.

Sliding scale of expertise depending on the complexity

The WP29 Guidelines recognise that the necessary level of expert knowledge should be commensurate with the sensitivity, complexity and amount of data that is being processed.

It follows that in the case of straightforward and lower risk processing activities, a seasoned DPO may not be required and a candidate with less experience could be considered for the role, provided of course that they are still in a position to fulfil the mandated DPO responsibilities.

DPO as one of many hats

Article 38(6) of the GDPR permits the DPO to fulfil other tasks and duties. The UK Information Commissioner's Office Guide to the GDPR further clarifies that the DPO can be an existing employee. The DPO function could therefore be assigned as part of an existing employee's job role, or as part of a new role with other responsibilities. However, important provisos are that the DPO should have sufficient time to fulfil their duties alongside those of their other role, and that this should not result in a conflict of interest. The WP29 Guidelines goes on to state that 'the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of processing of personal data.' There are also a number of positions that the WP29 considers will conflict with the DPO role as a general rule. These include chief executive, chief operating or financial officer, head of marketing, human resources or IT, or other roles lower down in the organisation if they involve deciding on the purposes and means of processing personal data. In applying these constraints, the list of internal candidates and the potential for combining the DPO with other roles may dwindle. Where this is a viable option, the WP29 recommends that the organisation take a number of good practice steps, including safeguards, to avoid potential conflicts.

The outsourced DPO

It is clear from Article 37(6) of the GDPR that the DPO does not need to be a staff member, and that the function can be performed by an external service provider. The WP29 affirmed that the DPO can be external, and their function exercised based on a service contract concluded with an individual or an organisation. This choice may be advantageous where the organisation is not certain whether or not a DPO is mandated, and/or they do not require the services of a full-time member of staff to perform the role. It is of course critical that the allocated hours are sufficient for the DPO to fulfil their duties, and the terms of the services contract require careful consideration to ensure that any 'spikes' in demand (for example, arising from personal data breaches or regulatory investigations) can be met. The WP29 recognised that a team of individuals can carry out the DPO tasks when the DPO function is exercised by an external service provider. This may be an efficient way to cover off the divergent areas of expertise that are identified as forming part of the DPO role. Outsourcing the DPO role does not avoid the possibility of a conflict of interest, although different considerations apply. The WP29 Guidelines give the example of an external DPO that is asked to represent the organisation that appointed them before the courts in cases involving data protection issues. This effectively rules out the appointment of an organisation's legal advisor as its DPO.

The group DPO

Article 37(2) of the GDPR allows a group of companies to appoint a single DPO. This is on the proviso that the DPO is easily accessible from the place of establishment of each organisation. The WP29 Guidelines shed some light on the notion of accessibility, which refer to the tasks of the DPO as a contact point with respect to data subjects, the regulator and also internally within the organisation. As the DPO must be in a position to efficiently communicate with data subjects and cooperate with the relevant regulator, the WP29 points out that this communication must take place in the language(s) used by them.

The day to day DPO

Although the DPO job description is

well documented in Articles 37-39 of the GDPR, there is often confusion about what the DPO day job looks like. Stated plainly, Article 38 of the GDPR requires the DPO to be involved "properly and in a timely manner, in all issues that relate to the protection of personal data." This would include serving as a key advisor to the business as it looks to implement new processing activities and needs to assess potential risks to personal data. It would also include ensuring the company's record of existing processing activities is maintained accurately and that the technical and organizational security measures in place to protect personal data are sufficient given the risk profile. The DPO must also be involved at the early stages of any security incident that is a potential personal data breach. The DPO will need to co-ordinate with other stakeholders in their assessment of the incident, the steps that can be taken in mitigation, and whether notification to the supervisory authority or to individuals is required. The advice of external experts may also be required, for example local counsel in the applicable jurisdictions and forensics or cybersecurity consultants. The limited window for notification to the supervisory authority means that the DPO and other players will need to move quickly. Following notification and the conclusion of any internal or external investigation, the DPO will be involved in advising on and documenting any remediation measures. Similarly, if the business is involved in a regulatory investigation then the DPO will be the point of contact for the supervisory authority. Neither security incidents nor regulatory investigations will be a daily occurrence, however.

When the DPO is not putting out fires, a critical part of their role is to embed privacy considerations into the business. In order to be successful, the DPO will need to be made aware of any new project or process that involves processing personal data, so that the DPO can consult on and arrange for a Data Protection Impact Assessment ('DPIA') to be carried out, for a true Privacy by Design approach to the new activity. For example, if the DPO is involved in the requirements gathering for a new software product, they will have the opportunity to ensure that it is aligned with legal requirements and privacy best practice including data minimisation, notices, security, and the need to capture and record any consents, where relevant.

In the same vein, involving the DPO at the due diligence phase of any potential acquisition will facilitate the early identification of any privacy risks, as well as in the post closing integration of the target with the acquiring business.

Workflow automation and data mapping platforms may be a useful resource for the business in ensuring that the DPO's time is not absorbed by performing tasks that could be automated, such as updating Article 30 records, tracking data subject consents and carrying out DPIAs, legitimate interests assessments or vendor due diligence. The business may increasingly rely upon technological solutions, in particular where they do not have a team or other colleagues who could assist the DPO and key stakeholders in completing these tasks.

None of this however should detract from the DPO's independent, advisory role: it is the data controller that is the decision maker in relation to the personal data being processed.

Where the DPO is appointed by a business that operates globally, the DPO will often be called to advise on privacy questions outside of Europe where the GDPR does not apply. Although the DPO's appointment is made by virtue of the GDPR, their expertise will be relevant to managing a privacy compliance programme in other jurisdictions. The proliferation of data protection regulation globally may mean that the DPO is in a position to influence the company's international privacy standards and strategy.

DPO risks and challenges

Conflicts may arise between the DPO and the business stakeholders, in particular around the assessment of privacy risk. Ultimately it is the business and not the DPO that must decide on the course of action to take, although any decision will be recorded and may not be privileged from disclosure. The UK supervisory authority's latest guidance is clear on this point, stating that DPOs should provide risk-based advice, but if organisations decide not to follow it, the decision should be documented in order to demonstrate accountability.

The DPO should be in a position to maintain their independence notwithstanding any perceived pressure from the business arising from competing objectives. The DPO's access to the organisation's senior management is intended to support this position. This may be difficult to facilitate in a global dispersed organisation where the DPO does not have a direct reporting line to the C suite, but can be achieved through regular reporting to the board and a procedure for escalating any issues, where required.

Another risk for the DPO is the issue of liability. It is clear from Article 24(1) of the GDPR that data protection compliance is the responsibility of the controller or the processor. Question 12 of the WP29 Guidelines also covers this specific question, and states that DPOs are not personally responsible for non-compliance with the GDPR. Other liabilities arising under applicable local laws may result in personal liability attaching to the individual.

Conclusion

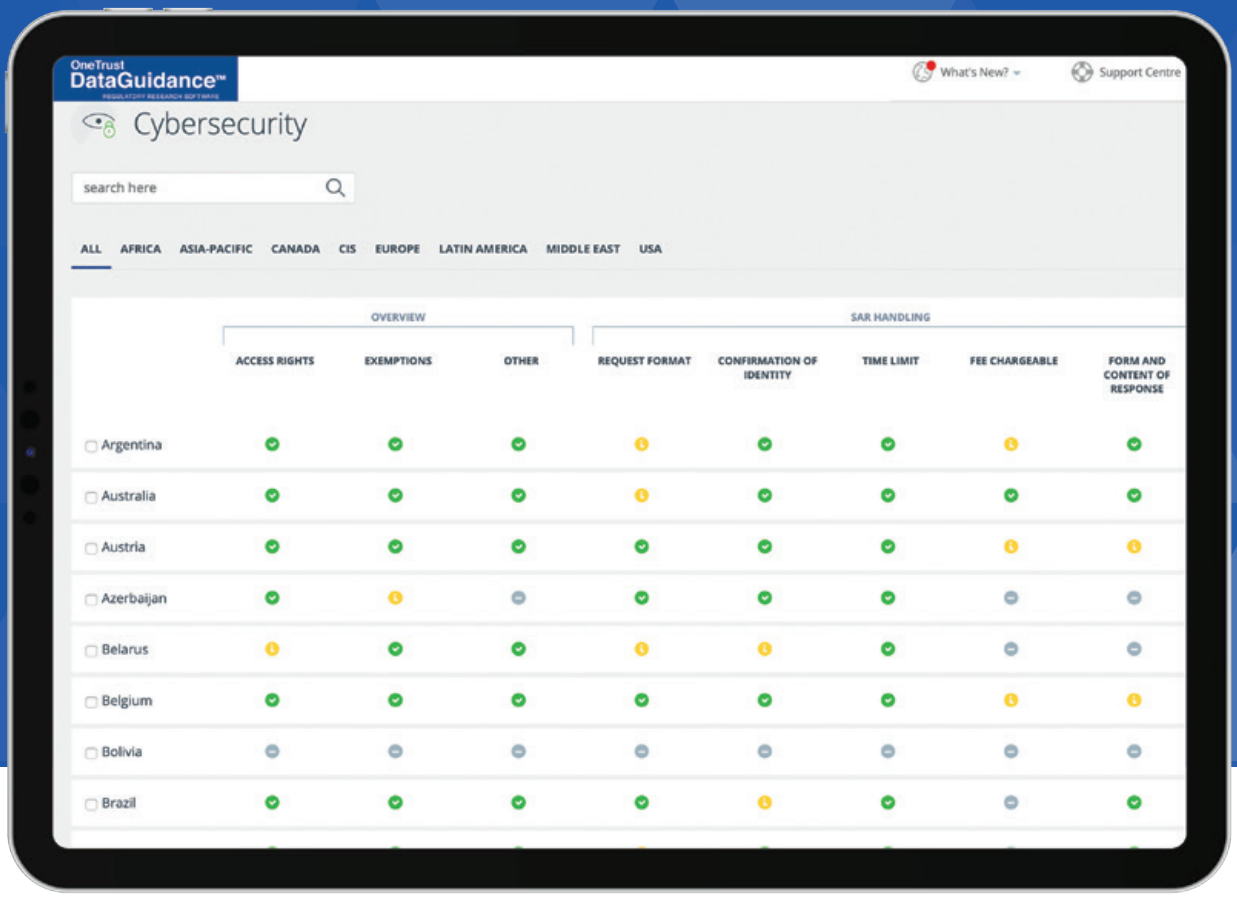
The scope of the DPO role has been further defined by the GDPR, but it will continue to evolve in light of the increasing proliferation of privacy regulations on a global scale.

1. WP29, Guidelines WP 243 rev.01 on DPOs, adopted on 13 December 2016 as last revised and adopted on 5 April 2017.
2. Article 37(5) of the GDPR.
3. Ibid, Article 38(1).
4. Ibid, Article 38(3).
5. Ibid, Article 39(1)(b).
6. Ibid.
7. Article 39(1)(c) of the GDPR.
8. Ibid, Article 39(1)(d) and (e).

Cybersecurity Comparative Resource

Understand and compare provisions across global cybersecurity legislation. Find detailed information regarding:

- The scope of application and requirements of each law, considering technical and organisational measures
- Notification of incidents
- Appointment of security officers



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

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

LATEST EDITION

Comparing privacy laws:
GDPR v. LGPD

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

B/LUZ ADV

On 25 May 2018, the General Data Protection Regulation (Regulation (EU 2016/679) ('GDPR') went into effect, and in August 2018, Brazil approved Law No. 13.709 of 14 August 2018, General Personal Data Protection Law ('LGPD'). This was further amended by Law No. 13.853 of 8 July 2019, and the LGPD is now expected to enter into effect in August 2020. As a result of the amendments, OneTrust DataGuidance and Baptista Luz Advogados have updated their report: Comparing privacy laws: LGPD v. GDPR aimed at highlighting the similarities and differences between the two pieces of legislation in order to help organisations develop their compliance activities.

David Longford, CEO at OneTrust DataGuidance, and Renato Leite Monteiro, Partner and Head of the Data Protection Practice at Baptista Luz Advogados comment on the recent amendments and the release of the updated report.

David Longford
Privacy professionals working internationally should look for global patterns trends, but be aware that significant differences exist between regulations such as the GDPR and the LGPD, even if some of the driving factors and focus are on the importance of data protection law to protect individual rights. A jurisdiction's unique history, culture, legislative landscape, and the types of data processing common locally, will all shape the focus and application of a data protection law. Influence does not necessarily lead to equivalence and/or compliance.

Renato Leite Monteiro
Even though the LGPD was highly influenced by the GDPR, it is far from being the same regulation. However, it is quite common to hear that if one is compliant with the GDPR, one would also be compliant with the LGPD. This affirmation is far from being correct. From the scope of the LGPD, to the rights granted to data subjects, to the legal basis of processing, to data protection officers and Data Protection Impact Assessment requirements, the concept of personal data in the LGPD can be deemed as wider than the GDPR. It is an extremely over-reaching regulation that is flexible enough, without improperly impacting legal certainty, to be adapted to intensive data-driven business models. The LGPD puts Brazil on the map of countries that will probably provide an adequate region for processing personal data when it enters into effect, which in August 2020. If an organisation needs to build a global privacy program that encompasses both the EU and Brazil, a benchmark with the differences and similarities between the two regulations is necessary. This is the main purpose of the GDPR v. LGPD Report.

It is also important to bear in mind that the gap between the two regulations can increase or decrease according to events that might take place in the near future. Therefore, it is necessary to take a closer look at them.

Firstly, even though the LGPD created a national data protection authority, it still needs to be established, and the five directors need to be appointed by the presidency. Preferably this should happen within a timeframe long enough for the authority to provide guidance to organisations still in process of compliance with the regulation.

Secondly, guidance should be provided on topics such as:

- when data protection officers do not need to be appointed;
- how legacy databases should treated in order for its processing to be deemed as lawful when LGPD enters into effect;
- if and when DPIAs are necessary, such as when the processing relies on the legitimate interest of the controller; and
- limitations to data subjects rights, since the LGPD does not differ how they should be handled according to the legal basis in place.

All of these should be addressed before August 2020 in order to help organisations with their efforts to comply with the LGPD.

Lastly, it needs to be considered whether or not an organisation should observe the decisions and orientations provided by EU authorities and supervisory authorities to guide their interpretation of the LGPD, or if Brazil will provide its own view of similar cases and innovate on the application of data protection principles and rules.

In the end, the LGPD and the GDPR will continue to be aligned, since the EU has been effective on exporting its data protection models to the world. However, the differences are big and the fact that Brazil is still in its infancy when it comes to privacy culture maturity, it may prove that its regulatory delay can be a force to promote innovation and protection within the data driven world. Only time will tell.

To read the latest issue of the report by OneTrust DataGuidance and Baptista Luz Advogados, request a free trial or sign-in to the OneTrust DataGuidance Platform.

OPINION

Ukraine: The rights to deceased individuals' data

At the time of publication, there is no legislation specific for the personal data of a deceased person in the Ukraine. However, with more and more concerns around this topic, questions are being raised as to what protections there should be in place for deceased individuals' personal data. Olga Belyakov and Mykola Heletiy, from CMS Cameron McKenna Nabarro Olswang, discuss the current legislation that exists in the Ukraine concerning the rights to deceased individuals' data, and why the protection of this data needs to be considered.

Presently, with high-speed internet and social media platforms spreading all over the world, data has become the most valuable resource of the 21st Century, and online personal data is now an object that can be transferred, disposed of, and accessed without authorisation by hackers.

New rules and regulations aimed at protecting personal data have been adopted in recent years. The rules and regulations for the living are more or less straightforward, but what is the status of that data when we die?

Like most countries, Ukraine has no laws protecting the personal data of the deceased. After all, if a person is dead, whom does it harm?

Why protect the personal data of the deceased?

Personal data often includes highly personal and sensitive information, such as health records. Since disclosing such data could harm patients while they are still alive, people might be reluctant to receive adequate healthcare if their records can be accessed and disclosed upon their death.

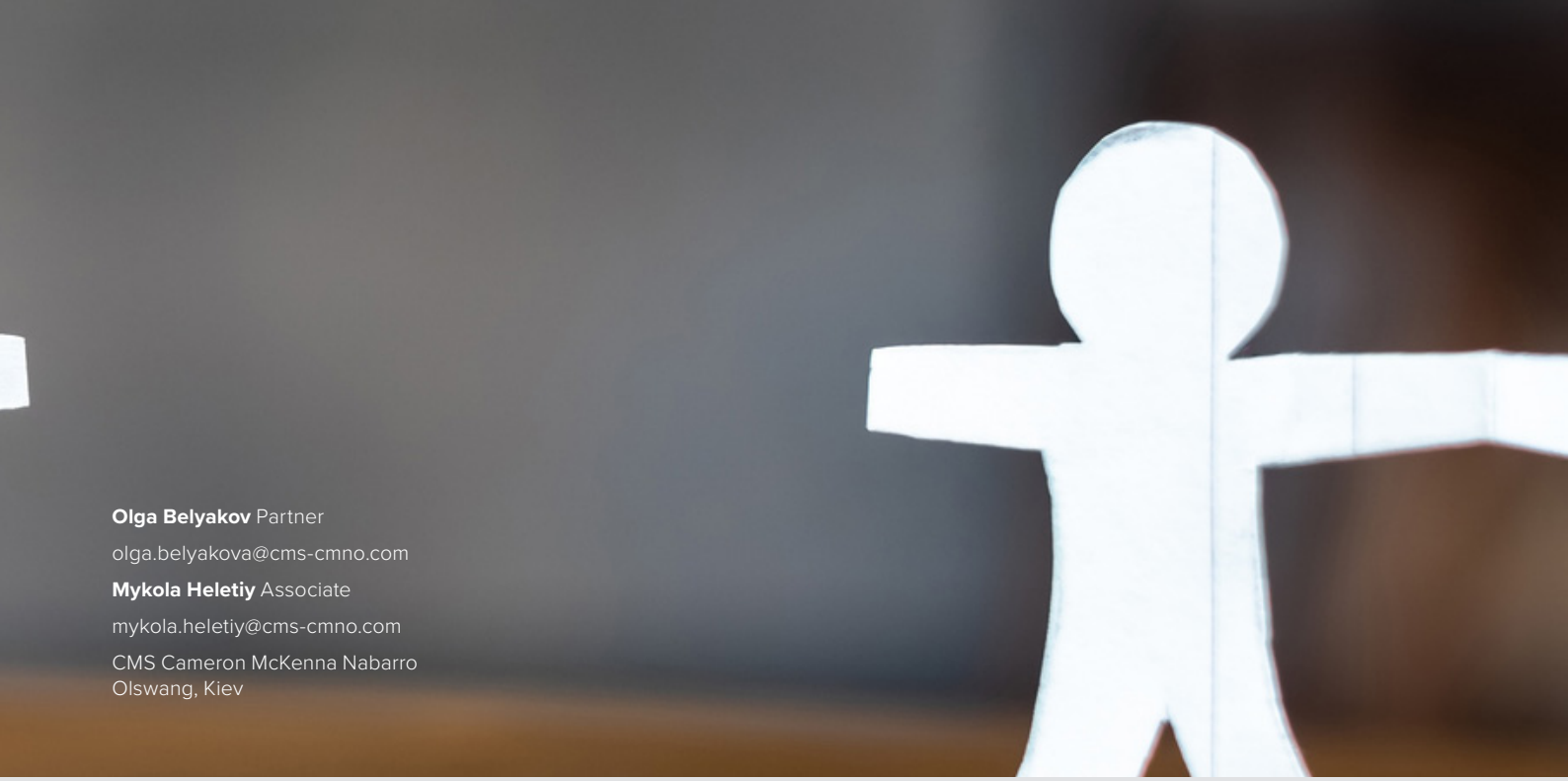
Disclosure of such data may also cause harm after a person's death. An example given under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') is haemophilia. If a father suffered from it, his living son could be afflicted as well, therefore the release of medical information after a father's death could impact the privacy of a surviving child.

There have also been countless disputes over the morality of digital deaths in social media, and the question, 'what should happen to the data in a social media account after the death of its owner?' Should heirs have the right to access the social media accounts of dead relatives, should this data be a part of an heir's inherited property, and if not, how should this data be disposed of?

The rules in Ukraine

Ukrainian personal data regulations do not provide special provisions for the processing of the personal data of deceased persons. The words 'living' or 'deceased' do not even appear in the national data protection laws.

Several examples touching upon this subject can be found in some non-sector specific regulations. For example, the Ukrainian tax authorities process the data (including personal data) of taxpayers and store it in the state register for the whole lifetime of an individual, and also for 75 years after their death.



Olga Belyakov Partner
olga.belyakova@cms-cmno.com
Mykola Heletiy Associate
mykola.heletiy@cms-cmno.com
CMS Cameron McKenna Nabarro Olswang, Kiev

In its turn, the Human Rights Ombudsman of Ukraine ('the Ombudsman') takes the position that Ukrainian data protections laws do not cover dead individuals for the simple reason that under Ukrainian law, deceased persons are not legally considered natural persons.

The Law of 1 June 2010 No. 2297-VI on Personal Data Protection (as amended) ('the Law') identifies personal data as any information about a natural person that is identified or could be identified. The Law makes no direct distinction between deceased or living individuals.

Furthermore, under the Civil Code of Ukraine, a natural person is considered to be an individual with civil capacity, which is defined as a person from the moment of birth until death. Hence, information relating to dead individuals is in principle not considered personal data, subject to the current personal data protection framework. The Ombudsman confirmed this position in a recent official response letter.

Case law has been of little help in resolving these questions. Relevant court cases that have specifically clarified what should happen to the data of a deceased person after their death are, unfortunately, not publicly available. What is more, questions concerning deceased people and personal data are not commonly studied in detail by the courts. For this reason, there have been decisions where a court indirectly recognised the persistence of personal data rights after death and other decisions where the court took a different position.

Therefore, the issue of a deceased individual's personal data is far from being clear and settled from a legal and regulatory perspective. The personal data of the deceased, however, can still receive some protection in Ukraine.

The data of deceased individuals at a legal-conceptual level can refer to various areas, including not only personal data, but also confidential information, defamation cases, and so on.

The protection of the confidentiality of information, data privacy, of a deceased person is one of the principles of the Law of Ukraine of July 10, 2003 No. 1102-IV On the Burial and Funeral, which guarantees the protection of a deceased person's confidential information, including:

- nationality;
- education;
- marital status;
- religious beliefs;
- state of health;
- address; and
- the date and place of birth.

Although confidential information is not the same as personal data, most of the confidential information listed here may be considered personal data under certain circumstances. As a result, the legal conception of data privacy offers arguments for the protection of the deceased's personal data within the current data privacy framework.

There are also some other legal rules, such as doctor-patient confidentiality that could protect a deceased person's privacy, including their personal data. In addition to laws, the online privacy of deceased individuals is also regulated by the internal rules of the major social media market players.

Another form of protection for the non-commercial interests of the deceased derives from the legal rights of family members to bring claims, essentially defamation claims, before the courts for the protection of the public image and dignity of dead relatives. In practice, such cases might include the protection of the deceased individual's personal data if such data was misused.

In short, while the current Ukrainian data protection provisions do not legally recognise the protection of a deceased individual's personal data, there are a number of legal mechanisms which, despite being limited in scope, offer some post-mortem protection.

USA: BIPA Facebook class action decision "distinguised due to level of biometric collection involved"

The U.S. Court of Appeals for the Ninth Circuit ('the Ninth Circuit Court') affirmed, on 8 August 2019, in Nimesh Patel et al v. Facebook, Inc. ('the Decision'), the decision of a district court on the certification of a class of plaintiffs who alleged that Facebook's facial recognition technology violated the Illinois Biometric Information Privacy Act of 2008 ('BIPA').

The plaintiffs asserted that Facebook had violated Sections 15(a) and 15(b) of BIPA by collecting, using, and storing biometric identifiers from their photos without obtaining a written release or establishing a compliant retention schedule. Facebook, on the other hand, argued that the plaintiffs failed to demonstrate that they had suffered an injury-in-fact that is sufficiently concrete for purposes of standing.

Mary A. Smigielski, Partner at Lewis Brisbois Bisgaard & Smith LLP, told OneTrust DataGuidance, "The Decision can be distinguished due to the significant level of biometric collection involved and thus the level of alleged harm by Facebook [...] The Ninth Circuit Court describes the facial recognition technology as being able to obtain information that are 'detailed, encyclopaedic, and effortlessly compiled.' This is vastly different than technology that acquires an image of points on a person's finger, or even a fingerprint, particularly when the average person leaves their fingerprints on countless surfaces each day and the fingerprint technology typically cannot be reverse engineered [...] The 'harm' analysis is fact dependant, and [the facts of the Decision] are different from the average case, akin to Basset v. ABM Parking Services, Inc., where a company merely used technology that turned points on a finger into an algorithm that cannot be reverse engineered."

Further to the above, the Ninth Circuit Court addressed the question of whether the specific violations alleged actual harm or present a material risk of harm occurring from Facebook's facial recognition software. The Ninth Circuit Court noted that facial recognition is used for photo 'tag suggestions' which enables Facebook to extract geometric data points that make a face unique, such as the distance between the eyes, nose, and ears, to create a face signature. In addition, it stated that the technology then compares the face signature to faces in Facebook's database of user face templates, which are face signatures that have already been matched to the user's profile. If these match, Facebook may suggest tagging the person in the photo. Lauren Steinhaeuser, Attorney at Faegre Baker Daniels LLP, told OneTrust DataGuidance, "The Ninth Circuit Court found that violations of BIPA's statutory requirements 'amounted to a violation of [plaintiffs'] substantive privacy rights,' and, therefore, they 'suffered a concrete injury' sufficient to confer standing under Article III of the U.S. Constitution. The Ninth Circuit Court's decision that a procedural violation of BIPA may be sufficient to confer standing is key for businesses, as it suggests liability in the absence of any actual harm to the individual."

> *"The Ninth Circuit Court's decision that a procedural violation of BIPA may be sufficient to confer standing is key for businesses"*

The Ninth Circuit Court outlined that requirements under Section 15 of BIPA include establishing a retention schedule as well as guidelines for permanently destroying biometric identifiers and biometric information. In addition, it stipulated that businesses must notify the individual in writing and secure a written release before obtaining a biometric identifier. Finally, the Ninth Circuit Court noted that businesses should be aware that in case of a violation of a regulation, BIPA also provides for actual and liquidated damages.

Steinhaeuser added, "Facebook argued that, because its collection of biometric data and its creation of face templates occurred on servers outside of Illinois, alleged violations of BIPA would have occurred outside of Illinois, and, therefore, each plaintiff would have to provide individual proof that alleged events occurred in the state such that common issues would not predominate. The Ninth Circuit Court disagreed with Facebook [and] inferred that the Illinois Government had expected that BIPA would apply to individuals who are located in Illinois, even if some relevant activities occurred outside of the state. Nevertheless, the Ninth Circuit Court did recognise that future decisions or circumstances may lead the district court to determine that individual cases may be appropriate, at which time the district court could de-certify the class."

Lea Busch Privacy Analyst
lea.busch@dataguidance.com

OneTrust DataGuidance

EU: CJEU judgment in Fashion ID applies "to any website deploying third party cookies"

The Court of Justice of the European Union ('CJEU') issued, on 29 July 2019, its judgement ('the Judgment') in Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV (C-40/17), addressing a dispute concerning the insertion by Fashion ID of Facebook Ireland Ltd.'s 'Like' button on its website through a plug-in, allowing users' personal data, such as IP addresses and browser history, to be transferred to Facebook regardless of whether the user clicked on the 'Like' button.

Eduardo Ustaran, Partner at Hogan Lovells International LLP, told OneTrust DataGuidance, "The CJEU's views in this case go beyond the use of plug-ins and will apply to any website deploying third party cookies, since the website operator becomes a joint controller with the third party for the processing of personal data, which provides a commercial advantage to both parties. [As a consequence], website operators incorporating third party cookies shall ensure that the responsibilities as joint controllers under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') are contractually apportioned, explain how the collected data will be used in the privacy notice and consider which lawful ground applies [for the processing]."

"[...] Website operators will necessarily be responsible under Article 26 of the GDPR for providing notice to users, and obtaining their consent."

In particular, the Judgment responds to the Düsseldorf Higher Regional Court's request for a preliminary ruling in relation to the interpretation of certain provisions of the Data Protection Directive 95/46/EC ('the Data Protection Directive'), and states, among other things, that Fashion ID can be considered to be a joint controller with Facebook in respect of the collection and disclosure by transmission of data to the latter, because Fashion ID and Facebook jointly determine the means and purposes of those operations. Furthermore, the Judgment outlines that Fashion ID cannot be considered to be a controller in respect of the operations involving the processing of data carried out by Facebook after such data had been transmitted to it.

Dr. Carlo Piltz, Attorney at Law at Reuschlaw Legal Consultants, commented, "The derived principles [from the Judgement] will almost be completely transferrable to the actual legal situation under the GDPR, since the regulatory content of the Data Protection Directive and the GDPR are similar. [In addition], when the Proposal for a Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ('the Draft ePrivacy Regulation') enters into force, the individual legal conditions each Member State introduced in order to comply with the Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) ('ePrivacy Directive') will be harmonised and will take immediate legal effect [...]. [In turn this will resolve] the actual discrepancies with regard to the compliant adaptation of the ePrivacy Directive [...], since many Member States have different solutions for cookies such as an opt-in or an opt-out solution."

Furthermore, the Judgment highlights that the existence of joint liability between the website administrator and the third party does not necessarily imply equal responsibility of the operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of processing of personal data and to different degrees, with the result that the level of liability of each operator must be assessed with regard to the relevant circumstances of the particular case.

Claire François, Counsel at Hunton Andrews Kurth LLP, noted, "Article 26 of the GDPR requires joint controllers to enter into an agreement to determine their respective responsibilities for compliance with obligations under the GDPR. In practice, this means that website operators, as joint controllers, will need to enter into such an agreement with the provider of the social plug-in to determine, [among other things], who shall provide notice to users, obtain their prior consent, handle users' requests for the exercise of their data protection rights, and notify the competent supervisory authority and affected users in the event of a data breach. For these reasons, website operators will necessarily be responsible under Article 26 of the GDPR for providing notice to users, and obtaining their consent (where required), while the third party provider could be responsible for, e.g. handling users' requests, to the extent that the operator of the website does not have access to the data."

Matteo Quartieri Privacy Analyst
matteo.quartieri@dataguidance.com
OneTrust DataGuidance

To read more in-depth news stories written by the OneTrust DataGuidance team request free trial access or sign-in to the OneTrust DataGuidance Platform.

Australia: Parliament passes consumer data right bill

The Parliament of Australia passed, on 1 August 2019, the Treasury Laws Amendment (Consumer Data Right) Bill 2019 ('the Bill'), which amends the Competition and Consumer Act 2010, the Australian Information Commissioner Act 2010, and the Privacy Act 1988 ('the Privacy Act'), to introduce a data portability right for consumers in the form of a consumer data right ('CDR').

In particular, the Bill, which currently applies to the banking sector and will soon apply to the energy and telecommunication sectors, allows individuals and businesses to access specified data related to them and held by businesses, as well as authorises secure access to this data by accredited third parties.

The Bill's explanatory memorandum ('EM') notes that the CDR gives consumers more control, by allowing them to access information about themselves and their use of goods and services, which enables consumers to fairly harvest the value of their data. In addition, the Bill requires businesses to provide public access to data on product terms and conditions, transactions and usage, as well as empowers consumers to direct businesses to share their data in a CDR compliant format with other accredited service providers.

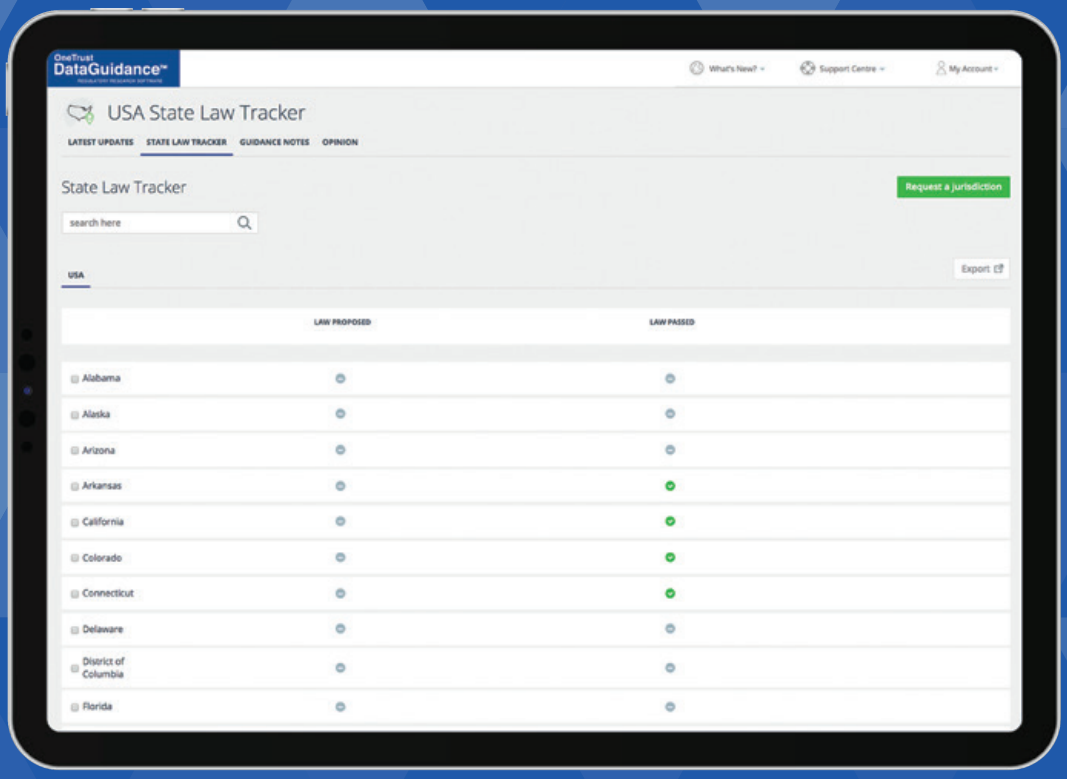
Moreover, whilst the Privacy Act gives consumers a right to access data about themselves, the CDR has a wider scope as it also provides access to data for individual consumers, business consumers, and on data relating to products. Furthermore, the CDR contains enhanced privacy safeguards to protect CDR data relating to an identifiable CDR consumer, including information not covered by the Privacy Act, as well as establishes a mandatory requirement for accredited data recipients and designated gateways to notify data breaches to the Office of the Australian Information Commissioner ('OAIC'). In addition, the Bill empowers the Australian Competition and Consumer Commission to grant accreditation to organisations and to jointly regulate this regime with the OAIC. The Bill also establishes a Data Standards Chair, which is charged with the duty to create standards consistent with consumer data rules.

The EM highlights the impact the CDR will have on businesses, predicting that compliance costs for accredited organisations in the banking sector will increase by AUD 86.6 million (approx. €52.6 million) per year and by AUD 9.9 million (approx. €6 million) per year for the energy sector. The EM states that the Government of Australia has committed to applying the CDR to the telecommunications sector and eventually across the whole economy, and the impact for other sectors will be considered on a case-by-case basis.

Tooba Kazmi Privacy Analyst
tooba.kazmi@dataguidance.com

OneTrust DataGuidance

NEW: USA State Law Tracker



Track and understand legislative developments with the USA State Law Tracker. Monitor privacy bills introduced and passed within every state, as well as relevant news and opinions provided by our in-house team of analysts and network of experts.

Use the tracker to:

- Stay notified of the latest updates on US privacy bills
- Compare privacy laws across multiple US jurisdictions
- Understand the requirements of key privacy laws within various states, including requirements on financial data, health data, employment data and privacy notices

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

OneTrust
DataGuidance™
REGULATORY RESEARCH 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