

Volume 1, Issue 5

November 2019

dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

Emerging Tech

OneTrust DataGuidance partners with Ashurst for Episode 3 of the series

6

Peter Fleischer

on how machine learning and artificial intelligence can be approached

14

CNIL's priorities

Erik Boucher discusses what the French data protection authority is looking at over the next 12 months

26

THE PRACTICALITIES OF ENFORCEMENT UNDER THE GDPR

Eduardo Ustaran considers enforcement under the GDPR and the key questions regarding regulators' approach 4

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



Julia Bonder-Le Berre, Hewlett Packard Enterprise

Julia Bonder-Le Berre is an attorney at law with an extensive experience in advising international organizations on privacy and data protection. Julia joined Hewlett Packard Enterprise (HPE) as a Senior Privacy Counsel in early 2017. In this role she has been focused on developing HPE global privacy and data governance program to ensure on-going compliance with the GDPR and other data protection laws around the world. Passionate about privacy by design, Julia enables business units and global functions to design privacy into HPE products, services and business operations.
julia.bonder-le-berre@hpe.com



Erik Boucher, CNIL

Erik Boucher is an IT expert the French data protection authority ('CNIL'). With 20 years of experience in software development, quality and security management, he is involved in the compliance checking of data processings subject to authorisation or control by the CNIL. He also participates in the development of the various tools proposed by the CNIL to carry out GDPR Privacy Impact Assessments and regularly hosts training sessions on this subject. He takes part in several working groups in charge of defining privacy and security standards for the French health sector (hospital IT, health data hosting, telemedicine systems and connected objects) as well as international standards (ISO/IEC) for privacy management.



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



Tara Waters, Ashurst

Tara Waters is a partner in Ashurst's Corporate team and Co-CEO of Ashurst Digital Ventures. She advises on US and UK law for a wide range of corporate and financing transactions, with a particular focus on the technology sector. Tara leads Ashurst's high growth & VC team in London and is a key member of the firm's fintech and distributed ledger technology & crypto asset practices. In her role as Co-CEO of Ashurst Digital Ventures, Tara is responsible for the firm's in-house development and investment arm of Ashurst Advance, providing innovative technology-led solutions to clients.
tara.waters@ashurst.com



Peter Fleisher, Google

Peter has worked as Google's Global Privacy Counsel since 2006. Based in Europe, Peter is Google's longest serving privacy leader. He counsels Google teams on how to design privacy sensitive and legally compliant products. Peter has designed many of Google's privacy compliance programs. He has met with thousands of privacy officials and leaders worldwide. Peter has managed scores of regulatory actions around the world, and appeared before some of the world's highest courts.

Image production credits

Cover / page 4 image: teekid / Signature collection / istockphoto.com
Page 9 image: Lokibaho / Signature collection / istockphoto.com
Page 10 image: MicroStockHub / Signature collection / istockphoto.com
Page 14 image: ayagiz / Signature collection / istockphoto.com
Page 22-23 image: bluejayphoto / Essentials collection / istockphoto.com
Page 28-29 image: Jason Leung / unsplash.com
Page 32 image: NASA / unsplash.com
Page 33 image: seb_ra / Essentials collection / istockphoto.com
Page 34 image: inho Lee / Signature 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 Limited. All Rights Reserved. Publication in whole or in part in any medium, electronic or otherwise, without written permission is strictly prohibited. ISSN 2398-9955

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, Lily Davies, Lucian-Gabriel Burcea

CONTENTS

4	The practicalities of enforcement under the GDPR
6	Emerging Tech: Blockchain and data privacy: an uneasy coexistence?
9	International: Five points for handling data breaches
10	EU: What a difference a Brexit deal makes
12	Thought Leaders in Privacy: Julia Bonder-Le Berre
14	Bahrain: New data protection law and its impact on businesses
18	Privacy Talks: Peter Fleischer, Google
21	Key takeaways: New Portuguese Data Protection Act v. GDPR
22	California: CCPA proposed regulations and more
26	Regulator Spotlight: Erik Boucher
28	France: The CNIL's new cookie guidelines and their impact on digital marketing
32	News in Brief

EDITORIAL



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

"Ultimately, and as the GDPR puts it, fines need to be effective, proportionate and dissuasive, so getting the practicalities right will take time."

Enforcement is happening (you just need to be patient)

There appears to be an increasingly popular view across social media that enforcement under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') is not happening. A recent opinion piece published in *The Guardian* went on as far as saying that the GDPR was failing us and our children, and it suggested that privacy regulators were pretty much powerless. Even Edward Snowden has chipped in and said that the GDPR will remain a 'paper tiger' until internet giants are hit with big fines. There is a real obsession with fines – or the lack of them, and even when they happen, they are never quite big enough for some.

In reality, privacy enforcement is not about fines – at least, not only about fines. It has never been, and it will never be. Fines are an important tool at the regulators' disposal to help achieve legal compliance. Regulators are very aware of this responsibility and they have acknowledged their duty to use a considered and balanced approach in their use of fines. Regulators do not necessarily see fines as a last resort, but they are wary of using them in a way that would devalue their effectiveness as a tool. For that reason, European data protection authorities are more likely to consider sanctions in the context of their wider corrective powers that the law gives them.

So far, the biggest GDPR fines announced – in the hundreds of millions of pounds – have come from the UK Information Commissioner's Office ('ICO'). The ICO approaches its duties in a very managerial fashion, as illustrated by its Regulatory Action Policy ('the Policy'), which sets out the rationale for the use of the various powers available to the regulator. The Policy starts by explaining the objectives of regulatory action, which include responding to breaches of the law as well as promoting compliance. The Policy goes on to list all of the possible regulatory activities that may be undertaken. This includes enough items to fill two pages, which shows the many different actions that the ICO may take. Crucially, the ICO's Policy defends adopting a selective approach to regulatory action, so that different breaches can be dealt with using different tools taking into account aggravating and mitigating factors.

The overall message is that we should trust the regulator to exercise its discretion in the manner in

which different situations are dealt with, taking into account the ultimate purpose of regulatory activity – even if those actions do not mean imposing fines. In any event, regulators are not shying away from issuing fines either. As demonstrated by the work being carried out by German data protection authorities, they are just learning to do it properly. A new and sophisticated methodology is in the process of being implemented to put theory into practice. This step-by-step approach looks at the size of the organisation and its value, the severity of the breach and the specific circumstances of a given case to decide the correct amount in an almost mathematical way. As with GDPR compliance itself, practice will make perfect, but this is an ongoing process that has barely started. Ultimately, and as the GDPR puts it, fines need to be effective, proportionate and dissuasive, so getting the practicalities right will take time.

The fundamental question is not whether enforcement will happen or not. It is happening – as evidenced by the various enforcement trackers available – and will undoubtedly continue to happen. The key issue is what type of enforcement will achieve the desired policy objective: the protection of fundamental rights and freedoms of individuals and their right to the protection of personal data. The carrot v. stick dilemma is not new. What is new is the significance of compliance v. non-compliance. Being responsible when handling personal data is essential to protect humanity. That does not mean that breaking the law needs to attract the most severe penalties as a matter of fact. It means that regulators must think more carefully than ever about what attitudes they adopt and what enforcement actions they choose.

Emerging Tech

Episode 3

Tara Waters Partner
tara.waters@ashurst.com

Gita Shivarattan Counsel
gita.shivarattan@ashurst.com

Ashurst LLP, London

OneTrust DataGuidance have partnered with Ashurst LLP to present Emerging Tech, a four-part series of articles and videos on the data protection issues relating to novel forms of technology. Alexis Katefides was joined by Tara Waters and Gita Shivarattan, from Ashurst, for the third instalment of the series. They introduce some of the key issues users should consider when working with blockchain, particularly its coexistence with data privacy law.

Introduction

Heralded as the great disrupter across hyperbolic headlines over the recent years, some may say that blockchain, or more correctly, distributed ledger technology, has underwhelmingly failed to deliver on its promise. Opinions on blockchain are often emotionally charged and divisive. However, most would agree that its benefits remain elusive and enigmatic for the everyday person.

Those actively working with blockchain still hold out hope, although the practical challenges of mass adoption remain many. One of the key challenges that blockchain faces is the conundrum of how a technology which purports to store data permanently and immutably can exist in a world of increasing regulatory obligations relating to data, particularly those dictating its amendment, correction, and deletion.

Can these seemingly irreconcilable concepts be reconciled? In the third part of the Emerging Tech Series, we consider the question of the coexistence of blockchain and data privacy law.

What is blockchain?

Blockchain is a technology that enables the secure validation, recording, and sharing of data. The data is stored in a distributed database, meaning there is not one centralised database controlled by a single person, but rather multiple copies of the database which are continuously updated in real time across the network of participants. Not

only does this eliminate one single point of failure risk, but it also makes tampering with the data a significantly more onerous task, as a person would need to tamper with all copies of the data near simultaneously.

The emergence of blockchain is considered notable, if not revolutionary, due to manner in which the technologies underpinning it, none of which are new, are used together to allow parties to transact directly with one another without the need for a trusted third-party intermediary, and for data relating to that transaction to be stored in an extremely secure manner.

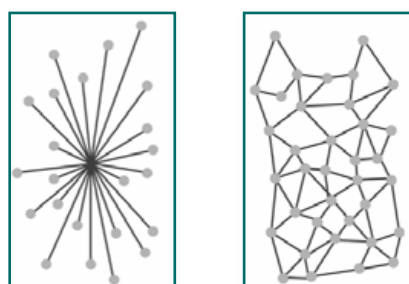


Figure 1: Centralised and distributed databases

Fundamental to this security are various cryptographic methods that:

- firstly, convert the data into a coded form, which is referred to as a hash, that bears no resemblance to the original data;
- secondly, are designed such that the hash cannot be reverse-engineered, meaning it can only be decoded by guessing the

underlying original data; and

- thirdly, store hashes in a manner which enables a user to easily confirm whether any of the original underlying data or hashes have been tampered with. This enables a user to trust the integrity of the data once stored, without necessarily having to trust its counterparts.

One of the key features of blockchain is its purported immutability, meaning that data stored in a blockchain-based database cannot be subsequently altered. Technically, this is not exactly correct, but because the hashes cannot be reverse-engineered that means it would generally require more computing power than is commercially available at present to not only guess, over and over, what the underlying data is, but to also then make the relevant changes across all copies of the database in the network as near to simultaneously as possible.

Moreover, blockchain networks implement specific rules, known as consensus protocols, most of which are designed to ensure that a single actor cannot unilaterally effect changes to the data. This is particularly true for widely distributed networks, such as the Bitcoin network and the Ethereum network, which were the first networks to be formed.

As participants in a blockchain network are working together to operate the network, there are limited incentives for those participants to join forces to enable tampering with the data.

For all of the above reasons, blockchain-based databases are considered to be one of the most secure means of recording information.

simplistic view. The truth is that there are many types of distributed networks that implement blockchain technology in a variety of ways.

across the network. This would involve the participants in the private network encoding specific rules for amending the database in



Figure 2: Blockchain

Blockchain and data privacy

The fallacy of immutability

The immutability of blockchain is often held out as antithetical to data privacy laws, such as the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), that empower data subjects to have control over their personal data, including how it is collected and stored, and dictates that persons collecting and storing such data must agree to hand over, correct, and delete that data on request. In addition to the data subject rights, the GDPR also contains a principle on data minimisation, whereby organisations should only process personal data that is relevant and necessary for the defined purpose, and the principle of storage limitation, whereby organisations should only keep personal data for as long as necessary for the purposes for which it was collected. Both of these principles result in an obligation on the organisation that collected the data to either delete or anonymise any personal data once it is no longer necessary for the purpose.

However, focussing exclusively on the immutability of blockchain is an over-

Therefore, understanding whether a particular network is data privacy compatible requires a case-by-case analysis. And, it is possible that technological mechanisms can be built into the blockchain network and relevant consensus protocol to facilitate regulatory compliance.

Public vs. private blockchain

At the highest level, there are two type of blockchain networks: public and private. Public networks can be accessed by anyone and typically utilise consensus protocols that make modification of data near impossible. Private networks are limited to invited participants, and thus are more likely to apply consensus protocols that are more flexible in terms of enabling modifications.

In a private network context with a limited number of participants and other active users, it may be deemed appropriate, subject to the consensus protocol, to allow the computing power of the network to be used to enable the amendment of the database such that the relevant hashes are updated

certain agreedcircumstances, which can be affected if the agreed consensus protocol threshold for those amendments is met.

Can hashed data be personal data?

Another threshold question when considering the compatibility of blockchain with data privacy is whether personal data stored in hash form would meet the definition of 'personal data' under applicable data privacy legislation.

In the EU, the answer to this question hinges on whether hashing the input data achieves anonymisation, which is not covered by data privacy laws, or only pseudonymisation, which is covered by data privacy laws, of that personal data. The Article 29 Working Party, in Opinion 05/2014 on Anonymisation Techniques, provided guidance that anonymisation, 'results from processing personal data in order to irreversibly prevent identification.'

The GDPR defines pseudonymisation as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use

In public/permissionless networks:	In private/permissioned networks:
<ul style="list-style-type: none"> anyone can: <ul style="list-style-type: none"> view the information on the ledger; submit information to be recorded on the ledger; and host the ledger; participants are more likely to participate pseudonymously; control is more likely to be fully decentralised; there is an increased risk that a network participant may have malicious intent; and there is a decreased risk that a network participant would have the computing power to carry out an effective attack. 	<ul style="list-style-type: none"> participants pre-selected or subjected to specified participation criteria or approval by an administrator (group); control is likely to be more concentrated amongst certain participants or an administrator (group); it is more likely to only be accessible by participants (but could be made available to the public or specific external entities); it is expected to be more commonly adopted where recording sensitive/private information; there is an increased risk if a participant has malicious intent because also more likely to have greater computing power vis-à-vis the network; and there is a lower incentivisation to abuse any computing power.

Figure 3: Public v. Private networks



of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.¹

If a hash of personal data cannot be reverse engineered but only guessed by chance, does the hash function irreversibly prevent identifying the data subject by reference to that hash? The above guidance and definitions are not entirely helpful. Provided it remains possible to identify the underlying input data, then under the GDPR hashing results in pseudonymisation and not anonymisation. However, at the time of publication, this remains untested.

It is worth noting, however, that the GDPR clearly supports pseudonymisation as a security measure and risk mitigation technique and, therefore, there is a good argument that blockchain is a 'Privacy by Design and Privacy by Default' technology.

Options to avoid storing personal data on blockchain

It may be decided that any personal data is not stored in the blockchain network, but somewhere off-chain, to make regulatory compliance more straightforward and to avoid complicating the operation of the network. Utilising separate off-chain databases to store private information, not just personal data, is not uncommon. However, data

privacy laws will apply to the collection and storage of that data, even if in an encrypted or pseudonymised form. It also follows that storing personal data in a single location may be more vulnerable to breach as well.

Controllers and processors

Under the GDPR, organisations that are processing personal data are categorised as either a controller, therefore they are deciding the means and purposes of the processing, or a processor, as they are only undertaking processing on behalf of a controller and under the controller's instructions. If the entry in a block contains personal data, participants may be acting as both a controller as they are writing on the chain, and miners acting as processors, in validating the entry. As a result, careful analysis is required to determine the roles of participants as controllers or processors on a case by case basis. The French data protection authority ('CNIL'), has released guidance in which it sets out an assessment of when blockchain participants are acting as data controllers and processors, which is a useful reference when assessing these roles.

The terms and conditions for participation in the blockchain will need to accurately identify the roles of the parties and allocate responsibility for issuing fair processing notices, responding to data subject requests, handling data breaches, Article 28 of the GDPR processor clauses, and liability.

Data Protection Impact Assessments

Prior to setting up a blockchain or entering into one, organisations should undertake a Data Protection Impact Assessment to help identify potential risks in respect of the technology and solution.

Conclusion

If blockchain and data privacy are not irreconcilable, can they coexist? Hopefully, the above makes clear that there are several considerations when seeking to understand how a blockchain network must be set-up and operated in order to enable regulatory compliance. By design, certain types of networks, such as public networks, are less compatible with data privacy principles, but compliance is still possible.

However, the trade-off when implementing a consensus protocol that allows for the editing and deletion of data may be that the network is more readily interfered with by a single actor or group of actors. Ultimately, though, to achieve compliance enabling such measures will be necessary.

So, there may remain an uneasy coexistence until such time as regulators provide more clarity about how to implement blockchain in a fully compliant manner. Whether that clarity will be forthcoming remains to be seen.

Watch Episode 3 of the Emerging Tech series on the OneTrust DataGuidance Platform.

For further video content produced by OneTrust DataGuidance, visit the OneTrust DataGuidance Video Hub.

1. Available at: <https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf>

International: Five points for handling data breaches

A data breach within a company involves the unauthorised release of sensitive or private data, and can be the result of inadequate security or a cyberattack. Jeffrey Lim, Director at Joyce A. Tan & Partners LLC, provides a recommendation of the steps that should be taken in the event of a data breach, and how companies can mitigate risks by preparing for such an incident.

Introduction

A popular modern nightmare scenario goes something like this: you are the data protection officer of company X, and cyberattackers have infiltrated your customer database. Financial and sensitive data have been extracted.

The storm is coming. Regulators will want to get into your records and your systems. Customers might want to get out. The media will want answers. Lawsuits may be looming over the horizon.

This article covers 5 points, distilled from experience, to help you think through what is needed in the thick of the storm.

One: Dealing with what you don't know yet

The discovery of data breaches is a forensic fact-finding process. Information will come in instalments and early intelligence may be wrong.

Establishing what actually happened takes time and professional care. The priorities will be to figure out what the scale of the breach is, whether there are false positives, what data has been compromised, and what is the likelihood or severity of harm.

Two: Speed of command, not chain of command

Establishing a crisis team, a reporting chain, and getting the right people involved – these are all crucial steps.

However, even with a chain of command established, it may be necessary to leapfrog a chain of command to get a quick resolution. Information may need to go up and across to all team members earlier rather than in sequence. When every minute counts, team members may need to be alerted, and be on standby.

Three: Own the remedy, if not the breach

In one particular breach, a team member in one organisation was reluctant to escalate information concerning a breach for

fear of the amount of the work that would ensue. He correctly anticipated the volume of work that followed, but the time lag in reporting that result certainly did not help.

He did not, in short, own the remedial steps entrusted to him.

Ownership also begins with management. One clear sign of ownership is whether you have made the effort to prepare your organisation in advance.

Four: What to say, when to say, and how to say it

Prematurely making disclosures only to have to double back and correct yourself can cause unintended complications down the road. Have you obtained sufficient certainty to give the statement you plan to make?

Giving some thought to when information can be released, and to whom, is important. Ask yourself:

- is the disclosure timely and on the right forum;
- have you considered your disclosure obligations to regulators;
- have you briefed to your management; and
- what other statements to stakeholders are needed?

Notices or harm-preventing disclosures to customers or affected individuals may be key. For example, telling someone to change their passwords in the wake of a freshly discovered breach in a timely manner may help prevent loss.

Also a big one: is your legal counsel involved, and does everyone understand what legal privilege means?

Legal privilege might have important variations in different countries but generally the idea is that certain disclosures to your legal counsel does not need to be disclosed. If anything, this should encourage early engagement of your legal advisers.

Five: Clean up begins even before you own up

Remediation is not something that has to wait for all the dust to settle. Taking risk mitigation steps or rectification early, even as a breach unfolds, may be an important mitigating factor to some regulators.

Steps that do not have to wait include:

- preserving evidence;
- shutting down and eliminating security vulnerabilities;
- recovering lost data;
- instituting an internal investigation; and
- planning for the next breach.

When the time comes to take responsibility in the proper forum, approaching it as a responsible organisation that did everything it could to make things right is often one saving grace you want to be able to point to.

Conclusion

Perhaps one of the most important principles to consider is one we have not discussed:

Do not wait for a breach to happen to be prepared.

Ask yourself:

- do you have a crisis team ready go into action;
- is every role in the team rostered;
- have you built a process flow in advance;
- do you have tools on hand; and
- have you kicked the proverbial tyres and road-tested scenarios?

Addressing these questions now, not when a breach is happening, will help you get through the storm.

Jeffrey Lim Director
jeffrey@joylaw.com

Joyce A. Tan & Partners LLC, Singapore

OPINION



Emma Drake Senior Associate

emma.drake@twobirds.com

Bird & Bird LLP

EU: What a difference a Brexit deal makes

The European Commission's ('the Commission') Task Force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 of the Treaty on European Union released, on 17 October 2019, a revised text of the Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom as agreed at negotiators' level ('the Revised Political Declaration'). Emma Drake, Senior Associate at Bird & Bird LLP, provides insight into how Brexit may affect data privacy in the UK, and what companies may want to plan for if the UK enters into a 'transition period.'

What is the current situation?

For many organisations, the focus of data protection preparation ahead of each delayed Brexit deadline had been on no-deal planning. This approach was supported not only by the general pessimism that any deal could be reached, but also by official guidance from governments and supervisory authorities, such as the Information Commissioner's Office ('ICO') and the French data protection authority. Now, as the UK heads to the polls following a promise made by UK Prime Minister, Boris Johnson, to Parliament that, 'one way or another, we will leave the EU with this deal,' many will need to refresh their memories of how the proposed withdrawal agreement ('the Current Withdrawal Agreement') will affect data processing and data flows.

What has changed on data protection in the Revised Withdrawal Agreement?

Since former Prime Minister Theresa May's deal, in short, nothing has changed. The Revised Political Declaration and the Current Withdrawal Agreement repeat word-for-word the commitments on personal data proposed in late 2018. Any previous planning done by your organisation for a Brexit based on the former withdrawal agreement can be dusted off and resurrected in the hope that the new British Government will push the Revised Withdrawal Agreement through Parliament following the election.

What do we need to do if the deal is agreed?

If a deal is formally approved, the UK will initially leave the EU once this is ratified and enter into a transition period. During this transition, the UK would be required to directly apply Union law, including the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), the Law No. 363/2018 transposing the EU Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) ('Law Enforcement Directive'), and the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) ('the ePrivacy Directive'), unless and until an adequacy decision is put in place by the Commission. The withdrawal agreement also ensures that the UK will be treated as a Member State under EU law for the same period.

This is with one substantial exception: the UK will be treated as a third country for the purposes of the GDPR's cooperation and consistency mechanisms during the transition period. This means that the UK will no longer be a member of the European Data Protection Board, and will no longer benefit from any one-stop shop arrangements. Potentially, organisations could see themselves subject to simultaneous action from both the ICO and EU supervisory authorities during transition. More positively, the effect of this transition is that:

- for the purposes of international transfers, the UK will be considered as a Member State until the end of transition or the implementation of an adequacy decision;

- UK organisations will not need to consider extra-territorial application of the GDPR until this no longer directly applies, including any requirement to appoint their own EU representative; and
- the GDPR remains the applicable law for UK organisations for this period, and there is a commitment that it will remain the applicable law for any data processed prior to the end of transition, unless and until an adequacy decision is in place.

Perhaps the major 'change' as compared to the position of last year is the length of transition will apply for. Despite over a year's worth of delay, transition remains set to end on 31 December 2020, just 11 months after the new Brexit deadline of 31 January 2020. This can be extended, but only with the consent of both parties, including parliamentary approval.

Is our no-deal data transfer planning wasted?

If your organisation has taken any steps to prepare for a no-deal, this is not wasted effort. There is no absolute guarantee that the new UK Parliament elected in December 2020 will be any more effective at passing the deal, although both major parties now back some form of deal-based Brexit. Even if the deal is ratified and implemented promptly, this is not the end of the road for an effective no-deal or no-adequacy Brexit. The Revised Political Declaration sets out a commitment from the EU to 'endeavour to adopt' an adequacy decision by the end of 2020, but there is no guarantee that this will be achieved in time for the UK's formal and final exit.

Similarly, other no-deal planning, such as revising contract precedents to anticipate the 'UK GDPR', moving representatives to other Member States, and inserting references to the UK in privacy notices, will remain useful for a final UK exit, even if the urgency of this may have seemingly reduced. In any event, until the shape of the new Parliament is known on 13 December, we cannot be certain that we will not be reliving the summer's no-deal concerns come Christmas.

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

To access more articles like this and further content from OneTrust DataGuidance, request free trial access or sign-in to the platform.

INTERVIEW



"we need to continuously assess these new laws and adjust our programme to them."

OneTrust DataGuidance spoke with Julia Bonder-Le Berre, Senior Privacy Counsel at Hewlett Packard Enterprise, at IAPP DPI: Deutschland in September 2019. Julia discusses the CCPA, its impact on global organisations and the future of US privacy law.

How is the CCPA and other new privacy laws impacting your organisation?

The California Consumer Privacy Act of 2018 ('CCPA') is an example of one of the privacy laws that are now emerging in different parts of the world. What we see now is that privacy laws follow the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') to some extent, but at

the same time they remain distinctive. I think what we can see is that there is an increased willingness to match GDPR standards in order to enhance the privacy and protection of personal data, to give individuals more rights, and to make organisations accountable for how they handle data.

On the other hand, we see material differences between new emerging laws and the GDPR, and it is interesting

INTERVIEW

continued



to see where they come from, the different legal regimes, and different cultures behind them, and even different understanding of what privacy is. So, for a global privacy programme like ours at Hewlett Packard Enterprise, it means we need to continuously assess these new laws and adjust our programme to them.

One of the challenges is to make sure that our global practices of handling personal data, which are part of our global business operation, remain aligned and manageable, whilst at the same time, enabling us to comply with those local differences.

What changes do you expect to see regarding the CCPA?

We are going through interesting times now observing how the CCPA is being shaped. Recently we saw the final text, but over the following years, we will see further developments. For instance, employees, temporary workers, and job applicants will be able to fully benefit from all the rights under the CCPA from 2021. When it comes to other amendments, my personal view would be to further work on the concept of the sale of data. As we see it now, it is very broad and it may go beyond what the legislators had in mind, in particular for companies which are not in the business of trading in data, and therefore, are not data brokers.

How do you see the US privacy landscape evolving and changing?

We see a lot of developments in the US when it comes to new privacy laws emerging, in particular in California and Nevada, with many other states to come. I think what is interesting to see is that if all the states legislate separately, and the privacy requirements are not fully aligned, which is inevitable in a situation like that, then that would create more challenges for organisations like ours which are based on global practices of handling personal data.

At the end of the day, we will need to assess all these differences, and we will need to incorporate them into our practices of handling personal data, even if just for the US market. In Europe, we dealt with privacy law fragmentation for many years. The GDPR has changed that and we now benefit from a more harmonised privacy framework. So, I think it would be welcomed if in the US, at Federal level, a similar harmonisation effect takes place. However, we know that it took Europe years to shape and legislate the GDPR, so the US may need to take a similar journey.

Which additional laws have you been closely monitoring?

We have recently been talking about privacy developments particularly in the US, but at the same time, there are many different laws emerging in all parts of the world, and it is not only now but that has been the case for many years.

Lately, for us, we have been busy with ensuring that we are compliant with the privacy law in Turkey. Data

protection law, and secondary regulation, closely follow the European data protection regime. However, there are some differences, for instance, when it comes to the legal bases for the processing of data, or international data transfers, or registrations with the regulators.

So, things are similar, but at the end of the day, you really need to go into detail, assess those differences, and see how you can manage them, either as part of your global privacy operations, or just to limit it to local handling of personal data.

Apart from looking into US, looking into Europe, and countries around Europe, our business is also looking into what is going on in Asia, particularly in China and in India. These are the markets where we have significant business operations, so it is important for us to make sure we know what is happening there and we can comply with those regulations. I think what is helpful for us is that our global privacy programme is based on the GDPR, and that gives us a lot of comfort to comply with the majority of privacy laws that are now emerging.



Julia Bonder-Le Berre
Senior Privacy Counsel at
Hewlett Packard Enterprise

Julia'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 U.S. State Law Tracker on the OneTrust DataGuidance Platform.

For access to all cross-border charts, request a free trial or sign-in.

Gordon Wade Senior Data Privacy and Protection Lawyer
 gordon.wade@pwc.com
 PwC Legal Middle East, Dubai

Bahrain: New data protection law and its impact on businesses

On 1 August 2019, Law No. (30) of the Year 2018 Issuing a Law on the Protection of Personal Data ('the Law') entered into force. The Law is just the second national law in the Gulf region to directly address the right to personal data protection after Qatar¹, and it will soon be followed by other Gulf Cooperation Council States in the near future². Gordon Wade, Senior Data Privacy and Protection Lawyer at PwC Legal Middle East, explores some interesting features of the Law and provides insight into how the new legislation may shape the Bahrain business environment around privacy for companies in the future.

Introduction

Largely modelled on the Data Protection Directive (Directive 95/46/EC) ('the Data Protection Directive'), the Law speaks directly of an individual's right to the protection of their personal data and will strictly regulate the processing of personal data by 'data managers,' the Law's equivalent of 'data controllers.' The Law requires businesses to be accountable for their personal data processing activities, including ensuring that personal data is processed fairly and remains transparent with individuals when collecting their personal data. These

compliance requirements are supported by enforcement powers granted to the 'Personal Data Protection Authority' ('the Authority') on one hand, and financial and penal sanctions on the other. The Authority may impose a range of penalties on defaulting organisations, including:

- withdrawing any authorisation to process certain specialised categories of personal data;
- administrative penalties up to BHD 20,000 (approx. €47,940) per act of non-compliance; and/or
- daily financial penalties up to BHD

2,000 (approx. €4,794) per day.

There are a number of different violations, including unlawfully processing sensitive personal data or unlawfully transferring personal data outside of Bahrain, where the courts of Bahrain may also:

- impose a term of imprisonment not exceeding 1 year; and/or
- issue a fine up to BHD 20,000 (approx. €47,940).

Individuals also enjoy a direct right of action before the courts of Bahrain for

any damage arising out of the unlawful processing of their personal data.

Scope of the Law

As with the Data Protection Directive, and now with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), the Law contains provisions clarifying its material and geographical scope. Materially, the Law applies to:

- any processing of personal data wholly or partly by automated means; and
- any non-automated processing of personal data which is intended to form part of a filing system.

The Law also has a wide territorial scope, granting strong individual rights to every individual ('data owner') normally living or working in Bahrain. Therefore, the Law does not only provide rights for citizens of Bahrain, it also imposes compliance obligations on:

- every organisation that has a place of business in Bahrain; and
- people and businesses outside of Bahrain who collect the personal data of individuals residing there using means, such as technologies and equipment etc., available, unless those means merely enable the transfer of that personal data through Bahrain without the information being used for any other purpose.

Principles-based approach

The Law, similarly to the Data Protection Directive and the GDPR, adopts a principles-based (rather than rules-based) approach to personal data protection, consistent with international best practices, calling on organisations to, *inter alia*:

- only process personal data fairly, lawfully, and for clear and specific purposes;
- adhere to the principle of data minimisation;
- respect and enable the exercise of the individuals personal data rights (transparency);
- only store data for as long as required;
- protect personal data that is stored from unauthorised access; and
- take responsibility for personal data processing and compliance with the Law, and be able to demonstrate this compliance (accountability).

Like its European counterparts, the Law is intended to provide flexibility for the way organisations comply with its

requirements. For example, the data security controls that organisations are required to deploy are not mandated but can include such measures as 'an appropriate level of security, subject to state-of-the-art technological protection methods and the cost arising therefrom, the nature of the data being processed, and the risks that may arise from this processing³.' Similarly, as one of the exceptions to the general rule against transferring personal data outside of Bahrain, such transfers may occur where the data manager can provide 'sufficient guarantees regarding the protection of privacy as well as individuals' basic rights and liberties⁴.'

Any data protection law that adopts a principles-based approach recognises that data protection is inexorably linked to the evolution of technology. Data protection laws need to be flexible, dynamic, and able to evolve over time as technology changes. Therefore, whilst language deployed in the Law may appear somewhat 'woolly' at times, risking inconsistency of interpretation and a lack of legal certainty on what the Law requires, proscriptive laws can actually hinder data protection if they are too rigid. Indeed, one of the reasons why the GDPR exists now at all is because the Data Protection Directive was designed for a time before social media, wearable technology, connected cars, artificial intelligence, etc.

Lawful bases

Data managers may only process personal data either with the consent of the data owner, or under one of the alternative conditions set out in the Law, such as:

- for the purposes of executing a contract with the data owner;
- to take steps at the request of a data owner before entering into a contract;
- for the purposes of carrying out a legal obligation;
- to protect the best interests of the data owner; or
- for the legitimate interests of the data manager or any third party, unless this conflicts with the rights of the data owner.

The Authority

The Law states that the Authority shall be established, and that the 'Board of Directors' of the Authority will issue such decisions and resolutions for the implementation of the provisions of the Law. Perhaps somewhat unlike its European counterparts, the Authority is subject to the overarching control of the

Minister of Justice Affairs and Islamic Affairs ('the Minister'). In particular, the Authority must submit regular reports to the Minister about its activities and work progress. In return the Minister:

- may request that the Authority provides them with any details, information, documents, minutes, registers, or reports which would enable them to carry out their control of the Authority's functions; and
- shall assume the responsibility of monitoring the level of compliance by the Authority with the Law.

The general overarching role of the Authority is to assume responsibility of all the duties and powers necessary to protect personal data, including:

- ensuring public and data manager awareness of the rights and obligations, and spreading the 'culture of personal data protection';
- carrying out compliance inspections on organisations;
- receiving applications for prior authorisation before carrying out certain processing activities; and
- investigating complaints regarding contraventions of the Law.

In October 2019, Decree No. 78 of 2019 determining the Administrative Body entrusted with the tasks and Competences of Personal Data Protection Authority, was published and states that Ministry of Justice, Islamic Affairs and Awqaf ('the Ministry') will assume the responsibility of the duties and powers for the Authority until the financial budget for the Authority has been allocated within the overall budget of the State, and a Decree forming the Board of Directors is issued. The Minister is responsible for the duties and powers prescribed under the Law for the Authority's Board of Directors and the Chairman of the Board. The Undersecretary for Justice and Islamic Affairs will be responsible for the duties and powers prescribed under the Law for the Authority's Chief Executive Officer. It is also known that the Board of Directors will be made up of representatives from the Central Bank of Bahrain, the Telecommunications Regulatory Authority and the Bahrain Chamber of Commerce and Industry.

To date, no decisions or resolutions clarifying certain aspects of the Law, such as the rules and procedures that data managers must follow when processing sensitive personal data, and the terms and conditions that

OPINION

continued

the technical and organisational data security measures must satisfy, have been published. Therefore, at this point, it is not possible to be certain about how the Authority will interpret and apply the Law, nor exactly what form and content any further decisions, resolutions, or guidance will take.

Prior authorisation

As alluded to above, the Authority is responsible for receiving applications for prior authorisation from organisations before they can carry out certain personal data processing activities. Specifically, organisations must obtain the prior written authorisation of the Authority before they may engage in any of the following activities:

- automatic processing of sensitive personal data of persons who cannot provide consent;
- automatic processing of biometric data;
- automatic processing of genetic data (except for treatment by physicians/healthcare specialists);
- automatic processing that entails the connection of personal data files that are in the possession of two or more data managers that are processing personal data for different purposes; and
- processing that consists of visual recordings to be used for monitoring purposes.

Notwithstanding the above, all data managers must notify the Authority before beginning any automatic data processing activity unless:

- the organisations have appointed a 'data protection supervisory' (the equivalent of a data protection officer);
- the organisation is processing the data as an employer, therefore processing is necessary in order for the employer to fulfil its tasks and obligations to its employees under the Law;
- the processing is for the purposes

of maintaining a public register in accordance with the Law; or

- the organisation is processing the data as an association, syndicate, or other non-profit entity.

Processing of biometric data

The Law prohibits any automatic processing of biometric data used for identification purposes without the prior written authorisation of the Authority. The Law, unlike the GDPR⁵, does not provide a definition for biometric data. However, biometric data is generally seen to refer to personal data relating to physical, physiological, or behavioural characteristics that may be used to identify an individual. Common examples include fingerprints, facial recognition scans relying on facial geometry, iris scans, and voice recognition. It is envisaged that the precise rules and procedures that employers will have to follow in applying to the Authority for prior-authorisation will be issued in the form of a decision from the Authority. No such decision has been published to date. However, the Law does state that applications must be accompanied by the following information:

- the name and address of the data manager and of any data processor;
- the purpose of processing biometric data;
- a description of the biometric data, a list of the categories of data owners, as well as the recipients of the data or their categories;
- any intended transfer of the biometric data outside Bahrain; and
- a statement enabling the Authority to conduct a preliminary evaluation, considering the suitability of the data manager and data processor's available technical and organisational measures, to ensure the security and integrity of the biometric data.

The Authority will assess all applications and may require any applicant to remedy any perceived deficiency in

its application and/or the supporting information. Decisions on whether to grant or deny authorisation must be made by the Authority within 30 days of receiving an application. A failure by the Authority to respond within this will mean an implicit rejection of any request.

Given the now-widespread use of biometrics in the workplace, employers should pay special attention to the prior-authorisation requirements of the Law. This is particularly the case given that the default position for any application not responded to is a rejection of that application, reflecting the particular sensitivity of biometric data. The effect is that employers who currently use, or intend to use biometric data in the workplace, for example using fingerprint or retina scanners for building access or voice recognition to activate recording technology, must apply to the Authority for authorisation before doing so.

What the future looks like

Data privacy has quickly become a matter of global concern. Organisations everywhere are being impacted both operationally and financially by the wave of new data privacy laws, and those operating in Bahrain will be no different. At the time of publication, only a few specific aspects of the Law are actually enforceable. For the Law to come into full force and effect, the Board of Directors of the Authority will need to publish technical and legal guidance on some of its provisions. However, even in its current form, the Law is a big leap forward both for Bahrain, and from the perspective of all individuals who value their rights to data privacy. Also, some of the most important sections, for example those dealing with individual rights, are already enforceable.

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

You can now access Opinion articles for free on the OneTrust DataGuidance platform.

1. Available at: Law No. 13 of 2016 Concerning Privacy and Protection of Personal Data, available at <http://www.motc.gov.qa/ar/documents/document/qatar-issues-personal-data-privacy-law-5>

2. Data protection laws for the United Arab Emirates and Saudi Arabia are expected by the end of 2020, and both Jordan and Oman have draft legislation in the works.

3. Article 8(1) of the Law.

4. Article 13(3) of the Law.

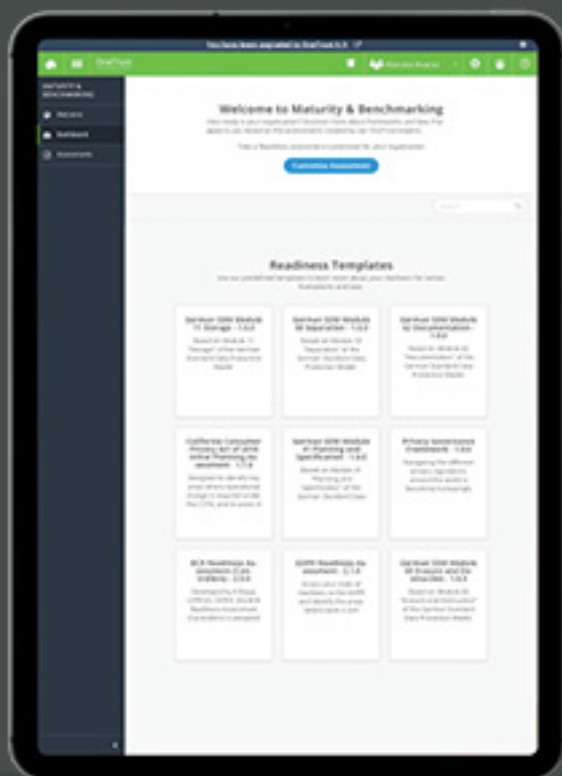
5. Article 4(14) of the GDPR defines 'biometric data' as any 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.'

OneTrust Privacy

PRIVACY MANAGEMENT SOFTWARE

Not Your Average Data Discovery

Revolutionary Technology for Responding to Consumer Rights Requests



Automate Manual Processes for Fulfilling Consumer Rights Requests



Works Across Thousands of Systems, On Premise, Cloud, Structured and Unstructured Data



Supports Email Redaction, Data Deletion, Identity Validation and Information Consolidation



Drastically Reduce Implementation Timelines, Get Up and Running within 48 hours

**Ready Your Consumer Rights Response
for January 2020 CCPA Deadline**
Trade Complexity for Simplicity with OneTrust

See What's Possible

OneTrust.com/Products/Targeted-Data-Discovery/



PRIVACY TALKS

Peter Fleischer is an expert in privacy compliance and advises Google's teams on how to design systems and products that are privacy focused and legally compliant. OneTrust DataGuidance spoke with Peter about the impact of privacy legislation globally, and how future technologies such as, machine learning and artificial intelligence, can be approached.



Peter Fleischer
Global Privacy
Counsel at Google

What was Google's process for complying with the GDPR, and how much has this cost?

We realised that the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') was going to be the biggest change in privacy law in our careers, probably in the history of Google LLC, and maybe in the history of our industry. It was going to be a big job. Granted, the GDPR was built on pre-existing privacy laws in Europe: the Data Protection Directive (95/46/EC). Nonetheless, there is a lot of new things that Google, and other companies, have to live up to doing. So, we never asked ourselves, "How much will it cost to do this?" We asked ourselves, "How are we going to do this?" We knew that we had to do this, and so we set in motion the process to comply with it. By the time of May 2018, when the GDPR entered into force, we had dedicated 500 human years of work to get ready for the GDPR. We now have 400 people working full time on privacy. So, I cannot tell you exactly how much that cost, but you can imagine what it cost if you have 400 people working full time in the field of privacy.

Globally, why has there been an increase in countries developing their own privacy legislation, and what trends are you seeing in the enforcement of these privacy legislations?

I think it is pretty clear that citizens around the world care about privacy. Citizens around the world are concerned about whether or not their privacy is being protected. So, it is very natural that citizens are telling their elected officials to do something about it. Governments have a responsibility to address their citizens concerns. Citizens are saying, 'I am worried about my privacy, you are my government, you should do something about it.' So, in response government officials are saying, 'Alright, well what are we supposed to be doing about it? What privacy laws should we pass? What should privacy laws look like? How do we enforce the privacy laws that are on the books to live up to our citizens expectations?'

Now, in Europe, obviously we have the GDPR, but around the world, we are seeing privacy laws either being passed for the first time in many countries or being updated in many others. Now we have well over the majority of countries on the planet that have comprehensive privacy legislation on the books. In Europe, we are used to that, we have had that for decades. In the United States, we have had it on a state to state basis for many years, not yet fully on a Federal level, but on the state to state on many occasions. In Latin America and South East Asia, for the first time over recent years, we have seen a proliferation of privacy laws and that is a change in the way that the privacy legal framework seen from a global perspective has evolved.

Some people say that the Internet needs a new business model. What do they mean by that?

When you look at the internet business model today, it is based on something pretty amazing. People can get a lot of services for free. You can use Google Search, Google Maps, lots of services on Google, for free. That is pretty astounding, and a lot of people like the fact they can use them for free. But, how are these things paid for? How do we make the money that allows us to invest in building and offering these services for free? Well, we show adverts.

People are familiar with adverts from the old television model, and from radio models, there is nothing new there. But on the internet, you are able to show adverts with a further degree of personalisation that had not been possible in prior generations of the advert-based model. So, on the internet today, we are seeing a lot of advert-sponsored models that are raising privacy questions. People are saying, 'Okay, well I love getting this service for free, but what exactly are they following in terms of me and my activities, my behaviour on sites, possibly even my profile, in order to show me the most relevant advert?' And those are very legitimate questions, so when people are saying, 'We need to think about the business model on the internet today,'

PRIVACY TALKS

continued

basically what they are saying is, 'Is it time to rethink the free model?' And, if you are going to rethink the free model, there is only really one alternative, and that is a paid model.

So, it is a tough debate. I mean, we are experimenting with both models. On YouTube, which is a Google company, we now have two models. People can say, 'Look, I am perfectly happy to get the free version of YouTube and in exchange for that I am going to watch adverts that are being shown to me, or alternatively, I will pay a fee and I will see an advert-free model of YouTube.' We are offering both alternatives, and it will be very interesting to see how consumers react to the offer of these two different models. When I look at the debates about the business models, they're partly a debate about the business models, but really, they are a debate about privacy choices that people are making. In other words, some people are saying, 'We do not want people to have the freedom to make a choice about the adverts they see or how they are going to manage their privacy settings, we are going to demand that a paid service be introduced as an alternative.' But that is a tough issue.

If you stop and think about it for a minute, I am not sure consumers want to pay for something that they are currently getting for free, and when something is a paid service, the company has to have a person's name, their credit card, their address, that is what a paid service means. You have to have real information about a real human being, not a pseudonymised user. So, even in purely 'privacy terms,' it is not clear to me which is the preferable model.

Nonetheless, I recognise there is this debate, and I think it is actually a really good thing that there is this experimentation of models. We, in Google, are experimenting with these different business models ourselves, and we will see how it works out, and how consumers respond to them.

Looking into the future, how are you approaching machine learning and artificial intelligence?

I am one of these people who believes that machine learning and artificial intelligence is not just a trend, it is not just a revolution, but this is perhaps the revolution of our lifetime. I am not someone who exaggerates, but I personally believe this is the revolution of our species. I mean, this is a time where we are moving from machines which we programmed and we created, to machines that learn. They learn themselves. They increase their own understanding of the world. They do not just increase on biological limits, they increase on machine-based limits, which means that they double in power every two years. They double in their ability to understand the world on a logarithmic basis. So, we are just at the beginning of a machine learning and AI revolution. This will be profound, and it will affect not just the tech industry, but it will affect all of us in every way.

Now, that being said, I think we have a profound responsibility to be thinking about the ethical obligations of what this revolution means, and can we set it on the right track at these early stages. When I look at machine learning from a

privacy point of view, since that is my field, privacy, I think there are a few things that we can do, and that we are doing. These are things that we need to be very focussed on at Google, in the industry as a whole, and beyond, to make sure that the machine learning AI revolution continues to respect basic privacy principles. What are they?

Well first, machine learning is always trained off a data set. It needs to learn from data. So the first that we need to do is to make sure that the data that is being used to train the machines is actually accurate, that it is not full of mistakes, that it is not full of human bias, whatever the kind of bias might be. The quality of the data training will in turn influence the quality of what the machine learning algorithms are able to do with it.

The second thing is, people say, 'Well, we do not want machine learning algorithmic black boxes, we do not want a lack of transparency about how this thing works, how it is making decisions.' So, we need to think hard about how we create transparency into that black box. How do we let people understand how the decisions are being made?

And finally, we need to look at the output of machine learning. We need to look at the outputs, the decisions, the choices, that machine learning algorithms are making. We need to access them. Are they accurate? Are they doing what they were programmed to do? Are they reinforcing bias against vulnerable groups in our society that we do not want them to reinforce? And we can correct the mistakes, and correct bias when we see it, and feed it back into the loop to correct itself, to improve itself. That is, after all, what machine learning is all about.

So, those three steps: the quality of the input, the transparency into what people have been calling the black box, and the quality of the output. We need to access all of those along the process to make sure the entire process is respecting the goals and the values that we as people want it to respect.

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

Video content can now be accessed for free on the OneTrust DataGuidance platform.

Key takeaways: New Portuguese Data Protection Act v. GDPR

This webinar provides a comparison between Portugal's Law No. 58/2019, which Ensures the Implementation in the National Legal Order of the General Data Protection Regulation (Regulation (EU) 2016/679) on the Protection of Individuals with Regards to the Processing of Personal Data and the Free Movement of Such Data ('the New Portuguese Data Protection Act') to the GDPR. In particular, the webinar examines data subject rights, duties of data protection officers, genetic and health data processing, children and employee data, privacy of deceased persons, video surveillance and retention periods, as well as sanctions and liability.

Key takeaways

Duty of secrecy in processing of health and genetic data
The New Portuguese Data Protection Act highlights that the duty of secrecy for medical professionals, nurses or any other party means that processing of health and genetic data, must be conducted in secrecy. It is unclear how the Portuguese data protection authority ('CNPd') will interpret this requirement. The New Portuguese Data Protection Act also states that data subjects must be informed of data accessed. In this regard, medical professionals also need to comply with other sectoral regulations in order to ensure confidentiality.

Processing of employee data for access and attendance

The CNPD stated that the processing of biometric data can only be conducted to control access and attendance of the employees. Consent to process personal data will not be lawful if the processing results in a legal or economic advantage for the employee. According to the speakers, there is a possible contradiction of the CNPD, considering the general rule under which consent must be avoided in employment. In addition, employee data collected through remote surveillance can only be used within the scope of criminal proceedings.

Permitted uses of CCTV

Data controllers based in Portugal need to comply with Article 19 of the New Portuguese Data Protection Act and with Law 34/2013 of 16 May 2013 on Private Security. The data collected from CCTV surveillance, such as images and videos, can only be used for the security of people and goods and not for other purposes. Controllers need to make sure they do not install cameras in public streets, areas where people use ATMs, food markets or areas for the employees such as, gyms, canteens, bathrooms and resting areas. When video surveillance is allowed, sound recording is prohibited unless the surveilled facilities are closed, or prior authorisation has been obtained from the CNPD.

Criminal liability

Prison sentences of up to one year or a fine up to 120 days can be issued for offences including use of data in an incompatible way with the purpose for which they were

collected, unauthorised access, breach of the duty of secrecy, or data misappropriation. Prison up to two years or fine up to 240 days can be issued if data has been unlawfully destroyed or false data added to a database.

How OneTrust DataGuidance helps

OneTrust DataGuidance provides a suite of privacy solutions designed to help you monitor regulatory developments, mitigate risk, and achieve global compliance, including Portugal. With focused guidance around core topics, comparative cross-border charts, a daily customised news service, and expert analysis, OneTrust DataGuidance provides industry leading solutions to design and support your entire privacy program.

OneTrust DataGuidance offers a GDPR Benchmarking tool, as well as specific comparison charts regarding national implementation of the GDPR. The suite of tools assist organisations to understand and examine core requirements under each law in order to determine their consistency for gap analysis and assessment, and contribute to the development of global compliance programs.

OneTrust DataGuidance also offers reports comparing the GDPR to other global legislation in key jurisdictions such as California, Brazil, and Japan, providing analysis on their scope, definitions, legal basis, the rights they provide, and their approach to enforcement. Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the legislations.

This webinar is available now on the OneTrust DataGuidance Video Hub.

Request a free trial to receive email notifications for upcoming webinars and access to the OneTrust DataGuidance platform.

Past webinars can now also be accessed for free through the OneTrust DataGuidance Video Hub.



California: CCPA proposed regulations and more

On 10 October 2019, after much anticipation, the California Attorney General ('AG'), Xavier Becerra, held a press conference and announced the release of proposed regulations¹ ('the Draft Regulations'), intended to further the purposes of the California Consumer Privacy Act of 2018 ('CCPA'). Jim Snell, Marina Gatto, and Zachary Watterson, from Perkins Coie LLP, provide an overview of the Draft Regulations, and look at what impact the Draft Regulations and other privacy developments in California will have on businesses.

The CCPA Draft Regulations

The AG stated that data is today's gold, and much like California's gold rush over 100 years ago, where people rushed to mine gold from the land, today there is a rush to mine data. The Draft Regulations will be open for public comment until 6 December 2019, and the AG will hold four public hearings² across the state. The AG's office has also indicated that the Draft Regulations will be updated to reflect the 2019 amendments to the CCPA that were signed into law by Governor Gavin Newsom earlier this month. The AG stated during a press conference that it is his office's goal to have the final CCPA regulations filed sometime in January 2020.

The Draft Regulations would provide important clarification on some aspects

of the CCPA, and would also add new requirements that businesses subject to the CCPA would need to address. We highlight several of these provisions below. Many businesses' operations would likely be impacted by the Draft Regulations, and businesses are assessing how to factor them into compliance efforts before the CCPA goes into effect on 1 January 2020. Data may be viewed as the new gold, as declared by the AG, but businesses, after waiting nearly a year for the Draft Regulations, are still left mining for answers as to what exactly their obligations are under the CCPA.

'Non-discrimination' and financial incentives clarification

The Draft Regulations would add some clarification to the CCPA's non-

discrimination provision by noting that a differential price or service offering is permitted if it is 'reasonably related' to the value of the consumer data. This is a helpful clarification, especially when coupled with the recent CCPA amendments which were signed into law by the Governor earlier this month, as the CCPA currently states that a business can only offer 'a different price, rate, level or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data,' according to §1798.125(b)(1) of Part 4 of Division 3 of the California Civil Code ('Cal. Civ. Code'). Thus, businesses may now have some flexibility in making reasonable distinctions between users whose choices impact the ability to offer a particular service.



Jim Snell Partner
jsnell@perkinscoie.com
Marina Gatto Associate
mgatto@perkinscoie.com
Zachary Watterson
zwatterson@perkinscoie.com
Perkins Coie LLP, Palo Alto

The Draft Regulations also provide clarification on how a business that offers financial incentives should provide the notice to consumers required under §1798.125 of the CCPA. In §999.307(b)(5) of the Draft Regulations, it is specified that businesses would need to provide notice that includes an explanation of why the financial incentive, price, or service difference is permitted, and should include a 'good-faith estimate of the value of the consumer's data that forms the basis for offering,' the incentive or difference, and a 'description of the method the business used to calculate the value of the consumer's data.'

Service provider clarifications

In clarifying the role of a 'service provider' under the CCPA, the Draft Regulations make it clear that service providers can collect data directly from a business' end-users and do not need to receive this data from the business itself. Additionally, in §999.314(c) of the Draft Regulations, service providers are permitted to combine personal information received from multiple business customers 'to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.'

Complying with requests to delete

The Draft Regulations specify that in responding to a request to delete, if the requestor's identity cannot be verified, the business' do not need to comply with the request to delete. However, the Draft Regulations would impose additional requirements where the requestor's identity cannot be verified. The business would need to notify the requestor that the business will not comply with the request, including the bases for the denial and any exceptions relied upon, and treat their deletion request as a request to opt-out of sale.

Where a business complies with a consumer's request to delete, the Draft Regulations add several new requirements in §999.313(d)(2), including that a business must 'specify the manner in which it has deleted the personal information,' and inform the consumer that it will maintain a record of their deletion requests.

No notice required for indirect collection

Under §1798.100(b) of the Cal. Civ. Code, the CCPA requires that a business provides notice to consumers 'at or before the point of collection' as to the categories of personal information to be collected and

the purposes for which it will be used. Under the Draft Regulations, a business that indirectly collects personal information would not need to provide notice to consumers. However, if businesses were to sell the personal information that was indirectly collected, then the business would need to either contact the consumer directly, to provide notice and an opportunity to opt-out, or obtain signed attestations from the source of the data on how the source gave notice at the collection point.

No requirement to provide sensitive data

The Draft Regulations would confirm that businesses do not need to provide sensitive data, such as social security numbers, government ID numbers, financial account numbers, health insurance or medical ID numbers, or account passwords, to consumers in response to a verified request. This is an important privacy protective clarification.

Additional consent requirements
The Draft Regulations would impose a new burden on businesses to obtain explicit consent for any new uses of personal information that the consumer was not previously notified

OPINION

continued

of. Under the Draft Regulations, prior to using any category of a consumer's personal information for a new or additional business or commercial purpose, a business would need to provide notice and obtain explicit consent from the consumer to use the data for the new purpose.

Additional opt-out requirements

The Draft Regulations appear to broaden what would be considered a request to opt-out of the sale of personal information. For example, the Draft Regulations specify in §999.315(h) that a 'request to opt-out need not be a verifiable consumer request.' Additionally, §999.315 of the Draft Regulations would require businesses to honour 'sale' opt-outs sent by browsers, devices, or other user agents.

New timing requirements

The Draft Regulations go beyond the CCPA's current requirements by imposing additional obligations on businesses to take certain actions within certain timeframes. The CCPA, under §1798.130(a)(2) of the Cal. Civ. Code, currently requires businesses to disclose and deliver information requested within 45 days of receipt of a consumer's request. Under §999.313(a) of the Draft Regulations, businesses would be required to confirm receipt of a request to know or delete within 10 days and provide the consumer with information about how they would process the request. Likewise, under §999.315(e) of the Draft Regulations, businesses would be required to act upon an opt-out request 'as soon as feasibly possible, but no later than 15 days from the date the business receives the request.' These new timing requirements may impact business's CCPA compliance tools in order to take into account these new time frames.

New record keeping requirements

In §999.317(b) of the Draft Regulations, businesses are required to 'maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.'

In addition, businesses that buy, receive, sell, or share the personal information of 4 million California residents or more, would also be required to compile detailed metrics for the previous calendar year, such as the median number of days it took the business to respond to consumer requests, and publish this information in their privacy policy.

What happens next?

With the announcement and release of the Draft Regulations, the AG initiated the formal rule-making process for the statutorily mandated rules under the CCPA. From the time of publication until 5:00 p.m. PST on 6 December 2019, the Draft Regulations will be in a public comment period phase, during which the AG's office will be collecting feedback on the Draft Regulations, including during public hearings held across the state.

After the public comment period ends, the AG will review the feedback given and make any further changes to the Draft Regulations deemed necessary. Depending on how substantial those potential changes are, there may be an additional public comment period before the final regulations are adopted. As stated, however, the AG announced that it is his goal to have the Draft Regulations adopted and filed with the California Secretary of State by early January 2020.

With the CCPA set to go into effect on 1 January 2020, many businesses will be spending the next few months considering how to address the Draft Regulations and still evolving regulations into their CCPA compliance efforts.

Other California privacy law developments

CCPA 2.0: The California Privacy Enforcement Act

The Draft Regulations are not the only noteworthy privacy development currently taking place in California. On 25 September 2019, Alistair MacTaggart, whose efforts to introduce a California privacy ballot

initiative resulted in the California legislature enacting the CCPA in 2018, introduced a new ballot initiative, the California Privacy Enforcement Act ('the Initiative'). He has since introduced a second and third version of this initiative and Mr. MacTaggart intends to put the Initiative on California's November 2020 general election ballot.

The Initiative would amend the CCPA, and include a number of new provisions, obligations, and enforcement mechanisms. Most notably, the Initiative would create a new statewide agency, the California Privacy Protection Agency ('the Agency'), which would be designed to enforce the CCPA. The Agency would be required to investigate consumer complaints of possible CCPA violations and have the authority to issue cease and desist orders, and fine businesses \$2,500 for each violation of the CCPA and \$7,500 for each intentional violation. The funds from these fines would support a Consumer Privacy Fund.

If the Initiative is enacted, it would mean that the compliance mechanisms put in place for the CCPA would need to be updated to address new obligations in the Initiative.

Conclusion

While the Draft Regulations released by the AG remain in draft form, and will likely undergo further changes, businesses should consider how to engage in the CCPA compliance efforts that take the Draft Regulations and the Initiative into account.

To download the OneTrust DataGuidance 'What You Need To Know' guides for the CCPA and the California Privacy Rights and Enforcement Act request free trial access or sign-in to the OneTrust DataGuidance platform.

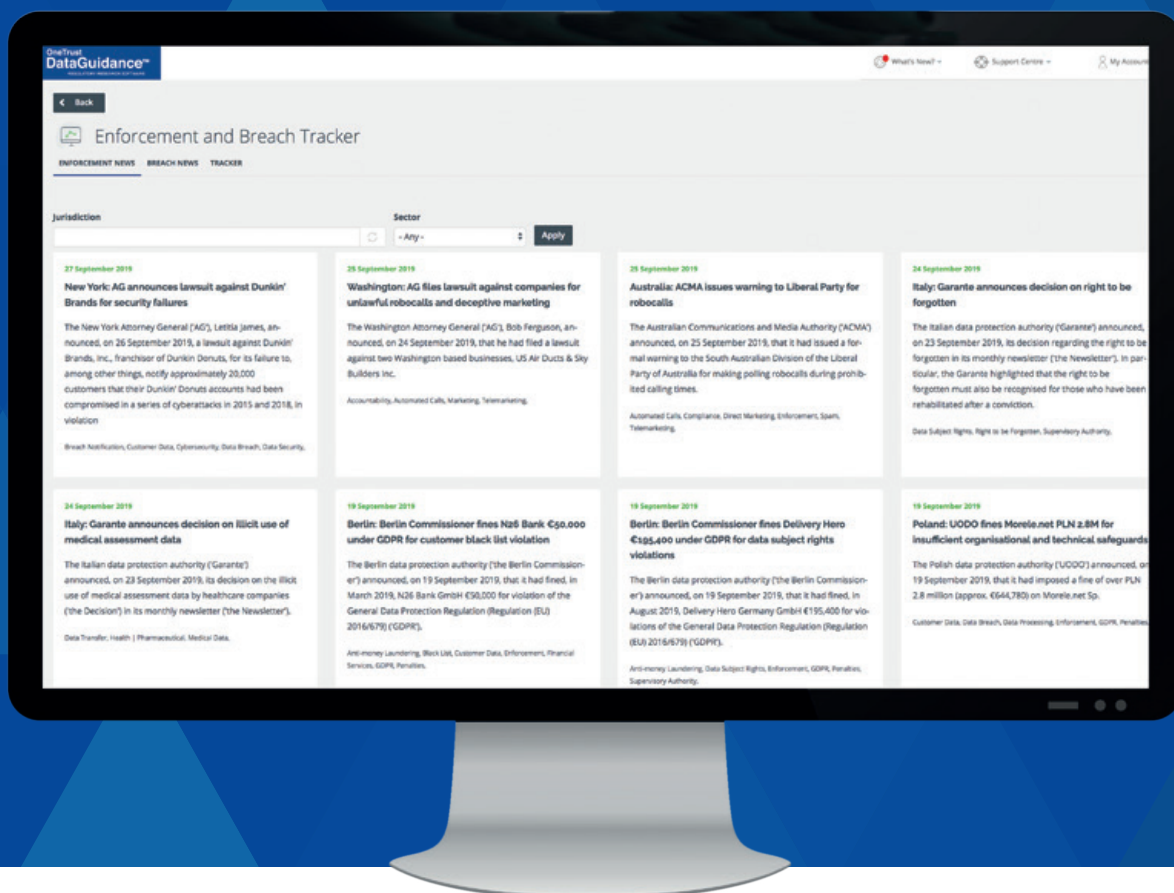
1. Available at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>

2. Available at: <https://oag.ca.gov/privacy/ccpa>

NEW Enforcement and Breach Tracker

Leverage data to assess privacy and data protection risk with our Enforcement and Breach Tracker. Stay up to date and compare across numerous jurisdictions and sectors when it comes to:

- Numbers of complaints
- Investigations
- Data breaches
- Enforcement actions
- Monetary penalties



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



OneTrust
DataGuidance™

REGULATORY RESEARCH SOFTWARE





At OneTrust PrivacyTech: London in June 2019, OneTrust DataGuidance spoke with Erik Boucher, Information Technology Expert at the French data protection authority ('CNIL'). Erik provides insight into CNIL's approach to implementing the GDPR, and CNIL's areas of focus in terms of guidance.

What are the key takeaways from CNIL's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') implementation activity report?

Among the key findings, there was a global awareness from citizens about their rights. The GDPR and also some other recent developments, such as data breaches, have made people gain awareness about their rights and about how companies handle their data, and so we have seen a raise in complaints and questions. So, it is quite amazing to see how people are really getting used to the GDPR and, for example, we have had many complaints on delisting, but also on other kind of rights, such as the use of biometric data, and we will also have a look next year into the protection of children's data. That is quite a challenging thing because it is very sensitive and also because there is a question of the legal age for consent, parental control, etc., so that will be a trend for the next few years.

What has required CNIL's recent focus on providing guidance for start-ups and developers?

We noticed that with the GDPR, many, many small businesses, and start-ups came to CNIL for advice and we could not handle them all. So, we started to write compliance books, for small-medium sized enterprise's for example, and also guidelines for how to use a software development kit in mobile applications. So yes, our idea is to give key recommendations to every actor in the whole chain, from the very developer to the chairman. You see, you have to get this awareness to everyone in the data chain, I would say, so that the idea of Privacy by Design is really implemented.

What are CNIL's priorities over the next 12 months with respect to technology and privacy?

I would say that we are really focussing on data warehouses because before artificial intelligence, and before machine learning, you first have to collect the data. With data collection you have many, many questions around consent, how to get consent, how to express purpose when you do not really know what you will be doing with the data in the next year, and also some more technical issues surrounding the pseudonymisation, or data de-identification as they say in the US, or full anonymity of the data. How do you handle de-identification because Big

Data and machine learning need quite rich, detailed, and still individual data, which is quite difficult to achieve if you want to be completely compliant with the GDPR. Therefore, you have to find some ways to identify at what point will the data be de-identified enough so more people can access it. You have to identify the data scientist group, what they can do with the data, and how to control what they do with it. That will be quite challenging to have a variation in the sensitivity of the data, and who can access it and what they do with it. In France, there is a big project, the Health Data Hub, which will gather every data on people's health, the medicines that they take, the doctors they see, their biology, etc., and the idea is to have a call system, or different systems, that will be used for research. Then, there are the questions of, 'Is the data deidentified? Did we get the consent? Did we express the purpose right?' and that will be a real challenge.



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

For daily updates regarding regulatory developments, and news from over 300 jurisdictions request a free trial and visit the OneTrust DataGuidance News Tracker.

France: The CNIL's new cookie guidelines and their impact on digital marketing

The French data protection authority ('CNIL') has recently published an action plan geared towards updating guidelines related to targeted online marketing ('the Action Plan'). As part of its two-step plan, the CNIL has adopted guidelines to update rules relating to the use of cookies and similar technologies ('the Guidelines'). Aurélie Pacaud, Associate at Gide Loyrette Nouel, provides insight into the key changes to cookie rules and how this will affect online marketing in France.

The Action Plan

Having observed that more than 20% of the complaints it receives relate to marketing, and in the light of its recent decisions on geolocated targeted advertising, the CNIL has developed an action plan ('the Action Plan') for targeted advertising for 2019-2020, which it published on 28 June 2019¹.

One aspect of the Action Plan concerns direct marketing, and refers to the updated position of the CNIL², which in particular strengthens information requirements with regards to 'third-party opt-in.'

The other central aspect of the Action Plan, upon which this piece focuses, relates to the use of tracking mechanisms, more commonly referred to as 'cookies'.

The Action Plan may be considered a timely development from the CNIL, considering the slow progress in the adoption of the proposed Regulation on Privacy and Electronic Communications ('the Draft ePrivacy regulation'), and the shortcomings of the principles

set forth in its 2013 guidelines³ ('the 2013 Guidelines') when viewed in light of the strengthened definition of consent contained within the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR')

In order to effectively update its position on cookie use, the CNIL has developed a two-step approach in the Action Plan: first, the issuance of new guidelines, repealing and replacing its 2013 guidelines on the same topic; and, second, the organisation of workshops with stakeholders in the digital marketing sector in order to draw up a practical mechanism to obtaining consent, which is to be integrated into the finalised version of the Guidelines.

Shortly after the publication of the Action Plan, CNIL announced, on 18 July 2019, that it had implemented the first step of the Action Plan, having adopted new and updated guidelines on cookie use ('the Guidelines') on 4 July 2019.


This piece aims to offer an overview and analysis of the changes in the rules relating to cookie use following

the publication of the Action Plan and the Guidelines, with particular attention to their potential impact on the digital marketing sector.

The 2013 Guidelines

At the time, after a consultation with the relevant market stakeholders, the CNIL had considered that consent, as required by Article 32 of Act No.78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (which transposes Article 5(3) of the Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the ePrivacy Directive')), could be obtained through a two-step mechanism, consisting of:

1. displaying a banner to users, informing them of the purposes of the cookies, of the possibility to refuse cookies or to manage their settings, and of the fact that continuing browsing on the website would be deemed as consent; and
2. providing to users the means to refuse cookies depending on their purpose (e.g. advertising, social networks sharing buttons, audience measurement).



This approach to consent is the so called 'soft opt-in' approach which the CNIL has now decided to reconsider. Considering the general trend of increased user protection, and the ineffectiveness of the current cookie banner mechanism, the CNIL has revisited its interpretation of Article 82 of Act No.78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (as amended to implement the GDPR), which transposes Article 32 of the pre-GDPR Act.

The Guidelines: a return to positive action

In the Guidelines, the CNIL restates some long standing principles. In particular, the Guidelines highlight that cookies should be understood broadly to include any type of tracking mechanism, but that certain audience measurement cookies may be exempted from consent requirements, provided certain conditions are fulfilled. The CNIL also clarifies other principles, such as the prohibition on using 'cookie walls,' mechanisms that block access to a website until the user has accepted the cookies.

However, as touched on above, the main addition introduced by the Guidelines concerns the interpretation of the 'positive action' requirement, which sees the CNIL repealing its old approach and expressly rejecting the notion that continued navigation of a website may amount to the giving of consent. In this

respect, the Guidelines affirm that, to be considered valid, consent must be given independently and specifically for each distinct purpose.

In addition, the Guidelines preclude the use of browser settings as an adequate mechanism to obtain consent, considering that this method does not allow users to choose a selection of the cookies based on their specific purpose, and that it is not efficient for certain tracking mechanisms, such as fingerprinting.

What does position action mean in practice?

Under the old approach, as long as sufficient information was provided through the banner, cookies could be installed whenever the user scrolled down the screen or accessed another page on the website. It is safe to say that, most of the time, users would neither read, nor even notice the banner, and consequently, would have not be aware of the cookies installed on their device.

Following the adoption of the Guidelines, the installation of any 'non-exempted cookies' is prohibited unless the user has expressly consented through a positive action (e.g. by clicking on a button or ticking a box).

Practical mechanisms to obtain consent have yet to be precisely outlined by the CNIL, which announced in the Action Plan that such mechanisms

would be discussed and developed in workshops with stakeholders in the digital marketing sector in the months to come. Nonetheless, the CNIL has shed some initial light on this matter, explaining that the mechanism to be implemented shall enable users to consent purpose by purpose, and controller by controller, while conserving a blanket choice option (e.g. 'yes I accept all cookies' and 'no I refuse all cookies'), as long as the granular choice remains an option.

The concept of 'granular' consent, which allows users to accept advertising cookies from publisher A and to refuse those from publisher B, has already been discussed in the context of a series of decisions by the CNIL with respect to mobile marketing service providers.

In these cases, the CNIL found that the aforementioned mobile marketing service providers were using Software Development Kit technology that enabled the collection of users' geolocation data when they opened the application. This data would subsequently be used by the service providers to send targeted ads to the same users. In this context, the CNIL noted that the data subjects' data had been processed without valid consent because users, when opening the application, were neither informed that their geolocation data was being collected for targeted advertising purposes, nor that it was transmitted

OPINION

continued

to third parties. In response to these cases, the CNIL suggested the implementation of an interface enabling users to select the purposes they consent to, and the third parties with whom they accept sharing their data.

A not so user-friendly solution

In theory, the mechanism prescribed by the CNIL could be easily implemented, as consent management platforms complying with these requirements have already been made available on the market and are ready to use. The question is whether, in practice, users will benefit from such a consent mechanism, when some applications are known to share data with hundreds of partners. What will be the reaction of a user presented with an interface displaying dozens of purposes, and hundreds of partners? One could presume that such a user will either accept all cookies, and remain as unprotected as he/she is today, or refuse all cookies, including those which are less intrusive, such as audience measurement cookies, which will in the end be detrimental to service providers, and more generally to the digital marketing industry.

The potential effect of the Draft ePrivacy Regulation

As alluded to above, the aim of the Guidelines issued by the CNIL, and indeed of guidelines issued by other data protection authorities such as the UK's Information Commissioner's Office's ('ICO') Guidance on Cookies and Similar Technologies⁴, is to fill the gaps left by the lengthy negotiations over the Draft ePrivacy Regulation.

The latest version of the Draft ePrivacy Regulation, published on 26 July by the Presidency of the Council of the European Union, has adopted another approach, considers that

'consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.'

Some of the risks that had been commonly pointed out in relation to such an approach were the decontextualisation of the process of giving consent to the installation of cookies, as the information will always be more precise when provided when accessing a specific service, and the concentration of knowledge and access to data concerning users of the most widely used operating systems and browsers, such as Google LLC, Amazon.com Inc, Facebook, Inc. and Apple Inc.

What will be the immediate impact?

The CNIL has indicated in the Action Plan that a transitional period of 12 months will be established, in order to enable market players to comply with the new principles of the Guidelines.

During this 12 month period, workshops will be conducted with content publishers, advertisers, intermediaries, and service providers within the marketing ecosystem, in order to discuss and develop the Guidelines. The results of such discussions will be integrated into the finalised version of the Guidelines, which will be published by the beginning of 2020, at the latest, outlining the operational mechanisms to obtain consent. The CNIL will start to regulate compliance with the finalised version of the Guidelines within 6 months of their official adoption.

However, there is a possibility that this timeline could be disrupted by the decision to come of the Conseil

d'Etat, which, on November 30, will hear the association La Quadrature du Net, which filed an action to obtain the suspension of the finalised version of CNIL's Guidelines, on the basis that the 12 months transitional period is in violation of the GDPR⁵.

For now, those involved in the French digital marketing ecosystem should closely follow, on the one hand, the evolution of the CNIL's position, in particular, in the light of the imminent decision of the Conseil d'Etat, and, on the other hand, the ePrivacy negotiations. In any case, digital marketing in France should start to work as soon as possible on a mechanism that will not rely anymore on the 'soft opt-in' approach to consent.

Aurélié Pacaud Associate

aurelie.pacaud@gide.com

Gide Loyrette Nouel

For Opinion, webinars, guidance and more regarding cookies and the draft ePrivacy Regulation, visit the OneTrust DataGuidance platform or request trial access.

1. Available at: <https://www.cnil.fr/en/online-targeted-advertisement-what-action-plan-cnil>

2. Available at: <https://www.cnil.fr/fr/la-prospection-commerciale-par-courrier-electronique>

3. Available at: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028380...>

4. Available at: <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-o...>

5. La Quadrature du Net, together with Calipien, had filed in July a 'référé-suspension' with the Conseil d'Etat, which is an emergency procedure to obtain without delay the suspension of an administrative decision. The Conseil d'Etat has ruled on August 14 that there was no emergency in ruling on the matter whether the CNIL recommendation violates the GDPR considering that the hearing on the merits would be held on November 30. The decision of the Conseil d'Etat is available at: <https://www.laquadrature.net/wp-content/uploads/sites/8/2019/08/d%C3%A9c...>

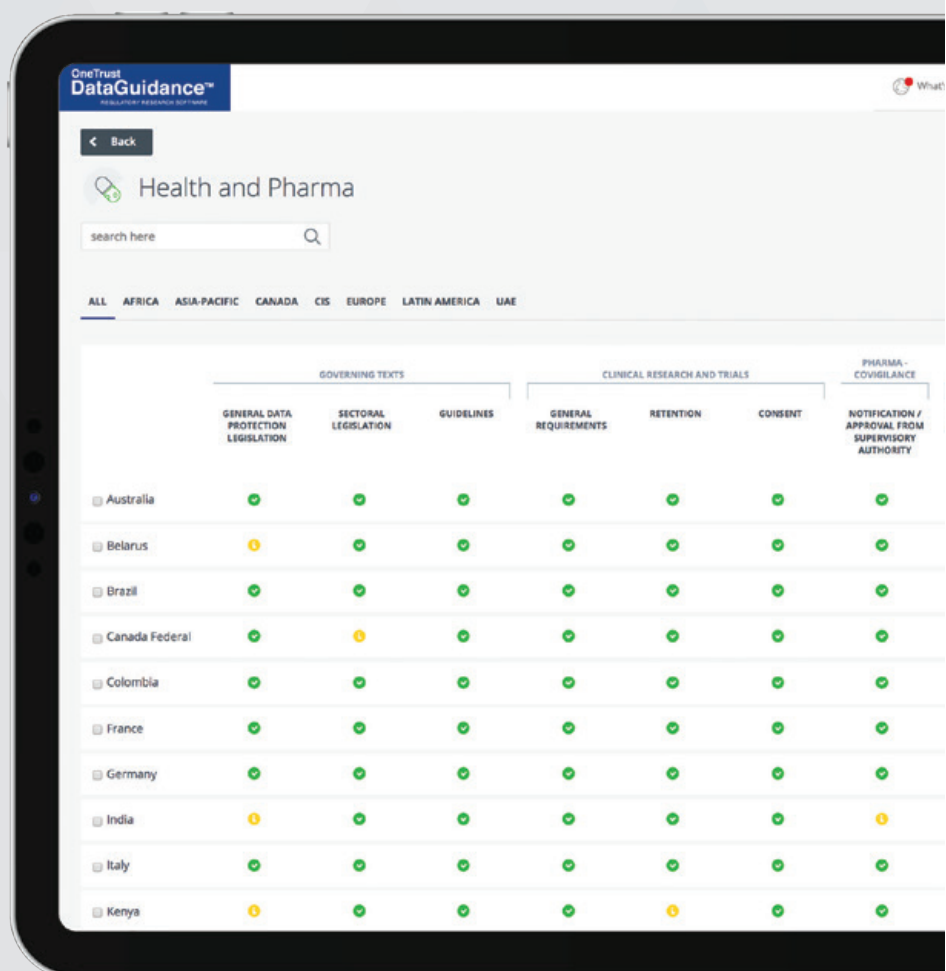
NEW

Health and Pharma Chart

Understand and compare sector specific requirements globally with the Health and Pharma comparison chart.

Utilise detailed analysis of privacy laws and sector specific legislation, including requirements on:

- Clinical Research and Trials
- Pharmacovigilance
- Biobanking
- Data Management
- Data Transfers
- Breach Notification
- Penalties



OneTrust DataGuidance™

Health and Pharma

search here

ALL AFRICA ASIA-PACIFIC CANADA CIS EUROPE LATIN AMERICA UAE

	GOVERNING TEXTS			CLINICAL RESEARCH AND TRIALS			PHARMA - COVIGILANCE
	GENERAL DATA PROTECTION LEGISLATION	SECTORAL LEGISLATION	GUIDELINES	GENERAL REQUIREMENTS	RETENTION	CONSENT	NOTIFICATION / APPROVAL FROM SUPERVISORY AUTHORITY
Australia	✓	✓	✓	✓	✓	✓	✓
Belarus	!	✓	✓	✓	✓	✓	✓
Brazil	✓	✓	✓	✓	✓	✓	✓
Canada Federal	✓	!	✓	✓	✓	✓	✓
Colombia	✓	✓	✓	✓	✓	✓	✓
France	✓	✓	✓	✓	✓	✓	✓
Germany	✓	✓	✓	✓	✓	✓	✓
India	!	✓	✓	✓	✓	✓	!
Italy	✓	✓	✓	✓	✓	✓	✓
Kenya	!	✓	✓	✓	!	✓	✓

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



OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

International: UK-US data sharing agreement "may create difficulties between UK and EU in event of hard Brexit"

The UK Government published, on 7 October 2019, the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime ('the Agreement').

In particular, the Agreement would allow the UK and US' ('the Parties') law enforcement agencies to request electronic data regarding serious crime, including terrorism, child sexual abuse, and cybercrime, directly from 'covered providers' based in either country, without legal barriers. The Agreement defines 'covered provider' as any private entity which provides to the public the ability to communicate, process or store computer data, by means of a computer or a telecommunications system, or process or store content of an electronic or wire communication. The Agreement will enter into force following a six month review by the UK Parliament and the U.S. Congress, as mandated by the US Clarifying Lawful Overseas Use of Data Act 2018 ('the CLOUD Act').

"Corporations are at relatively little direct risk as a result of the Agreement"

Tim Hickman, Partner at White & Case LLP, told OneTrust DataGuidance, "The European Data Protection Board and the European Data Protection Supervisor concluded in their Initial Legal Assessment of the Impact of the the CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of An EU-US Agreement on Cross-Border Access to Electronic Evidence, that the CLOUD Act does not provide a valid justification for cross-border data transfers. Their conclusion is unsurprising, given that the CLOUD Act is a piece of US legislation that seeks to apply certain powers unilaterally, in part as a result of the United States v. Microsoft Corporation case [...] [Moreover,] the Agreement may create difficulties between the UK and the EU in the event of a hard Brexit. In that scenario, the UK will likely seek an adequacy decision from the European Commission in order to allow for the continued free flow of personal data between the EU and the UK. However, suspicions regarding intelligence sharing between the Parties have become a key reason why some EU


politicians and bureaucrats are resistant to the idea of granting the UK an adequacy decision. The Agreement may well add to those suspicions and could mean that the UK is unable to secure an adequacy decision in the event of a hard Brexit. This would make it significantly harder for businesses to freely share data between the EU and the UK in a post-Brexit world."

In addition, the Agreement highlights that timely access to electronic data for authorised law enforcement purposes is essential for the purpose of protecting public safety and combating serious crime and terrorism. Moreover, the Agreement aims to provide standards of protection that comply with the Parties' laws regarding the treatment of electronic data containing personal data, and to create a legally binding and enforceable instrument between public authorities that provides appropriate safeguards for the same. Furthermore, the Agreement stipulates that the Parties will undertake measures to ensure that their domestic laws relating to the preservation, authentication, disclosure, and production of electronic data permit 'covered providers' to comply with the Parties' respective requirements to disclose or produce content, such as computer data stored or processed for a user, traffic data and subscriber information.

Hickman concluded, "Corporations are at relatively little direct risk as a result of the Agreement, because the Agreement does not compel disclosure of [certain categories of] data, as such. However, the Agreement does oblige the UK Government to make the necessary changes to the UK's laws in order to give effect to the Agreement, and those changes may compel such disclosure. This is not directly contradictory to the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which permits processing, disclosure, and transfer, of personal data to the extent that such processing is required by applicable laws in the UK. If a business is obliged by the laws applicable to it in the UK to disclose personal data, the GDPR does not stand in the way of such disclosures."

Lucian-Gabriel Burcea Privacy Analyst
lucian.burcea@dataguidance.com

OneTrust DataGuidance



Germany: DSK issues five-step sanction model which "may result in considerably higher GDPR fines"

The German Data Protection Conference ('DSK') issued, on 16 October 2019, its five-step model ('the Model') for state data protection authorities to calculate the monetary amount of fines issued to companies under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), following initial negotiations at the European level.

The DSK outlined that the first step of the Model is to allocate the company to one of four classes, based on its size, followed by subclass, based on its annual turnover for the previous year. The DSK noted the second step is to calculate the average annual turnover of the respective subgroup and the third step to determine a base economic rate by dividing the average annual turnover by 360. Furthermore, the DSK specified that the fourth step is to multiply the base economic rate, depending on the severity of the infringement, by a factor of one to six for violations of Article 83(4) of the GDPR and a factor of greater than six for violations of Article 83(5) and (6). Finally, the DSK clarified that the fifth step is to take into account any further case specific circumstances.

Dr Wolf-Tassilo Böhm, Associate at Latham Watkins, told OneTrust DataGuidance, "The Model may result in considerably higher GDPR fines, in particular for companies and corporations with significant revenue. The DSK explicitly provides that German data protection authorities should determine the respective revenue based on the corporate group's global revenue. [...] Company actuaries and risk managers will have to consider the new fine calculation model to determine accruals for risks and liabilities more accurately [and] may also attach greater importance to robust data protection management and governance structures, as this may count as a mitigating factor under Article 82(2) of the GDPR. [...] Companies who find themselves issued with a fine calculated under the new model should evaluate all strategic options including challenging the fine in court."

The DSK stipulated that the turnover of a company is a suitable, proper and fair measure to ensure the effectiveness and proportionality of fines, as required under Article 83 of the GDPR, and highlighted that there may be potential changes and additions to the Model and supervisory authorities' practice, following results from future Europe-wide votes. In addition, the DSK noted that German courts are not bound by the Model. Dr Simon Assion, Senior Associate at Bird & Bird, told OneTrust DataGuidance, "Companies have many options to keep fines as low as possible. [...] The best risk mitigation method is to correct the alleged infringement quickly and thoroughly, to remedy

any damage to third parties that might have occurred, and to cooperate well with the authority from the beginning. [...] If the authority commences fine proceedings nonetheless, these steps will at least lead to a reduction of the fine in 'stage 5' of the calculation. [...] Fines are subject to legal appeal before the competent courts [...] [which] will make their own assessment of whether the calculation of a fine was appropriate. [Furthermore] courts could impose a fine that is even higher [than that issued by the supervisory authority]. The courts can in some circumstances change the amount of a fine to the detriment of companies and are not bound to the limits enshrined in the DSK model."

"The courts can in some circumstances change the amount of a fine to the detriment of companies"

The DSK stated that the Model aims to give data protection supervisory authorities a uniform method for a systematic, transparent and comprehensible assessment when issuing fines, as well as improving data controllers' and data processors' understanding of the supervisory authorities' decisions. Moreover, the DSK noted that the federal and Länder supervisory authorities may at any time request an annulment, modification or extension of the Model in the future. Furthermore, the DSK outlined that the Model will lose its validity as soon as the European Data Protection Board ('EDPB') completes its final guidelines on the issuing of fines.

Assion added, "To be frank, I do not see this model as a transparent and systematic way of calculating potential fines. It provides a mathematical basis for the calculation, but all relevant decisions remain in the unchecked discretion of the authorities. There is, in particular, no indication of how breaches should be classified into the categories of 'slight,' 'medium,' 'serious,' and 'very serious.' And almost all criteria that should be taken into account when calculating a fine according to Article 83(2) of the GDPR are simply pushed into step 5, without any indication how they should be weighed. [...] For risk management purposes, [predictive fine] calculations should then be treated as a 'worst-case scenario,' but not as a precise prediction."

Lily Davies Privacy Analyst
lily.davies@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.

Egypt: Draft Law represents first "law protecting personal data"

OneTrust DataGuidance confirmed, on 4 November 2019, with Dr. Mohamed Hegazy, Head of Regulations and Laws Committee, Ministry of Communications and Information Technology, that the Egyptian House of Representatives had approved, in principle, on 3 November 2019, the draft of Egypt's first law on data protection ('the Draft Law'), which is estimated to enter into force by the end of 2019.

In particular, the Draft Law includes consent requirements for the collection, processing and disclosure of personal data, provisions on data transfers and fines for violations, which can also be found in the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). Moreover, the Draft Law also contains unique provisions regarding, among other things, the lawfulness of data processing and the processing of special categories of personal data.

Mohamed Hashish, Partner at Soliman, Hashish & Partners, told OneTrust DataGuidance, "This is the first time for Egypt to have a special law protecting personal data. [...] Despite the fact that the GDPR was taken as a base for the Draft Law, the level of drafting and protection adopted under the GDPR is not comparable with the Draft Law [...]. The GDPR puts great emphasis on the transparency principle relating to processing of personal data, while the Draft Law does not follow the same level of emphasis [and] [...] exempts [from its scope] the Central Bank of Egypt ('CBE') and all entities (including banks) that are subject to CBE's supervision. [...] [Moreover], the Draft Law does not allow the processing of personal data when the same is necessary for the purpose of legitimate interest of the controller or by a third party, [...] [and] does not restrict the processing of special categories of personal data [...] and/or personal data related to criminal convictions and offences, which is the case in the GDPR.

"The Executive Chairman may issue actions [such as] warnings of suspension of licensing, authorisation or accreditation."

Furthermore, the Draft Law contains different data transfer requirements than the GDPR. While Article 49 of the GDPR contains a list of exemptions under which data transfers are allowed, such as explicit consent of the data subject, the performance of a contract between the data subject and the controller, important reasons of public interest or the establishment, exercise or defence of legal claims, the Draft Law provides for one, two-fold exception.

Hashish highlighted, "Article 14 of the Draft Law prohibits any act of transfer, storage and/or sharing of personal data which was collected or prepared for processing to any foreign State unless [...] [there is a] protection level that is not less than the one adopted by the Draft Law and a license by the Personal Data Protection Centre ('the Centre') is obtained. [...] It is not clear yet how the licensing process will work, however, [...] [it] will depend on a number of factors including, inter alia, the country to which the personal data will be transferred, national security concerns, and whether or not the said country allows the transfer of personal data to Egypt.

Moreover, the Draft Law also introduces enforcement powers to ensure the data protection within Egypt, in addition to the provisions of civil and criminal liability. In particular, Article 29 of the Draft Law vests the Executive Chairman of the Centre, in case of any breach of the provisions of the Draft Law, with the authority to remove the violation's causes and effects.

Esraa Mohamed, Attorney at Youssry Saleh & Partners, told OneTrust DataGuidance "[...] [In particular, the Executive Chairman may issue actions [such as] warnings of suspension of licensing, authorisation or accreditation, in whole or in part, for a specified period, [as well as] suspensions or withdrawals, in whole or in part, [of] the license, permit or accreditation [...]. [Moreover, the Executive Chairman can] publish a statement of the violations that have been proven in one or more mass media at the expense of the violator [and] subject the controller or processor to the technical supervision of the Centre [in order] to ensure the protection of personal data at their expense [...]."

Lea Busch Privacy Analyst
lea.busch@dataguidance.com
OneTrust DataGuidance

OneTrust Privacy

PRIVACY MANAGEMENT SOFTWARE

The background of the right side of the image features a collage of the California state flag, which includes a grizzly bear and the text 'CALIFORNIA REPUBLIC', and the California State Capitol building. These elements are overlaid with a green geometric pattern of triangles.

CCPA Master Class Series

Master CCPA Requirements
Implement with Confidence

Free Expert-Led Webinar Series

Prepare for CCPA-Specific Requirements

Webinar Topics Include

Consumer Rights | Do Not Sell | Identity Verification
Targeted Data Discovery™ | Data Mapping for CCPA
Cookie Banner Management | Vendor Management

Watch Now

onetrust.com/ccpa-compliance/masterclass/

