Volume 2, Issue 5
September 2020
dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

UNSPOKEN TRUTHS ABOUT SCHREMS II

Eduardo Ustaran discusses the impact of Schrems II on international data sharing 4

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTRIBUTORS TO THIS ISSUE

Eduardo Ustaran, Hogan Lovells
Eduardo Ustaran is Global co-head of the Hogan Lovells Privacy and Cybersecurity practice and is widely recognised as one of the world's leading privacy and data protection lawyers and thought leaders. With over two decades of experience, Eduardo advises multinationals and governments around the world on the adoption of privacy and cybersecurity strategies and policies.
Based in London, Eduardo leads a highly dedicated team advising on all aspects of data protection law – from strategic issues related to the latest technological developments such as artificial intelligence and connected devices to the implementation of global privacy compliance programs and mechanisms to legitimise international data flows.

Claire François, Hunton Andrews Kurth LLP
With more than 12 years of experience addressing complex privacy issues, Claire advises on a variety of French and international data compliance projects. Clients turn to Claire to get prepared for the GDPR and handle data compliance projects tailored to their needs. She has significant experience with French and EU data compliance law issues, including implementation of Binding Corporate Rules (BCRs) and other international data transfer mechanisms, and notification of data breaches. Her experience allows her help clients prepare the transition into the EU new legal data protection framework. Claire also represents clients before the French Data Protection Authority.

Dr Carlo Piltz, reuschlaw Legal Consultants
A data expert with many years of experience, Dr. Carlo Piltz continues to be active in the training of lawyers in the field of data protection law. Dr. Carlo Piltz studied law in Göttingen. Following his period as a trainee, some of which he spent at the European Commission in Brussels, he also worked as legal counsel in the law department of a social network operator.

Dr. Marie-Louise Gächter-Alge
Dr. Marie-Louise Gächter has been the Data Protection Commissioner of the Principality of Liechtenstein since the beginning of 2018. Since 2009, Dr. Marie-Louise has worked as a lecturer at the Chair of International and European Law at the Faculty of Law at the University of Freiburg.

Evan Davies, YouGov
As YouGov's Group Data Protection Officer, Evan is responsible for the coordination of the company's data protection measures globally. The nature of the role combined with YouGov's global footprint provides daily opportunities to work with colleagues, clients, suppliers and partners across the world.

Odia Kagan, Fox Rothschild LLP
Odia is a Partner and Chair of the GDPR Compliance & International Privacy Practice Group at Fox Rothschild LLP, a national law firm. Odia has worked with over 100 companies of varying industries and sizes on their paths to compliance with the EU GDPR. She leverages her in depth knowledge of GDPR to assist companies on the road to compliance with the California Consumer Privacy Act (CCPA).

Jason Burns, Bristol-Myers Squibb
Jason is the EU Data Protection and Governance Lead at Bristol-Myers Squibb Ireland, where he works on the challenges that can arise in relation to the cross-over between pharma-specific and data protection legislation and the key operational challenges for the organisation with respect to the GDPR.

Alice Gravenor, PwC Legal Middle East
Alice is a Senior Associate in the Privacy and Data Protection practice at PwC Legal Middle East, based in Dubai. She has experience working on a vast range of data privacy matters for global clients across a diverse range of industries including hospitality, aviation, government, financial, services and technology.Her current focus is on the GDPR, in light of its extraterritorial scope and consequential applicability in the Middle East.

Image production credits
Cover / page 4 image: peterschreiber.media / Essentials collection / istockphoto.com
Page 6 image: akinbostanci / Signature collection / istockphoto.com
Page 14 image: piranka / Signature collection / istockphoto.com
Page 16 image: tunart / Portfolio / istockphoto.com
Page 23 image: adamkaz / Signature collection / istockphoto.com
Page 24-25 image: gremlin / Signature collection / istockphoto.com
Page 28-29 image: 35007 / Signature collection / istockphoto.com
Page 32-33 image: Gabrielle Vissoto / unsplash.com
Page 34-35 image: Agence Olloweb / unsplash.com
Page 36-37 image: tolgart / Signature collection / istockphoto.com

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

Website www.dataguidance.com

Email DPL@onetrust.com

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Editor Eduardo Ustaran
eduardo.ustaran@hoganlovells.com

Managing Editor Alexis Kateifides
akateifides@onetrust.com

Editorial Victoria Ashcroft
vashcroft@onetrust.com

OneTrust DataGuidance™ Content Team
Nikolaos Papageorgiou, Iana Gaytandjieva, Mona Benaissa, Robb Hiscock

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

EDITORIAL

This decision has exposed once again the natural and constant tension between the protection of privacy and the need for the state to access personal data to perform its functions

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

Editorial: Unspoken truths about Schrems II

One of the most remarkable things about the Schrems II decision has been the truly deafening amount of noise it has generated. Some have boldly claimed that transfers of data from the EU to the US are now illegal. This has led to further claims that the only solution is for the US radically to change its legal framework or that all European personal data should just be kept in Europe. Others have responded that such an approach only reveals the hypocrisy of ignoring the extent of government access to data in Europe. Many more have said that since this is a political problem, it is unfeasible for any organisation involved in data transfers to come up with a solution and therefore, it is outside their control. Meantime, vociferous legal complaints have contributed to a climate of anxiety that threatens to cripple data globalisation as we know it.

It is important therefore to uncover some truths about the Court of Justice of the European Union's ('CJEU') decision, which seem lost amid all this noise. First of all, this decision has exposed once again the natural and constant tension between the protection of privacy and the need for the state to access personal data to perform its functions. Law enforcement, taxation, public health, and national security are all dependent on the access to and use of personal data. In Europe and many other parts of the world, it is paramount that any such data activities by the state do not breach democratic principles and individuals' rights. Every instance of government access to data creates a risk, so what the CJEU is saying is that when European data becomes available to foreign states, we must remain vigilant about this risk and take steps to ensure that the democratic balance is not lost. This is not radical political grandstanding, but a court doing its job.

At a more mundane, data protection-specific level, the CJEU also reminds us that the limitations on international data transfers are simply intended to ensure the continuity of the level of protection established by the European framework. This raises the issue of whether those limitations are even relevant given the powerful extraterritorial reach of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). In other words, the applicability of the GDPR far beyond the boundaries of the EU means that, at least in principle, the level of protection provided by this framework will be extended to data processing activities taking place in other jurisdictions. However, in judging what an 'adequate level of protection' means, the CJEU goes much further and essentially gives extraterritorial application to the Charter of Fundamental Rights of the European Union. This sets a very high bar for other jurisdictions to reach.

Understandably, some have seen this as an impossible task for them to undertake. How can anyone make an assessment of the world's public authorities' powers and take a view on their level of interference with the rights to privacy and data protection? Is it even possible to identify the additional safeguards that could compensate for an excessive degree of interference? More specifically, how can two parties to a data transfer agreement possibly question a government's binding request for access to data? These are difficult questions that the CJEU has thrown to those involved in global data flows, but their answers may not be as problematic as we think. Disproportionate access to data by governments is not just a European concern. It is a universal challenge and the measures to tackle this challenge are also universal. Contractual provisions that restrict the way in which access to personal data may be granted and measures that render personal data transferred inaccessible in practice or that apply when disclosing that data to third parties are commonly used throughout the world.

So next time you hear that Schrems II is too radical, and too difficult to implement or comply with, think about what is possible. What can you possibly do to make something that sounds disproportionate, proportionate? What steps would you take to challenge someone who may be overstepping their powers? The CJEU is not looking for heroic actions. The same is true of the European data protection authorities. They are looking for a balanced approach to doing business globally that is mindful of democratic principles, questions possible abuses of power and respects the right to data protection.

INSIGHTS: EXCLUSIVE

UK: Explaining decisions made with AI: Guidance from the ICO and Alan Turing Institute

Artificial intelligence ('AI') is a commonly used technology, and its widespread adoption increasingly raises the issue of how to ensure transparency and accountability for the underlying data processing activities involved in its use. Following the publication of a report commissioned by the UK Government in 2017, the UK's Information Commissioner's Office ('ICO') and the Alan Turing Institute were tasked with developing 'guidance to assist in explaining AI decisions,' with a view to improving transparency and accountability. The guidance, 'Explaining decisions made with AI' ('the Guidance'), was published in May 2020 and offers organisations a framework for considering how to explain decisions made using AI systems that process personal data to individuals. Bridget Treacy and Olivia Lee, of Hunton Andrews Kurth LLP, examine some of the data protection challenges associated with using AI systems and how the Guidance helps to highlight some of these challenge, such as ensuring transparency.

The use of personal data in AI systems

The Guidance describes three key phases of AI development during which personal data is likely to be used: training, testing, and deployment. During the training stage, data is fed into the AI system, enabling it to identify associations between data points, and to build a framework of understanding. This can be achieved through 'supervised' learning, where the AI system is taught to recognise associations between pre-labelled data points (e.g. pictures of animals labelled as such), and to reproduce these patterns using the rules it has learned. Alternatively, the training may involve 'unsupervised' learning, where the AI system is not provided with pre-determined associations but is instead fed a large data set and left to identify patterns, similarities, and anomalies on its own. AI systems can also be taught through 'reinforcement,' whereby the system is either punished or rewarded for the steps it takes to solve a problem, enabling it to develop problem-solving strategies to maximise its rewards. Whichever type of learning is used for training, the training phase requires a significant amount of data.

During testing, data is used to check the accuracy of the AI system's understanding. In the deployment phase, data related to the use case under examination is fed into the AI system, and the AI system generates output, in the form of a classification, prediction, or recommendation. This output allows a decision to be made, either by the AI system itself, or by a human assisted by the AI system's output.

Data protection issues raised by AI systems

The use of personal data in AI systems raises a number of data protection compliance issues under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Data Protection Act 2018 ('the Act'). Most obviously, the use of personal data invokes several transparency requirements, such as the notice requirements under Articles 13 and 14 of the GDPR. These provisions require that individuals whose personal data is processed are provided with information related to that processing, including the purposes of the processing, the applicable legal basis, and the recipients with whom the data is shared. Organisations that process personal data must also inform individuals of their rights in relation to their personal data, such as rights of access and the right to object to processing.

In addition to the general transparency requirements, Articles 13 and 14 of the GDPR specifically address automated decision-making, including profiling, that produces legal or similarly significant effects (e.g. decisions made or profiling conducted by an AI system). Where automated decision-making is used, the individual must be provided with meaningful information about: (i) the logic involved; and (ii) the significance and envisaged consequences of the automated processing for them.

Individuals also have a qualified right not to be subject to solely automated decisions under Article 22 of the GDPR. Similar provisions are set out in the Act in relation to data processing by law enforcement and intelligence services.

Further, transparency is one of the core data protection principles in Article 5 of the GDPR, which requires that data be processed lawfully, fairly, and transparently. Also of relevance are the accountability obligations under Articles 5(2) and 24(1) of the GDPR, which require organisations to demonstrate compliance with the GDPR. In this context, organisations need to be able to show that they have treated individuals in a fair and transparent manner when using AI systems to make decisions about them. The Guidance emphasises that providing explanations regarding AI-assisted decisions to individuals is one way to demonstrate that these requirements have been met.

> **The core purpose of the Guidance is to help organisations explain decisions made by AI systems to those who are affected by them, with a view to improving transparency and accountability.**

Challenges in ensuring transparency and explainability

Ensuring transparency and explainability can be challenging in the context of AI systems. These systems are often designed to solve problems and spot patterns beyond the capability of humans, and the manner in which they achieve this may not be fully understandable to those deploying the AI, let alone explainable to those whose personal data is utilised. In addition, AI systems may provide unexpected outputs, changing the nature of the processing first envisioned by their designers. As

such, providing information that is both comprehensive and comprehensible to individuals may amount to a near-impossible task at times. A balance needs to be struck between providing sufficient information to allow individuals to understand the nature of an AI system's processing activity, without overwhelming them with technical details that, while relevant, may obscure rather than clarify.

The Guidance suggests that organisations use both process-based and outcome-based explanations of their AI systems

The Guidance describes the benefits of pursuing transparency and explainability. Besides the obvious avoidance of enforcement by regulators for non-compliance with data protection law, a comprehensive explanation of data use is likely to reassure consumers that their personal data is used responsibly, increasing consumer trust. At a wider level, better public awareness of how AI systems use personal data may promote more constructive debate and involvement in their design. Better awareness also enables individuals to exercise their rights and places the interests of individuals front-and-centre in the minds of those designing and deploying the technology. Furthermore, better public awareness encourages those designing and deploying AI systems to maintain full oversight of the systems, in order to be able to provide such explanations. As a by-product of this approach, overseers are likely to have better insight into how and in what respects an AI system falls short of expectations, enabling them to remedy deficiencies and address any discriminatory outcomes caused or exacerbated by the technology.

If interpreted too stringently in the context of AI, however, transparency requirements may also raise some risks. The Guidance notes that incomprehensibly detailed explanations of AI may hinder more than help a layperson's understanding of the system, increasing public distrust. AI systems, particularly proprietary systems, can be extremely valuable to companies. Divulging extensive information regarding their use may risk revealing sensitive commercial or design details. Such information may also equip malicious actors to exploit or manipulate an AI system, disrupting its functioning. There is also a risk that personal data relating to other individuals whose data is processed by the AI system could be exposed if organisations provide overly detailed explanations.

Explanation types

The core purpose of the Guidance is to help organisations explain decisions made by AI systems to those who are affected by them, with a view to improving transparency and accountability. To be effective, an explanation needs to take into account the context in which it is given, and the target audience. Explanations should not necessarily be approached in the same way, and there is no 'one size fits all' formula for creating an appropriate explanation. As the Guidance notes, 'What people want to understand, and the 'details' or 'reasons' that make it 'clear' or 'easy' for them to do so, may differ.' In addition, there may be instances where one AI system requires explanation to multiple audiences, which may include staff who use the AI system to assist with decision making and who must then be able to communicate relevant information to individuals affected by the AI-assisted decisions, individuals who are affected by decisions (including vulnerable groups and children), and auditors or external reviewers who monitor or oversee the system. These groups will have differing levels of knowledge about the underlying AI system, and will require different levels of detail.

Given that the objective of the explanation is to justify a particular result to an individual affected by it, the organisation will need to demonstrate how it acted responsibly in designing and deploying the AI system, and ensuring that the reasoning behind a decision is clear. The Guidance suggests that organisations use both process-based and outcome-based explanations of their AI systems. Process-based explanations focus on describing relevant governance and best practice measures adopted throughout the design and deployment phases. Outcome-based explanations focus on a specific decision, explaining the reasoning behind a particular outcome using clear and understandable language. The Guidance recommends bearing in mind the distinction between process-based and outcome-based explanations in utilising the six main approaches to explaining AI decisions set out below. Further, to provide an effective explanation, several of the different types of explanation may be combined. Which explanation to use should be determined by considering what information will be required by all affected individuals, and the context in which the AI-assisted decision will be made.

The rationale explanation

This explanation focusses on the reasons leading to a decision, or the 'why' of a decision, enabling individuals to understand (and challenge) an outcome, or to change their behaviour to ensure a favourable outcome in future. This explanation would be helpful where AI has been used to determine suitability for a loan, for example, or access to a service, enabling individuals to understand the basis for their approval or denial and, if appropriate, counter that determination with relevant evidence. Alternatively, someone rejected by an AI system assisting with job recruitment because they lacked suitable experience could seek out such experience before reapplying.

The details most relevant to this explanation may include which factors were considered most significant by the AI system, the logic underpinning its weighing of these factors, and the way in which the AI system assesses these factors in reaching its decision – for example whether the AI categorises individuals according to specific data points (e.g. automatically rejecting job applicants without experience for roles that could be dangerous to the inexperienced), or takes a more holistic overview of the candidate, such as by weighting experience of candidates according to whether they come from affluent or more disadvantaged backgrounds, in order to identify potential rather than achievement.

The responsibility explanation

This explanation points to those accountable for an AI system, including who to contact for human review of a decision. As with the rationale explanation, this assists individuals in challenging a decision, as well as in obtaining additional information, by directing them to the most appropriate person or team within the organisation. Consequently, those responsible for the functioning of the AI system can be held to account directly by individuals, including those who deploy the AI system and also those responsible for designing and training it.

If a data subject feels that their personal data was used incorrectly, for example because the information was out of date, the AI system's operator will be the first point of contact. However if a data subject feels that the underlying algorithm is biased, either due to its design or biases in its training data, those responsible for the

AI's development and training would be more appropriate contact points.

The data explanation

A data explanation focusses on the 'what' of an AI system's output, providing information on the actual data used to reach a decision, the manner in which the data was used, and the source of the data. This assists in providing insight as to how an AI system was trained and allows individuals to challenge the specific sets of data used, or the specific data points included in the AI system's training. It may also include an explanation of how the organisation has ensured that the data used is of a sufficiently high quality, and the measures taken to minimise any potential bias.

As an example, if an AI system assists with decisions relating to university admissions, the applicant should be able to understand from the explanation which data points are considered by the AI system, such as grades, recommendations from teachers, and any other notable achievements. If the AI system includes the school attended by the student in its determination, an applicant may wish to challenge this, on the basis that it might risk discrimination based on that school's record of producing viable applicants.

The fairness explanation

This approach helps individuals to understand the steps taken to ensure that the AI system is unbiased and treats individuals fairly. This type of explanation will be appropriate where the functioning of the AI system is complex, opaque and difficult to explain. Instead of providing a technical explanation, it seeks to reassure individuals that measures are in place to ensure that they are not subjected to unfair treatment. It may include assurances that the datasets used for training were adequately relevant, diverse and representative, that care has been taken to eradicate any pre-existing biases in the training data, that the AI system has been trained to understand what a 'fair' outcome looks like, and that it is deployed by those suitably trained for the task and capable of disregarding the AI system's output if they, based on their expertise and judgment, feel the output is incorrect. Individuals may also be provided with statistics and outcomes of fairness testing.

For instance, if an AI system is designed to triage patients for emergency medical purposes, it may not be possible for doctors to explain exactly what combination of symptoms or what data from the patient's medical history caused the AI system to assign the patient to a low risk category, but instead the patient can be reassured that the AI system is rigorously tested to ensure that it does not inadvertently classify patients based on ethnicity or gender, and that the output is considered by medical professionals and is not determinative by itself. They can also be reassured that the AI system has a 99% success rate in identifying high-risk patients.

The safety and performance explanation

This explanation focusses on the measures that ensure that the AI system is designed and implemented in a manner that maximises its accuracy, reliability, security and robustness, and may also include details explaining how the AI was selected and how it compares to similar systems of the same type. The explanation may include details relating to the system's accuracy rates, how often it performs as intended, steps the organisation takes when this does not happen, and the stress-testing exercises undertaken to ensure robustness against attacks or ineffective implementation. This type of explanation may be most appropriate for more technically proficient audiences, such as statisticians or those using AI for academic research.

The impact explanation

This explanation informs individuals of how the organisation has considered and will monitor the impact of its AI system on them and on society more generally. It explains the consequences that the AI system's use may have and the measures taken by the organisation to mitigate negative impacts, or advice on behavioural changes that may result in a more positive impact for individuals.

The Guidance suggests that this type of explanation is best suited when information is being provided before an AI-assisted decision has been taken, and where individuals have a choice of whether or not to participate.

The Guidance highlights that elements of the rationality and responsibility explanations are likely to be required in most instances, although the information provided under one explanation heading may overlap with other types of explanation.

Selecting the appropriate explanation types

Determining which types of explanations to use can be extremely challenging. The Guidance identifies five key contextual factors that can assist, namely:

- Domain: the sector or setting in which AI is deployed;
- Impact of the AI system: consider impact on individuals and on society as a whole;
- Nature of the data used by the AI system: type, sensitivity, source and whether or not the data is malleable (i.e. whether it can be changed through behaviour);
- Urgency: will a decision be taken quickly using the AI system or will there be time to reflect on the output? Should some types of explanation be prioritised and delivered quickly?
- Audience: who is the intended recipient of the explanation, what do they need to know, and how can this best be communicated to aid understanding?

Better public awareness encourages those designing and deploying AI systems to maintain full oversight of the systems

The Guidance suggests that the domain factor will likely be the most crucial consideration. In scenarios in which bias and discrimination are a particular concern for individuals, such as in the criminal justice system or in relation to access to higher education, the fairness explanation is likely to be key. Those affected by the outcome need to be reassured that the AI system will operate fairly in processing their data.

Conversely, in a domain in which the potential impact on data subjects is lower, the rationale and responsibility explanations may be more appropriate. The Guidance emphasises, however, that even in sectors in which discrimination appears to pose less of a risk, AI operators should be sensitive when seeking to target specific demographics or utilise existing stereotypes, for example through targeted advertising, as this raises potential societal impacts. Providing a fairness explanation may be appropriate even when the domain appears to be low risk.

The fairness, safety and performance, and impact explanations will be appropriate for situations in which AI-assisted decisions could have a high impact, such as in the context of

medical or health-related decisions. Prioritising these particular explanations may reassure those subject to high-impact determinations that decisions have been taken fairly and having regard to the decision's likely impact on them. Where the output of the AI system is subjective and therefore more susceptible to challenge, the Guidance suggests that the rationale and responsibility explanations will also be useful. When considering the likely impact, the Guidance recommends that AI operators select the relevant explanation approach on a case-by-case basis, ensuring that the potential impact of the AI system's decision is fully understood.

Next steps

The selection of an appropriate explanation, or combination of explanation types, is the first step recommended by the Guidance, which points to the benefits of developing AI systems in an 'explanation-aware' fashion, rather than seeking to explain a system once it has been built. Viewed through a data protection lens, this approach embodies Data Protection by Design and by Default. It is also about planning ahead - given that an explanation will be required for legal compliance, the nature, scope and content of the explanation should be a consideration from the outset. As the Guidance notes, the way in which data is collected and pre-processed will have a bearing on the quality of the explanation that is ultimately given, as will an understanding of the system's design. As an example, when using the fairness explanation, organisations must consider how they will demonstrate that the data collected was representative, or whether certain factors should be weighted before processing in order to achieve a fair result. If using the impact explanation, a data protection impact assessment undertaken in relation to the AI system at the outset of the project may help determine relevant impacts to be included in the explanation itself.

Organisations must also ensure that when building or selecting an AI system, they focus on the need to ensure transparency, not merely for the compliance reasons above but to reassure consumers that their personal data is used responsibly, increasing consumer trust. The chosen model should be capable of explanation, allowing extraction of relevant information needed to inform the explanation. By way of example, the Guidance suggests selecting an optimally interpretable model when using data that relates to demographics, given the potential for discrimination, whereas for less risky data, or where the AI system will be used purely for scientific purposes, a 'black-box' AI model that limits information extraction may be sufficient.

Explainability amounts to more than merely meeting a legal requirement; it requires developers and users of AI systems to actively understand how their systems operate and to be accountable for them

Once extracted, organisations need to be able to translate what may be complex and obscure information into an explanation that is practically understandable to its audience. The Guidance suggests a number of approaches that may assist with this translation process, including visualisation media, graphics or summary tables. The Guidance also highlights that this will require judgment on the explainer's part, both in identifying which factors assessed by the AI were relevant or determinative to its output, as well as ensuring sensitivity to the data subject's specific circumstances where individuals are involved. The Guidance states: '[d]ecision recipients should be able to easily understand how the statistical result has been applied to their particular case, and why the implementer assessed the outcome as they did.' It is important, therefore, that those assigned to oversee the functioning of the AI system have sufficient expertise to make sense of the system's output.

In line with this, implementers and explainers of AI systems require adequate training and preparation in order to be able to use the AI system responsibly and explain outcomes when required. Where AI systems are used to assist decision-making, those using them should be made aware of its limitations and the importance of using their judgment to sense-check the output. Implementers must also be aware of the potential for bias, either in favour of overreliance on the AI system's output, or distrust of it, and instructed on how best to address this.

Finally, when it comes to the actual delivery of the explanation, AI users need to consider the best medium. That may be a standard privacy notice, but in certain cases delivery of the information in person may even be appropriate. A layered approach can also be used, providing access to key information upfront and making further details available if desired, to avoid overloading a recipient with technical detail. The Guidance recommends reconsidering the contextual factors highlighted above in determining the most appropriate delivery method.

The Guidance notes that the process outlined above may not be linear, and that organisations may wish to develop their own procedures for implementing explainability rather than follow the steps described above. There is also more in-depth technical guidance prepared specifically for those involved in model selection. The Guidance further highlights the specific roles and teams within the organisation that will likely play a part in the explanation process and the policies and documentation that should be implemented to support the process. This latter section targets senior management.

At a time in which there is both an increased awareness of the benefits of AI systems, and increased suspicion and scrutiny from individuals, in particular in relation to their data protection rights, the Guidance offers a welcome and multilayered approach to improving transparency, and holding organisations to account. Explainability amounts to more than merely meeting a legal requirement; it requires developers and users of AI systems to actively understand how their systems operate and to be accountable for them. As Albert Einstein said 'If you can't explain it simply, you don't understand it well enough'. This Guidance is a welcome contribution to the challenge of improving transparency and accountability in AI.

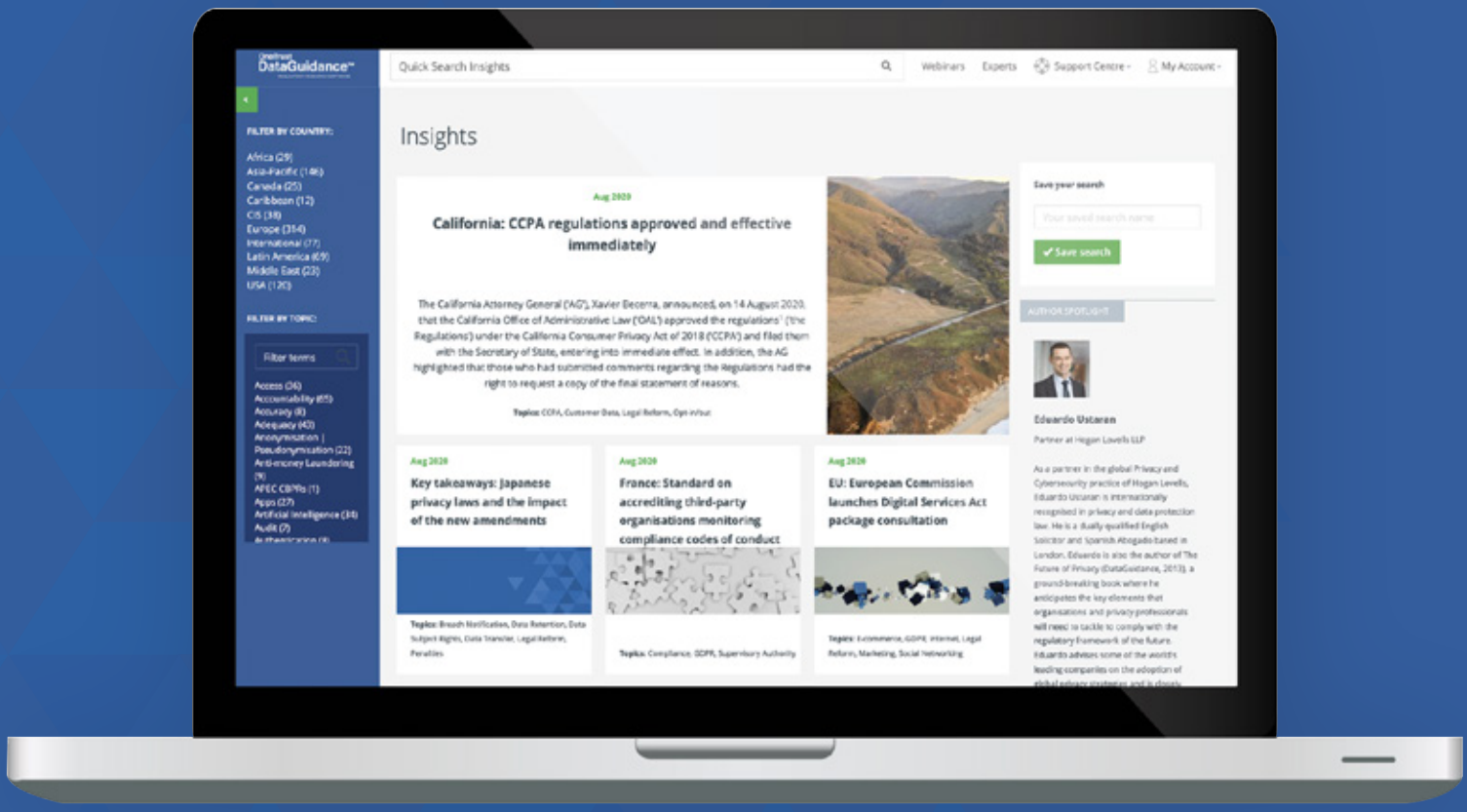
Bridget Treacy Partner

btreacy@HuntonAK.com

Olivia Lee Associate

olee@huntonAK.com

Hunton Andrews Kurth LLP, London



An In-Depth and Up-to-Date Privacy and Security Regulatory Research Platform Featuring:

- 40 in-house privacy researchers and a network of 500 lawyers across 300 jurisdictions
- Two decades of global privacy law research
- Regulatory information on hundreds of global privacy laws & over ***10,000*** additional resources

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Access for Free

Privacy Talks

Jason Burns is the EU Data Protection and Governance Lead at Bristol-Myers Squibb. He has a wealth of experience designing, leading, and overseeing data protection and information security governance frameworks.

OneTrust DataGuidance spoke with Jason in February 2020 regarding privacy program management, GDPR compliance, the interaction between pharma-specific and privacy laws, and how technology can facilitate data protection.

Privacy programs

Privacy programs are not necessarily specific to pharmaceuticals. This goes for all companies, but if you are serious about data protection and creating a proper program, it starts with the team. You need to have a team that is first of all interested in data protection and has an understanding of the business. These are the people that are running the applications and running the programs and that are delivering projects within the company that are pushing the company forward and creating more business. So, we need to have a team that has got the personnel skills and the personality to be able to push through what we need to happen from a regulatory point of view, whilst not talking about it in a regulatory kind of way. They also need to make sure that we're not blocking anything as we're not strictly compliance either, and because the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') can sometimes be not terribly specific or prescriptive about what you should do. So, it's working with teams, bringing them on board, understanding what they're trying to do, not just laying down the letter of the law but working with them. We're evolving as a team. We've certainly learned a huge amount since we started up officially a year and a half ago.

It is necessary that the team learns about the GDPR, alongside us, as an organisation and as an industry, as well as having the freedom to make calls and things. We're very process-heavy and documentation-heavy, we audit everything, we've got key performance indicators, and we have all those things, but the team needs that personality in place of, 'we're all in this together and we're here to help and to work with people,' I think that's absolutely key.

In terms of setting up a program, I'm a big believer in the high-level strategy that is meaningful without just slogans for the sake of having them. So, for example, Privacy by Design and Default, and understanding what that actually means. It's a nice thing that my boss said to me a couple

of weeks ago and there's a genuine view of, 'OK, we're doing data protection, we do it quite well, but let's be the best that we can.' It's not a kind of a glib statement either, we're always trying to move forward, whether we're implementing new technology to help us do things, working with teams to better understand what they do so that we can update how we interact with them, and so on.

It's difficult to sometimes see the wood for the trees when you're focusing at a very low level: you're dealing with thousands of tickets, we're well over the 1,000-mark number in a short space of time; and there's new challenges all the time. You can lose sight of what it is the team is meant to be doing as a whole, so that's the really important thing. Having those kinds of high-level things that everybody's bought into, and then you can always trickle up if there is a decision to be made about what we prioritise and all that, it should filter up to what we decided at the beginning.

We're lucky at Bristol-Myers Squibb that we've got a lot of buy in and definitely financially there's a lot of money put into the team. So there's a belief there that what we're doing is important, but there's a general view that we're taking this very seriously and we took that approach from the get go as the GDPR is a really serious regulation. We do not want to be a pharmaceutical company that's being casual about this in any way, pharmaceuticals don't tend to take regulation casually anyway, but we're lucky to get that buy in as a lot of organisations don't have it. But again, the personality skills to be able to have those conversations, maybe build those relationships, it's going to be worth much more than having a privacy program that's just in paper only, and you don't have any support to actually carry it out.

Operational challenges

The local grounds for processing: a good example of that is something that I think the pharmaceutical industry is struggling with at the moment, clinical trials. There is a consent that you need for a patient to partake in a clinical trial and up to now, a subset of that was, as part of this, you agree to your information being used for the purposes of the clinical trial, but it never mentioned anything else that you might want to know about, such as the information being very, very useful for scientific research and the betterment of public interest, and so on so on, and for their benefit as well as legitimate interests.

There is lots of legal grounds that could have been used, but when consent is used you're tied then to that consent and if somebody withdraws it then that could invalidate the secondary uses of that data in the trial. So, there is consent needed for pharmaceutical regulatory purposes in clinical trials, but then there's what we need to make the best use of that data to make the best medicines that can help people. So, it's coming up against these issues where it's hard sometimes to build consensus among all the different stakeholders and discuss what should we actually do. And that's where the data protection office is young, it hasn't been around for that long, but we're starting to get a position now where we need to take the role and make the decision on that, and that's getting there. But that's the challenge and it's something that's evolving.

In terms of the challenges that we've had with ticketing: there's two aspects to it. We have employees requesting or using the GDPR for issues they might have with a company, a legal dispute in some way, so we can defer to the legal team a lot and work closely with them. But then we just get blanket requests. They're small in number, but huge in terms of complexity for us and trying to manage that. Giving somebody access to 60,000 or 70,000 emails, it's not good for them, it is not good for us, but sometimes we get those requests. I suppose the spikes that we've had where we've really been pushed to the limit is where local markets, for whatever reason, decide to engage in a weak consent program or they're communicating with healthcare professions that previously, we wouldn't have had a good relationship with. Then, the data protection office gets inundated because we've made it easy to contact us, so we get these 100's of requests.

This time last year was kind of horrific. It was seven days a week and it was 'tell me everything you've got, delete everything you've got,' and they didn't really know why they were asking that, they were just annoyed, or they didn't know why they were contacting us. And then we had to go through the whole process again to get them back into our system. So, that goes back to the legal basis, as well as finding out if there are other ways that you can, if you want to, communicate with people around this, and also to be sure of what you're communicating about and clear on your own legal basis. I wouldn't use this terminology, but to say, 'look, help us to help you, we're doing this because we think it benefits us. And we were being clear about that. Do you agree. Do you not agree.'

> **If you are serious about data protection and creating a proper program, it starts with the team**

There are multiple different ways of doing it, rather than going in legally: 'you consent to this and this because you've read this, you're going to do it.' We're trying to move away from being heavily legal and the focused terms of our language and all. But definitely spikes and tickets because of local action, such as local level employee requests which are difficult, but just also the complexity of a company like Bristol-Myers Squibb. It's difficult, especially as a US-based company, to get into the GDPR and whether it's a good thing. But it's not just a regulation or a one-time thing. This is an ongoing thing. There's not one law for the whole of Europe either. There are local employment laws that affect different laws in France and Germany depending on what type of clinical research you're doing, and so on. That's the debate that we've been running into at an operations level.

Jason's interview was part of the Privacy in Motion: Health and Pharma series. Visit the OneTrust DataGuidance video for related interviews and more.

www.dataguidance.com/videos

Schrems II: Post-Schrems II guidance on data transfers from the LfDI Baden-Württemberg

In the wake of the Court of Justice of the European Union's ('CJEU') judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (Case-311/18) ('the Schrems II Case'), the future of international data transfers hangs in the balance, with EU supervisory authorities playing a crucial role in shaping the case's impact. Dr. Carlo Plitz and Philipp Quiel, Partner and Senior Associate respectively at reuschlaw Legal Consultants, discuss recent guidelines published by the Baden-Württemberg data protection authority ('LfDI Baden-Württemberg') on 24 August 2020[1] and the updated version of the guidelines published on 7 September 2020[2] ('the Guidelines'), covering topics such as additional measures usable when transferring data to the US through Standard Contractual Clauses ('SCCs'), among other things.

On 24 August 2020, the LfDI Baden-Württemberg published the Guidelines, addressing international data transfers following the the Schrems II Case. The Guidelines explain under which conditions data transfers to third countries are legal, provide a checklist for companies transferring data, and recommend additional safeguards and changes to specific clauses of the SCCs that could ensure compliance with Chapter V of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). In the following, the Guidelines of the LfDI Baden-Württemberg are summarised, as well as the next steps companies should take according to the Guidelines and which enforcement actions the LfDI Baden-Württemberg plans to take.

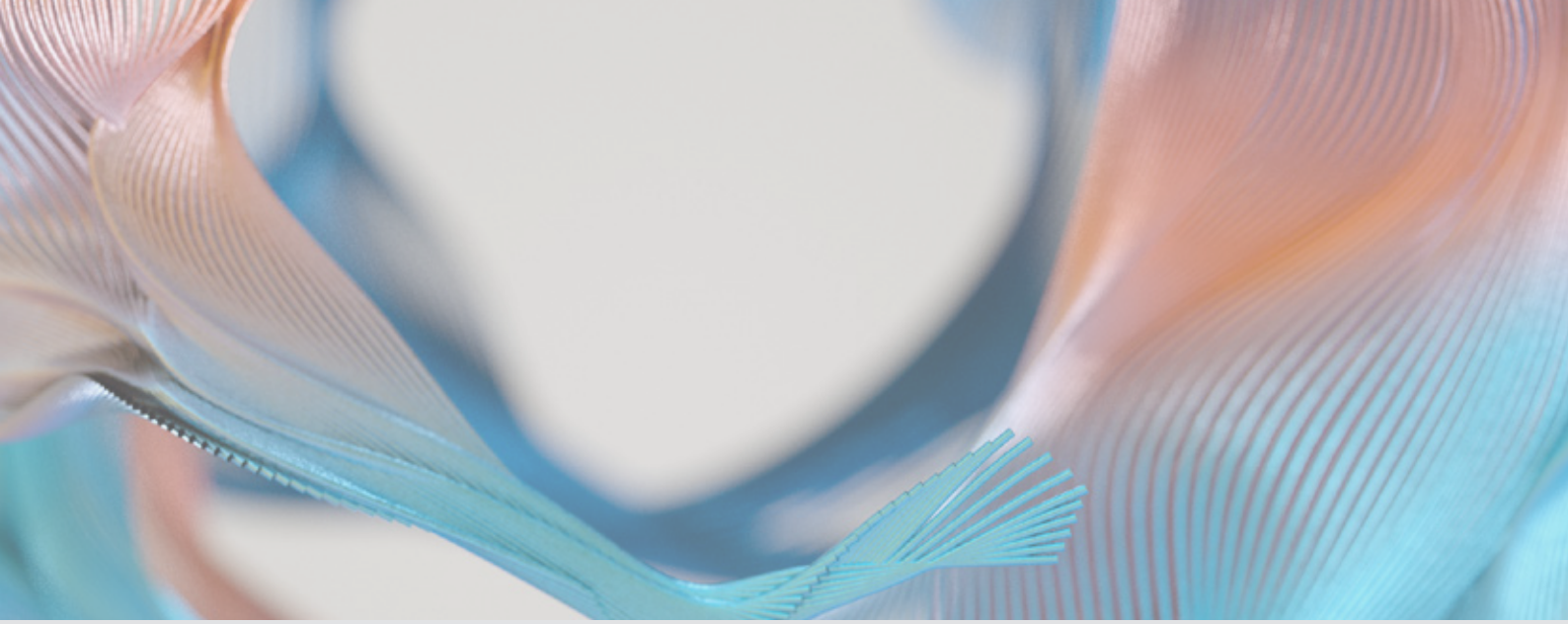
Opinion of the LfDI Baden-Württemberg

As one of the first statements, the Guidelines recall what has been written and said many times after the judgment was published: data transfers based solely on the EU-U.S. Privacy Shield ('the Privacy Shield') are no longer lawful, since the Privacy Shield was declared invalid by the CJEU with immediate effect. In contrary to what companies that are located in the US may hear from the U.S. Department of Commerce, data importers continuing to rely on the Privacy Shield is not of help for ensuring that data transfers meet the conditions set out in Chapter V of the GDPR. The Guidelines stress that the Privacy Shield is not a valid transfer mechanism anymore and that if companies continue to rely on it, they are illegally transferring data and are risking fines and compensation for damages.

The Guidelines also emphasise that, in general, SCCs are valid, but that it must be ensured that the level of protection in the third country is appropriate in relation to the level of protection guaranteed under EU law. This makes sense, since under the SCCs both contractual parties agree to follow applicable European data protection laws; that is, the GDPR.

Within the Guidelines, it is also made clear once more that in order to be able to rely on SCCs or other appropriate safeguards such as Binding Corporate Rules ('BCRs'), there must also exist enforceable data subject rights and effective legal remedies for data subjects in the third country. The Guidelines stipulate that SCCs cannot bind authorities of third countries. It also recalls marginal 135 of the CJEU's judgment and highlights the importance of being aware of national laws which conflict with obligations under the SCCs. In cases where authorities, in accordance with the law in the third country, are authorised to intervene in the rights of data subjects, additional safeguards must be implemented. If in those cases, additional safeguards are not implemented, then there is no adequate level of protection. The Guidelines emphasise that this must be assessed on a case-by-case basis, taking into account whether the law of a respective third country provides enough protection and, where this is not the case, implementing additional measures to ensure an adequate level of protection.

Regarding the territorial scope of the implications of the CJEU's judgment, the Guidelines stress that this extends beyond data transfers to the US, also impacting every third country without an adequacy decision in the meaning of Article 45 of the GDPR. However, the Guidelines also explicitly mentions that the situation regarding data transfers to the US is currently very complicated: 'Using SCCs is therefore only possible for transfers to the USA in very limited cases and only with additional guarantees



(e.g. encryption).' Companies must be able to protect data from access by US intelligence agencies and for that should consider using:

- encryption, where only the data exporter has the key, and which cannot be broken even by US services; and/or
- anonymisation of all data, where only the data exporter can match the information with the data subject.

It is positive to note that the Guidelines make a concrete proposal here. Nevertheless, it remains unclear to what extent companies can effectively protect data from being accessed by intelligence agencies. It is also worth noting that pseudonymisation, where only the data exporter can match the information with the data subject, was mentioned in the first version of the guidelines, but is not mentioned in the updated Guidelines.

As one possible transfer mechanism, the Guidelines refer to Article 49(1) of the GDPR, but at the same time also recall the narrow interpretation of the scope of Article 49 by European Data Protection Board ('EDPB') within the Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679[3]. In general, the Guidelines stress that an exception should not become the rule. As an example of a data processing activity for which Article 49(1) of the GDPR can be used as transfer mechanism, the Guidelines refer in abstract to data transfers within company groups.

Checklist for data transfers and proposed changes to SCCs

One part of the Guidelines which may be particularly helpful for companies is the checklist provided under 'IV Where should I start? / checklist.' The Guidelines state that companies should immediately take the following steps:

- create an inventory of the cases in which your company exports personal data to third countries, this may include also mere access rights by private or public bodies in third countries to data held by you, so a physical export of the data is not necessary;
- contact the company's service providers in third countries and inform them about the judgment of the CJEU and its consequences;
- check and adjust (e.g. if the Privacy Shield is still named as transfer mechanism, this must be deleted) your data protection policies, especially regarding informational duties under Article 13(1)(f) of the GDPR; information must be provided not only about the fact that data is transferred to a third country, but also what exact mechanism from Chapter V of the GDPR is used;
- check and adjust your records of processing activities regarding data transfers;
- immediately instruct all processors who transfer data to the US based on the Privacy Shield or process personal data there, in writing or by email (as required by the relevant contract), to suspend the transfer of personal data to the US with immediate effect until your processor or its sub-contractor has ensured a level of data protection there that complies with the GDPR, for example by using alternative processing and transfer mechanisms;
- inform yourself about the law applicable in third countries (data protection laws of the third country; access to your data by state authorities including the secret services; rights and legal protection options available to you, the data importer and the data subject; jurisdiction and official practice in the third country with regard to the level of data protection); public bodies, such as the DPAs, the EDPB, the EU Commission and the foreign office should be able to provide information;
- consider whether you can avoid transferring data to third countries by: (i) using only services that do not transfer data to a third country; (ii) entering into a contractual agreement that no data will be transferred to a third country; or (iii) encrypting the data and having sole access to the key; again, the entire legal situation in the third country must be taken into account (e.g. national regulations on access to data outside of the country's own territory, see US Cloud Act;
- assess whether there is an adequacy decision for third countries the company is transferring data to (the Commission has issued a list of such countries[4]);
- assess if SCCs can be used for the respective country, this will not be the case if authorities or other bodies in the third country can interfere in a disproportionate manner with the rights of the data subjects (e.g. mass retrieval of data without informing the data subjects and without procedural safeguards such as a court decision requirement) and if there is no effective legal protection for the data subjects; and
- assess if additional safeguards can be implemented.

Furthermore, the Guidelines add that, 'in order to demonstrate and document willingness to act in accordance with the law,' companies should contact the recipient of data from the EU and agree to certain amendments of the clauses of the SCCs. It is worth noting

that the Guidelines do not say that the proposed actions for companies and additional measures are indeed able to ensure an adequate level of protection. It rather provides a recommendation for demonstrating 'willingness.'

In the first version of the guidelines, the wording 'amendments' on the one hand and 'addition' on the other hand used in some sections of the initial draft was criticised by some legal practitioners in Germany, since amended SCCs cannot be used without prior authorisation of a data protection authority. Others argued that the changes to the SCCs initially proposed are not amendments as such, but separate agreements between the parties on additional obligations, similar to any obligations under data processing agreement according to Article 28(3) of the GDPR. Within the updated version, by using a different wording the DPA tries to make clear, that it only meant additional agreements and not changes to the SCCs. Per the Guidelines, companies should contact the respective recipient of the data and agree in particular on the following changes to the provisions of the SCCs:

- Addition to annex to clause 4 f: Information provided to the data subjects not only when transmitting special categories of data, but when any data transfer (before or as soon as possible after the transfer) to a third country which does not provide an adequate level of protection within the meaning of GDPR is carried out.
- Addition to annex to clause 5 d i: Obligation for the data importer to inform without delay not only the data exporter, but also the data subject (where known that certain people are affected), of any legally binding request by an authority for the transfer of personal data to the authority – inclusion of this addition in the third-party beneficiary rules, in addition to clause 3 paragraph 2; if providing this information to data subjects is prohibited, for example by a criminal prohibition to maintain the secrecy of the investigation in case of criminal investigations, you must contact the data protection authority and clarify how to proceed further. In these cases, the data importer shall be obliged to regularly provide the data exporter with general information on requests received from authorities concerning personal data processed under this contract (at least number of requests, type of data requested, requesting party).
- Addition to annex to clause 5 d: Addition of the obligation of the data importer to take legal action against the disclosure of personal data and to refrain from disclosing the personal data to the respective authorities until a competent court of last instance has issued a final judgment ordering the disclosure of the data – inclusion of this addition in the third-party beneficiary rules, in addition to clause 3 paragraph 2.
- Addition to annex to clause 5 h: Addition of the obligation of the data importer, if known to him/her, to also notify the data subject of the assignment of a processing order to a sub-processor – inclusion of this addition in the third-party beneficiary rules, in addition to clause 3 paragraph 2.
- Addition to clause 6: Adding that a data subject who has suffered damage as a result of a breach by a party or the sub-processor of the obligations referred to in clause 3 or 11 is entitled to obtain compensation for the damage suffered not only from the data exporter but also from the data importer.
- General addition: Adding an obligation on the data importer to indemnify the data subject from all damage caused by access to the data of the data subject by authorities in his country, regardless of fault given or not given.
- Addition of the example for a compensation clause that is set out in Annex 2 of the SCCs.

In the initial draft version of the guidelines, the DPA also proposed a change to annex to clause 7 (1) b that governed a referral to the courts of the Member State in which the data exporter is established, in case of dispute where the data subject exercises towards the data importer third party beneficiary rights or claims in accordance with the clauses. This additional clause is not mentioned in the guidelines anymore.

Next steps the LfDI Baden-Württemberg will take in enforcement

At the end of the Guidelines, the the LfDI Baden-Württemberg shares information on its next steps in enforcement, stating that: '[...] at the centre of the further procedure of the LfDI Baden- Württemberg will be the question as to whether there are reasonable alternative offers to the service provider/contract partner selected by companies without transfer problems. If you are unable to convince us that the service provider/ contract partner with transfer problems you are using is not replaceable by a reasonable service provider/ contract partner without transfer problems in the short and medium term, the LfDI Baden-Württemberg will prohibit the transfer of data.'

Within this statement it becomes clear that, on the one hand, the LfDI Baden-Württemberg understands that in some cases there are little to no alternative services offered. On the other hand, there is still a requirement that companies be able to convince them that such a situation is indeed the case.

Furthermore, the Guidelines acknowledge the large amount of effort that companies can incur by the current legal situation on data transfers: 'We are aware that the ruling of the CJEU may possibly entail extreme burdens for individual companies. The LfDI Baden-Württemberg will base its further action on the principle of proportionality. We will continue to monitor developments and will continuously review and develop our positions accordingly.'

Overall, the Guidelines are helpful for companies, as they now know what the position of the LfDI Baden-Württemberg is and how it plans to enforce the current legal situation. Companies under the supervision of the LfDI Baden-Württemberg that follow the Guidelines can probably expect the same to be satisfied with the companies' actions over the next few months.

Dr. Carlo Piltz Partner

carlo.piltz@reuschlaw.de

Philipp Quiel LL.M. Senior Associate

philipp.quiel@reuschlaw.de

reuschlaw Legal Consultants, Berlin

1. Only available in German at: https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-lfdi-bw-was-jetzt-in-sachen-internationaler-datentransfer/
2. Only available in German at: https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-lfdi-bw-was-jetzt-in-sachen-internationaler-datentransfer/
3. See: https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_en
4. See: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

ONETRUST FREE SCHREMS II VENDOR ASSESSMENT TEMPLATE

Operationalize the Schrems II decision today with free templates to help assess vendors and SCC validity. OneTrust's Schrems II Solutions help organizations:

- Identify data transfers and the mechanisms relied upon
- Assess vendors relying on SCCs with pre-built SCC validation templates
- Reduce the burden of vendor assessments through pre-completed assessments
- Manage contract updates and vendor on-boarding and off-boarding
- Get instant alerts on new Schrems II guidance

OneTrust

PRIVACY, SECURITY & GOVERNANCE

Get Started Today

USA: CMMC as competitive advantage and five things you can do today

Historically, the United States Department of Defense ('DoD') and its allies have been very vigilant in protecting their classified information. Over the years, the DoD has been turning its attention to providing the same level of focus and rigor to unclassified but sensitive information held by its contractors and suppliers. In January 2020, the DoD released the Cybersecurity Maturity Model Certification ('CMMC') specifically targeted at improving the security posture of defense contractors and their subsidiaries. Prior to this, compliance was through self-assessment. After many incidents and increased risk, it was time to ensure consistency while implementing a carrot and stick rewards system. Alex Sharpe, Principal at Sharpe Management Consulting LLC, who consults on cybersecurity, privacy, digital transformation, disruption, and other areas, draws on his experiences and provides insight into the CMMC, its advantages for organisations, and the key steps businesses can be taking to prepare.

CMMC

In principle, the CMMC is not all that different to other models. The difference lies in the impact to your business. Solicitations are being released which require bidders to be certified at a given level. The CMMC is not just a statement of your capabilities and risk but also a license to play in the big game.

The CMMC has lots of teeth and you do not have choice. Contractors and suppliers who do not achieve certain levels will not be allowed to bid on or be awarded a contract. For most, this will be Level 3 (Good). For some, it may be Level 1 (Basic). For the very select few, it will be Level 5 (Advanced).

Small business heads up

Word has it the Small Business Administration ('SBA') will be using the CMMC as the basis for a non-defence maturity model. Small businesses are being targeted more frequently and are more likely to go out of business after being attacked. It is not a bad idea to have a professional help you with an assessment.

Don't wait

Many contractors and supplies are waiting for the DoD to dot all of the i's and cross all of the t's before starting. This is a big mistake for three reasons:

1. First mover advantage. Non-compliance prohibits your competition from bidding or being awarded a contract. Being compliant gives you an instant edge. Why not start now and take the win?
2. You will fail and you will need to remediate. With very few exceptions, deficiencies will be found and you will need to remediate. In my experience, it is safe to say remediation will take at least six months. Do you really want to put your business on hold or give your competition an edge for that long?
3. Audits and assessments are hell. Unless you have been through something like this before and you are a machine, this is going to cause stress. It is estimated 300k contracts and vendors will need to be assessed. The overwhelming amount are privately held and have never been through a third-party audit or assessment before. Look around, the large firms are already preparing. Have you asked yourself why? Because they know what is coming. Why not learn from those who came before and stand on their shoulders?

Low cost things you can do today

The really good news is the mechanics of audits and assessments are very predictable by design. Having been on both sides of the fence for security, privacy, IT, financial and compliance audits and assessments along with their remediations, I can tell you the basic principles are predictable. And guess what: the most common headaches and why organisations fail is also predictable. Nothing can prepare you for the shock of having an outsider giving you the cybersecurity equivalent of a cavity check. We can help you prepare. Below is a list of the top five items auditors ask for, want and need but many organisations cannot produce.

The absolute best thing you can do and the best investment you can make is to have a trained third party perform a cybersecurity assessment using the National Institute of Standards and Technology's ('NIST') Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organisations[1].

Top five needed items

One of the first things the assessor will do is provide you a list of items for you to produce.

Hint: Ask for the list before they arrive. In my experience, below are the top 5 most valuable items that an organisation needs to produce.

1. Asset inventory and network diagrams

Don't laugh. You would be surprised to learn how many organisations cannot produce a network diagram. In the worst case, your IT folks will have something whether they admit it or not. Be sure it shows all internet connections and connections to different providers outside of the enterprise - Cloud, SaaS, PaaS, IaaS, trading partners, vendors, etc. Most organisations have a pretty good map of what is inside the perimeter. Fewer than you would think have mapped out what lies outside. In this highly connected world with more remote workers than ever, there is often more outside of the walls than inside the walls.

Asset inventories also tend to be a problem. There are many tools and techniques for keeping track. Here is a hint that always works for me. Ask your accounting department. Why? With few exceptions, everything you have is either owned or leased. If it is owned there will be a record of the purchase and most likely a depreciation schedule. If it is leased, there will be a contract and a record of payments.

2. Written policies and procedures

Straightforward, right? Well, firms often fall down in one of two ways. The most common is they do not have an inventory of their policies and procedures. Typically, an assessor does not want to review every document. Rather, they will look to see what you have, review the key items in depth and randomly select others.

Do yourself a favour, pull a copy of NIST SP 800-171 and verify you have what is required. If you would like to dig a bit deeper take a look at NIST SP 800-53[2] and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012[3].

Hint: One of the first things I ask for is a written Information Security Plan. The first thing I do is to check the last time it was updated. Be sure yours is current.

3. Flow diagrams and process mapping

Knowing what assets you have and how they are connected is great. Knowing the sensitivity of the information, where it is stored and how it is shared is golden. If an assessor does not ask for it, they will love you for handing them one.

Many organisations will say, this is not required to properly secure the enterprise. That might be true for small shops but not for any enterprise of any size. There is a good chance, the exercise to produce these diagrams and to map these processes will make your business stronger and more secure.

Hint: The CMMC defines two types of sensitive data. Keeping this in mind while mapping out your enterprise will help you in the long run.

4. List of technical controls, safeguards and owners

In the end, it is all about controls and who owns them. Make the investment to map out the controls, the safeguards and the owners. It will be a good self-check and will help the assessor move through your assessment easily with minimal disruption to your business.

5. List of mitigations and remediations completed

There is a good chance you have been through some sort of assessment or audit. Even if it was a self-assessment or because of a data breach. Be prepared to show the results and your remediation.

Added bonus: a sixth item for good measure

Enterprises have become more and more reliant on third parties. Hackers know this, penetrations through third parties are on the rise. Some have made national news. Be prepared to produce the due diligence performed on your third parties including the contracts.

Closing remarks

The CMMC is being done for all of the right reasons. In the end, it will make your business stronger and the world a safer place. Near term, jump on it early and turn it to your advantage. Get ahead of your competition.

Alex Sharpe Principal

alex@sharpellc.com

Sharpe Management Consulting LLC

1. Available at: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
2. Available at:https://nvd.nist.gov/800-53
3. Available at: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm


Regulator
Spotlight

OneTrust DataGuidance spoke with Dr. Marie-Louise Gächter-Alge, Data Protection Commissioner of the Principality of Liechtenstein, in December 2019. Dr. Gachter-Alge discusses the list of activities requiring a DPIA, areas that organisations should be aware of in regard to the new law and the authority's recommendations regarding legitimate interest and other grounds for lawful bases of processing.

What should organisations be aware of regarding the new law and ordinance?
The national data protection law and ordinance entered into force on 1 January 2018, so what's really new in these two laws. For example, regarding video surveillance, organisations need to notify the authority if they want to have more video surveillance of publicly accessible places or areas, so that's new.

Then, something that was very important in Lichtenstein is that the issue of secrecy applications that ease secrecy, professional secrecy, and so on, prevails over the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). This concerns the rights of data subject whenever there is a secrecy obligation that prevails.

There are several provisions regarding public authorities, especially when it comes to the transfer of data from one authority to another one. This is a very important point of our law and as far as our approach shows it's a very important issue in the daily work of the authorities in Liechtenstein.

So, these are the main issues that are new in the law.

Our experience so far is that most companies are aware that there is an obligation to do a Data Protection Impact Assessment, but doing that in practice is a problem

Your authority recently sent a questionnaire to various organisations regarding compliance with the GDPR. Are there are particular trends that you have noted and that other organisations should be aware of?
We got all our replies back, however, we are not really satisfied with all the answers, and around three out of 10 answers are not sufficient. Therefore, we had to contact the companies again and ask them to resend the information for the answers because it's not sufficient for us and we can't work with that. This was a bit disappointing, especially when you look at the questionnaire, it's a questionnaire that refers to the nine steps we've published on our website, so it shouldn't be new to companies because they find all the templates there and the information. They should know what to do so it was a bit disappointing that this very basic questionnaire seemed to be a challenge for several companies, it shouldn't have been the case. We haven't looked into the details yet, but the first impression was a bit disappointing just with regard to some of the companies, it was not to all.

Your authority also released its list of activities requiring a DPIA. What are the main takeaways for organisations in this respect?
We published a blacklist, we do not have a white list as we don't consider that necessary and helpful for the companies, but we have the blacklist of course. Our experience so far is that most companies are aware that there is an obligation to do a Data Protection Impact Assessment ('DPIA') but doing that in practice is a problem.

For many of the companies, it's the question of where to start and how to do it. We recommended the tools from the French data protection authority ('CNIL'), and then the questionnaire from the UK's Information Commissioner's Office which we translated into German as well, and adapted to the situation Liechtenstein. We have got these tools available on our website with lots of information, but we see it's how to start the DPIA. That's the problem for the companies and that's why we decided to go a step further and publish another tool that is a tool where another questionnaire, drafted by my colleagues, which should help companies to know whether they have to conduct a DPIA or not. So, it's one step ahead and apparently this is the problem. There is a blacklist and there is information given on our website and there is the GDPR as well, but it's just how to start, that's the problem.

We have also planned a workshop for 2020 where companies can come and we'll look at their cases. It's a bit like getting back to university where you have your seminars with the cases, and you work with your professors on the case as well. In this case, this won't be a professor, but my colleagues will have several groups and say that companies can come and do a DPIA with my colleagues and then they should know how to do it.

What have been your recommendations regarding legitimate interests and other grounds for lawful bases of processing?
Legitimate interest is just one of the six legal bases that are possible to choose, and consent is one which is a bit controversial because it's not always easy to implement it. We recommend choosing one of the others

CONTINUED

Dr. Marie-Louise Gachter-Alge, Data Protection Commissioner of the Principality of Liechtenstein

and one of the others is the 'legitimate interests,' but they are, from my point of view, controversial as well because it's difficult to know what the exact content of legitimate interests is and you have to ask yourself lots of questions before you can be sure that you can rely on these interests, then even if you think you can, in the end it can be different. We try to give some guidance, nevertheless it's up to the companies or institutions to ask these questions and to come to a conclusion.

Some of the questions we receive regarding legitimate interest concern marketing. This is a big issue. What's allowed and what isn't allowed. There are still many questions which haven't got an answer yet.

It's difficult to know what the exact content of legitimate interests is and you have to ask yourself lots of question before you can be sure that you can rely on these interests, then even if you think you can, in the end it can be different

Are there other areas and topics that your authority has been working on that you would like to draw attention to?
Important issues in our daily work include the DPIA as this is a big issue.

Another issue is the question concerning cookies because we've got a very special situation Liechtenstein now, which is different from the EU countries, because there is the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) ('the ePrivacy Directive') which was implemented by Liechtenstein but then there was the amended version from 2009 and this one was not implemented.

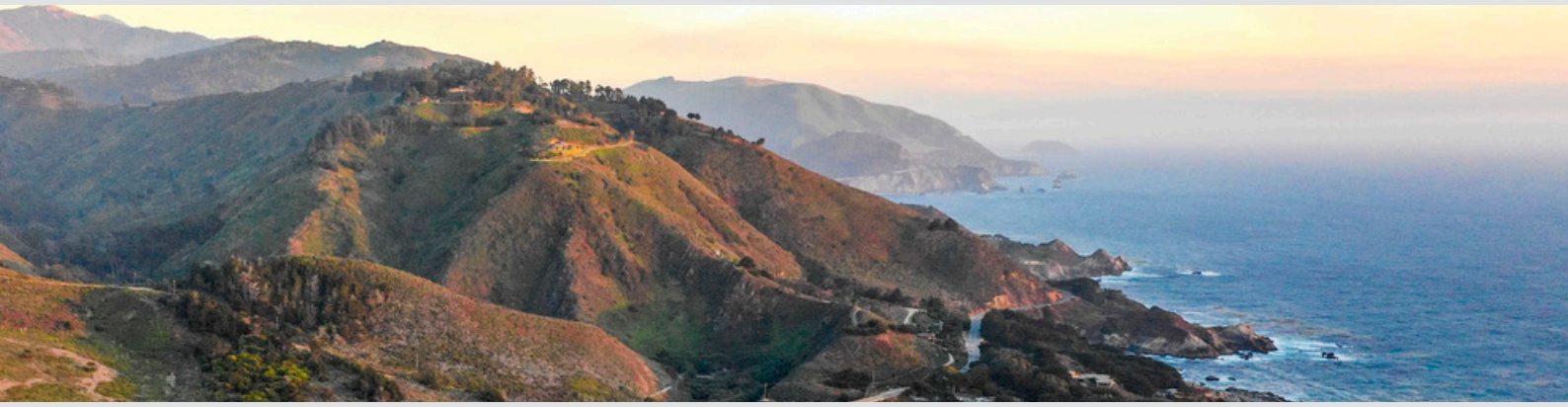
As well as this, the Planet 49 Case, which concerned the amended version of the ePrivacy Directive from 2009, doesn't exist in Liechtenstein, so the conclusion of the Court of Justice of the European Union ('CJEU') in the case doesn't apply in Liechtenstein and we have got a situation that is different from the other countries, that is we do not have consent and as consent doesn't exist in our legislation, we can't apply the CJEU decision. So, there are some kind of cookies which need consent and we have the only legal basis that helps us to decide whether it's opt out or opt in, and that is the GDPR. It's a situation that is a bit particular and different from the other countries in Europe.

What are your authority's priorities in 2020?
We have already decided what we will do next year, we will work together with one of the universities in Liechtenstein and offer workshops. These workshops will address companies and where companies can learn how to implement certain regulations. One is on video surveillance, then the next one will be on DPIAs, then there will be another one, but probably in 2021, on GDPR in the employment context because there are many questions. So, this is one thing we want to do.

Another one is that we want to concentrate on children. We want to launch a project called 'data protection goes to school,' so we will work together with school's in Liechtenstein and try to teach children what their rights are, how important these rights are, and that they should not ignore these rights, because digitalisation is a very important topic in Liechtenstein, even now for school children. I think you can't just launch a project discussing digitalisation in schools without making sure that the school children are aware of their rights within this digitalization.

Watch this interview on demand, as well as interviews with the European Data Protection Supervisor, the UN Special Rapporteur on The Right to Privacy, and more, through the OneTrust DataGuidance video hub.

California: CCPA regulations approved and effective



The California Attorney General ('AG'), Xavier Becerra, announced, on 14 August 2020, that the California Office of Administrative Law ('OAL') approved the regulations1 ('the Regulations') under the California Consumer Privacy Act of 2018 ('CCPA') and filed them with the Secretary of State, entering into immediate effect. In addition, the AG highlighted that those who had submitted comments regarding the Regulations had the right to request a copy of the final statement of reasons.

Most notable changes

In particular, the Regulations include certain changes in comparison to the version submitted by the AG on 1 June 2020, such as the deletion of the phrase 'Do Not Sell My Info' to align with the express language of the CCPA, the change of the terms 'minors' and 'minor' to 'consumers' and 'consumer,' as well as the removal of the requirement for businesses that substantially interact with consumers offline to also provide notice by an offline method that facilitates consumer awareness of their right to opt-out.

Caitlin Potratz Metcalf, Senior Associate at Linklaters LLP told OneTrust DataGuidance that, "While the final CCPA implementing regulations largely reflect the earlier draft regulations from June, the most noteworthy changes are in what was deleted from the text. Several of the key deletions dealt with how businesses subject to the CCPA would have had to notify California consumers and/or obtain their consent. For example, the provision (Section 999.305(a)(5)) requiring that consumers expressly opt in before a business can use their collected personal information for a different purpose—specifically one not included in the original notice at the time of collection—was cut from the final regulations. So too were the requirements that businesses ensure that it be 'easy' for consumers to opt out in only a few steps."

Ensuring compliance

The AG stated that the Regulations establish procedures for compliance and exercise of rights, as well as clarifies important transparency and accountability mechanisms for businesses subject to the law. In addition, the AG noted that it is particularly critical for businesses to be mindful of personal data security given the current COVID-19 pandemic. Further to this, Potratz outlined, " To ensure compliance going forward, businesses should review and update their privacy programs based on the final regulations and keep an eye on how the California AG's Office approaches enforcement in its first season. From what we have seen enforcement-wise to date, for most businesses, a 'nuts and bolts' approach will be best—in particular, ensuring that consumers receive timely notice when their personal information is collected, businesses maintain clear and accurate disclosures in their privacy policies, and consumers can readily opt out of the sale of their personal information via a conspicuous 'Do Not Sell My Personal Information' link online. As a baseline, it is critical that businesses prioritise transparency in their touch points with consumers."

Scope for expansion

Although the Regulations are now finalised, the AG, under Section 1798.185(a)) of the CCPA is given broad powers to update and adjust the policies outlined therein. Therefore, the scope of privacy protections guaranteed under the current legislative framework in California may be expanded. Potratz continued, "Considering these changes in context, it nevertheless seems unlikely that they will significantly erode the consumer privacy protections afforded by the CCPA and its implementing regulations in the long-term given the CCPA's framework requirements, not to mention the potential for more expansive privacy rights on the horizon if the California Privacy Rights Act (CPRA) is passed. It is also within the California AG's authority to revise the provisions deleted from the final regulations as he sees fit and resubmit them for approval at a later date."

Edidiong Udoh Privacy Analyst
eudoh@onetrust.com

Comments provided by:
Caitlin Potratz Metcalf Senior Associate
caitlin.metcalf@linklaters.com
Linklaters LLP, London and Washington D.C.

1. See: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf/index.do

EU: Practical steps post-Schrems II - Reconciling theory with reality

For many multinational companies attempting to navigate the challenges created by the COVID-19 ('Coronavirus') pandemic, the recent judgment on data transfers from the Court of Justice of the European Union ('CJEU') in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18) ('the Schrems II Case') has added fuel to the fire and made business-as-usual seem like an even more distant notion. Claire François, Counsel at Hunton Andrews Kurth LLP, breaks down the theoretical aspects of the CJEU's decision before moving on to outline some practical strategies that companies can adopt both in the short and long-term to meet the demands presented by the same.

Just as the Coronavirus pandemic creates the greatest economic uncertainty in decades, the CJEU's decision on 16 July 2020 in the Schrems II Case has added even further uncertainty in regards to transfers of personal data from the EU to the US and other countries[1]. The CJEU did not just invalidate the second most used data transfer mechanism but also significantly raised the standards of protection for personal data transferred pursuant to the most common mechanism, that of Standard Contractual Clauses ('SCC')[2]. Companies are now faced with the considerable challenge of reconciling the theoretical aspects of the CJEU's judgment with business reality at a time when they lack resources due to the current health crisis.

The theory: Schrems II high data protection standard

The CJEU's decision

Much has been written on the CJEU's decision in relation with the EU-US Privacy Shield Framework ('the Privacy Shield') and the Commission's SCC. Suffice it to say that the CJEU did not simply invalidate the Privacy Shield and confirm the validity of the SCC. The CJEU went far beyond its previous 2015 decision on the Safe Harbor mechanism in Maximillian Schrems v. Data Protection Commissioner (C-362/14), and required that the data exporter and the recipient of the data (i.e. the data importer) assess on a case-by-case basis, prior to any actual data transfer, the law of the destination country in order to determine whether that law allows the data importer to comply in practice with the relevant EU contractual data transfer mechanism (here, SCC), taking into account all the circumstances of the data transfer, as well as possible additional measures that the parties could put in place. If, following this assessment, the data exporter (i.e. the controller who transfers the data) comes to the conclusion that appropriate safeguards would not be ensured, the data exporter must suspend or cease the transfer of personal data to the data importer, and the data that has

already been transferred to the third country and the copies thereof must be returned or destroyed in their entirety. If, however, the data exporter intends to continue transferring the data despite this conclusion, the data exporter must notify the competent EU data protection authority ('DPA'), who must then suspend or prohibit the data transfer.

By increasing the standards of protection for the personal data transferred pursuant to SCC, the CJEU's decision makes it difficult to use SCC in practice and creates legal uncertainty for businesses: their assessment may be called into question at any time, and there is no guarantee that personal data can be validly transferred pursuant to SCC, despite all the additional measures that the parties could put in place.

The CJEU did not just invalidate the second most used data transfer mechanism but also significantly raised the standards of protection for personal data transferred pursuant to [...] Standard Contractual Clauses

Apparent consistency with the GDPR accountability obligations

The SCC were issued by the Commission under the previous EU data protection framework (Directive 95/46/EC). So far, in practice, most businesses have considered the conclusion of SCC as a mere formality or checkbox exercise: the SCC were filled in as applicable, executed, and then filed for record purposes. It was sufficient to do so to adduce adequate safeguards for the transfer of personal data to third countries. Some companies even incorporated the SCC into their data processing agreement by mere reference to them, and did not even bother annexing the SCC.

The CJEU's decision reminds everyone that implementing SCC can no longer be a mere formality. Data exporters and data importers have obligations under the SCC and must verify that these obligations can be complied with in practice. At a theoretical level, the CJEU's decision appears a logical development in light of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the increased compliance obligations it creates. The verification or assessment required by the CJEU is part of the data controller's accountability obligations under the GDPR and, as such, must be documented by the data controller/exporter.

In practice, however, the CJEU requires the parties to carry out an adequacy assessment similar to the assessment performed by the Commission for the purposes of adopting an adequacy decision under Article 45 of the GDPR: the data exporter and data importer using SCC must assess the law of the data importer (or destination country) 'as regards any access by the public authorities of that third country to the personal data transferred'3 in order to check if that country ensures an adequate level of protection, taking into account the factors to be considered by the Commission when carrying out its own adequacy assessment. Other than the fact the Commission has so far recognised only 12 countries4 as providing adequate protection (outside of the US via Safe Harbor and the Privacy Shield), the Commission's assessment proved to be wrong twice in regards to the US for both the aforementioned mechanisms, making it unclear how businesses could do a better job. That said, as EU DPAs (within the European Data Protection Board ('EDPB')) refused to grant a grace period to adjust to the CJEU decision, businesses necessarily need to take remediation actions both in the immediate, short, and medium to long term, if they wish to continue transferring personal data outside of the EU.

The reality: no perfect solution and a step-by-step strategy

SCC as an 'immediate fix'

For those businesses that have EU establishments and were relying on the Privacy Shield to transfer personal data to the US before the CJEU Decision, SCC will be the only immediately available data transfer mechanism to continue transferring the data.

The derogations under Article 49 of the GDPR referred to by the CJEU will not be a solution for most data transfers. The CJEU argued that the invalidation of the Privacy Shield does not create a legal vacuum because businesses can rely on these derogations. However, the most relevant derogations available to businesses typically include (i) the individual's explicit consent; and (ii) the 'contract' derogation. Given the high threshold for valid consent, and that consent may be withdrawn at any time, this will not be a feasible solution in practice. The same conclusion applies to the 'contract' derogation: such derogation may be used only for occasional data transfers, and when the transfer is objectively necessary for the performance of a contract with the individual, (i.e. in very limited cases).

Binding Corporate Rules ('BCRs') - the only other contractual mechanism currently used to transfer data - cannot be an immediate or feasible solution either. The preparation and implementation of BCRs can take years, and this solution is most appropriate for large corporate groups. Further, the EDPB confirmed that the CJEU's decision also applies in the context of BCRs, meaning that companies relying on BCRs must also assess the law of the destination country to determine whether the guarantees provided by the BCRs can be complied with in practice. From this perspective, BCRs are not a better solution than SCCs.

Assessing the adequacy of the transfers to the US (and other countries)

Implementing a valid (contractual) data transfer mechanism is no longer sufficient. Businesses must also ensure that the law of the destination country does not prevent the data importer from complying with that mechanism.

For data transfers to the US, the data exporter and the data importer should first determine the key types of US government surveillance and intelligence gathering mechanisms to which the data importer is subject. The CJEU focussed on Section 702 of the US Foreign Intelligence Surveillance Act of 1978 ('FISA') that applies to data collection from 'electronic communication service providers.' However, there are other laws and most of these laws are drafted broadly to apply to most businesses in the US. It is therefore not so much a question of whether the data importer is subject to US surveillance laws but whether the data importer has received in the past any requests or demands from US government authorities (such as law enforcement or intelligence agencies) that may concern personal data and how likely they may receive such requests or demands in the future.

One way to continue transferring personal data to the US pursuant to SCC is to demonstrate that the data importer, although subject to US surveillance laws in theory, has not received any requests or demands from government authorities for personal data, and has implemented appropriate additional safeguards.

In practice, EU data exporters should send due diligence questionnaires to US importers to help them carry out the above risk assessment, and US businesses should be ready to answer those questions. Due diligence questionnaires should also be sent to non-US importers that may receive personal data pursuant to SCC, and the parties should carry out a similar assessment.

Implementing additional safeguards

The CJEU made it clear that additional safeguards will have to be implemented in most cases, without specifying what these additional safeguards could be in practice. The EDPB is currently analysing the CJEU's decision to determine the types of additional measures that could be implemented in addition to SCC, whether legal, technical, or organisational, and will issue guidance in the future. Ultimately, these additional safeguards will depend on the results of the companies' risk assessment.

Some companies are already adding additional clauses to the SCC to adduce additional legal safeguards and avoid reopening data transfer agreements in the future. That additional language may however have to be revised once the EDPB will issue its guidance. Further, the Commission is still working on updating SCC in light of the GDPR; the new SCC will have to be executed, and agreements will have to be reopened anyway.

Towards data localisation?

Some commentators have suggested that one way to comply with the CJEU's decision is to use EU service providers, and as a matter of fact, on 17 July 2020, the Berlin data protection authority ('Berlin Commissioner') called for data currently stored in the US to be relocated to the EU.

Firstly, in this regard, calling for data localisation totally ignores business reality. Secondly, data localisation could be a solution from an EU data protection perspective only if personal data was to be stored in the EU and if there was no access to the data from third countries (i.e. absolutely no data transfer outside of the EU). From a practical perspective, while companies may wish to have their data stored in the EU, they also may want to receive prompt technical support (outside of EU standard business hours), which may justify access to the data by non-EU technical support locations. Thirdly, data localisation may have a cost for businesses that could be passed on consumers. Some service providers already allow their customers to select EU data centres, but at a higher cost. Finally, data localisation practices will trigger further data localisation initiatives abroad and is contrary to the Commission's objective to further facilitate international data flows and promote EU companies' competitiveness. That is why Vice-President Věra Jourová confirmed at the press conference following the CJEU's decision the importance to carry on working to ensure the continuity of safe data flows.

Conclusion

The CJEU's decision creates a lot of uncertainties and these uncertainties will remain for a while. Businesses should not wait for future DPA guidance or the updated SCC from the Commission to take remediation actions but should act promptly by developing and implementing a step-by-step strategy, while also bearing in mind that no safeguard now offers total legal certainty.

Claire François Counsel

cfrancois@HuntonAK.com

Hunton Andrews Kurth LLP, Brussels

1. The European Commission ('the Commission') has so far recognised only 12 countries as providing an adequate level of data protection. This includes Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. EU personal data can continue to be (freely) transferred to these countries, but companies should closely monitor any future developments in this respect, including the Commission's review of past adequacy decisions or eventual legal challenges in the CJEU.
2. According to IAPP research, approximately 88% of companies transferring personal data outside of the EU rely on SCC, while 60% use the Privacy Shield.
3. The Schrems II Case, para. 104.
4. 4. Supra footnote 1.

WEBINAR

Key takeaways: Privacy, data protection, and contact-tracing apps

Contact tracing is fast becoming a necessary tool to combat the spread of COVID-19 ('Coronavirus'). This webinar covers key data protection and privacy elements in contact tracing apps in the Coronavirus era. Our expert speakers discuss the latest developments regarding contact tracing apps, the US federal legislation that was introduced in response to the pandemic and compare approaches in the EU and the US.

Case investigation and contact tracing

The case investigation is part of the process of supporting patients with suspected or confirmed infection in which the goal is to help the patient recall everyone with whom they have had close contact during the timeframe while they may have been infectious. Contact tracing involves warning the potentially exposed individuals (contacts) of their potential exposure as rapidly and as sensitively as possible. In this case, contacts are only told they 'may' have been exposed. Whilst maintaining the anonymity of a patient who may have exposed them is crucial, equally important is educating the potentially infected individuals on risk, mitigation, and symptoms. This also helps to encourage individuals to self-isolate with the ultimate goal of stopping the chain of disease transmission.

Manual v. automated tracing

Contact tracing is still conducted manually in 2020. Public and private employers are automating the tracing process via data-driven technology. Examples include contact tracing apps installed on mobile phones with the ultimate goal to identify persons who may have been exposed to COVID-19 ('Coronavirus'). The contact tracing apps function to identify those who have been near someone identified as having an actual or suspected case of Coronavirus. There are warnings issued to exposed persons and each app can be designed for specific settings, e.g. employment monitoring. There have been many talks about making said apps as decentralised as possible and less intrusive. Some ways this can be accomplished is through Bluetooth or GPS technology. Bluetooth is more privacy-friendly and less intrusive to an individual's privacy and data can be kept on an phone. In addition, proximity data is less invasive than geolocation data

EU v. US approaches to privacy and data regulation

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') provides comprehensive data protection to covered data subjects, extraterritorial reach, and significant penalties for violation. The Directive on Privacy and Electronic Communications (Directive 2002/58/EC) ('the ePrivacy Directive'), which remains in effect while an update is being negotiated, strictly regulates the processing of personal data online. The European Data Protection Board issued, on 22 June 2020, a statement that said the "GDPR remains applicable and allows for efficient response to the pandemic, while at the same time protecting the fundamental rights and freedom." EU institutions have recognised the importance of contact tracing apps in ending the lockdown and the institutions have taken the lead in providing guidance to app developers and Member States that are using and developing contact-tracing apps. The eHealth Network, a voluntary network setup under Directive 2011/24 EU on the Application of Patients' Rights in Cross-border Healthcare, has developed and maintained an EU toolbox for the use of mobile applications that sets forth essential requirements and best practices. The Parliament cautioned, among other things, that the use of such apps should be voluntary, not mandatory.

Unlike Europe, the US takes a sector approach to data privacy. At the moment in the US, there is no federal contact tracing app. US-based organisations and health officials who want to use contact tracing apps must look to a patchwork of laws potentially regulating their use (e.g. the Health Insurance Portability and Accountability Act of 1996, the California Consumer Privacy Act of 2018, and the California Consumer Privacy Rights Act, etc.). The sector-specific and state laws apply based on the nature of the data being collected, the type of person from whom the data is being collected, the purpose of the processing, who will have access to the data during the data lifecycle, geographic location of both the organisation, and individuals that the organisation seeks to use contact-tracing apps to protect.

US federal privacy law

Unlike the EU, the US has failed to pass comprehensive federal privacy legislation. Since early May, three COVID-19 related federal privacy laws have been introduced in Congress. Senate Bill ('SB') 3663 for the COVID-19 Consumer Data Protection Act of 2020 ('CCDPA') was introduced by Republican U.S. Senators Roger Wicker, Jim Thune, Jerry Moran, and Marsha Blackburn on 7 May 2020, SB 3749 for the Public Health Emergency Privacy Act of 2020 ('PHEPA') was introduced by Democratic U.S. Senators Richard Blumenthal and Mark Warner, and U.S. Representatives Anna Eshoo, Jan Schakowvsky and Suzan DelBene on 14 May 2020, and the bipartisan SB 3861 for the Exposure Notification Privacy Act ('ENPA') followed on 1 June 2020.

The CCDPA covers entities including non-profits and covers data such as precise geolocation data, persistent identifiers, and personal health information. The PHEPA covers any entity that collects emergency health data, excluding health care providers, service providers, and public health authorities, and doesn't apply to entities covered by HIPAA. The ENPA includes non-profits and is an operator of an automated exposure notification service, other than a public health authority. The requirements of each bill can vary. The CCDPA establishes affirmative express consent by and individual (the natural person residing in the US), the PHEPA has affirmative express consent by an individual and the ENPA outlines express consent by an individual in which the operator must collaborate with a public health authority in the operation of a service and it must only process an "authorised diagnosis." Authorised diagnosis means an actual, potential, or presumptive positive diagnosis confirmed by a public health authority or licensed health care provider. The purposes of each bill can also be different. The CCDPA tracks the spread, signs, or symptoms of Coronavirus, measures compliance with social distancing guidelines or other requirements imposed under federal, state, or local government order, and conducts contact tracing. The PHEPA covers entities that collect emergency health data which shall only do so if necessary, proportionate, and limited for a good-faith public health purpose and mandates that the data cannot be collected, used or disclosed for e-commerce or to discriminate by creating or taking away opportunities (i.e. jobs, health benefits, etc.). The ENPA implements automated exposure notification services for public health purposes and cannot collect or process data for any commercial purposes.

INTERVIEW WITH:

Evan Davies Group Data Protection Officer at YouGov

THOUGHT LEADERS IN PRIVACY

We met with Evan Davies, Group Data Protection Officer at YouGov, in March 2020. YouGov is an international research data and analytics group headquartered in London. With a proprietary panel of over 8 million people globally and operations in the UK, North America, Mainland Europe, the Nordics, the Middle East and Asia Pacific, YouGov has one of the world's largest research networks.

Evan discusses how market research has changed over the years, in light of the vast amount of data that is now possible to collect and YouGov's approach to the GDPR's requirements regarding its information provision obligations to the data subject.

How has market research changed over the years, in light of the vast amount of data that is now possible to collect, and what role does law and regulation play?

Market research has changed quite considerably over the last 10 to 20 years, and even in the last five years. Even predating me, it was all telephone and face-to-face based because no one was really online, but now of course, everyone has at least one device and the vast majority of people have access to the internet. So, everything's moved online, which of course, means that we're able to access more people, more regularly which means there is more data being collected but also researchers have a challenge in offering a compelling and engaging research proposition to a representative group or audience because people have other things to do in their lives.

> **We made a decision to create a global privacy framework based on the principles of the GDPR, but it was also flexible enough to adapt to any other privacy laws and markets we were operating in**

The challenge is on us to make sure that what we're offering is interesting, and some of the recent examples of those types of projects are using technology that can read the contours of someone's face when they're watching something so that you can understand a bit more about what their emotions are or they can pick up where people's eyes are looking on a screen to understand what people are looking at.

Also, there's some passive data collection as well, so information about someone's location or how they're browsing the internet. Obviously, now we're talking about not only an increase in the volume of data, but different types of data, which is where privacy laws and regulations come in and they set the rules of how we need to comply with the laws. There's a strong compliance aspect that we all need to comply with.

That applies to market research, as well as other industries, but I think that market research also has an opportunity given the relatively unique nature of how we engage with our research participants, to engage with them and tell them a bit more of a conversational story about how we approach privacy, how we protect their data, and what rights they have, and I think that, as people become more familiar with what privacy means to them and what rights they have, that's telling people how that ethical uses of data is actually going to be a really important thing for all companies to do in the future.

How has YouGov approached its global compliance program?

YouGov is a truly global company, we're in over 40 markets now. So, while that's really positive from a business side of the story, it throws up quite a lot of challenges for the compliance side. Back when we started our privacy journey, we made a decision to create a global privacy framework based on the principles of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), but it was also flexible enough to adapt to any other privacy laws and markets we were operating in, and that was a really effective thing for us to do because it means that we're compliant in the countries we operate in now.

It also really helps us as we expand because we're able to take that framework and apply it in countries that we're moving into, and some of those countries may not even have privacy laws, so in those countries we're going over and above what we need to do. We feel that it's a really important thing to have a consistent offering across our group.

The GDPR includes detailed requirements regarding its information provision obligations to the data subject. What has been your organisation's approach to meeting these requirements?

We look at the GDPR as the foundation of our global

compliance framework, we look to Article 13 and 14 primarily for telling us what we need to tell people. I think that's quite useful on one hand, because it's quite a specific list of things we need to tell people. On the other hand, it really raises a challenge, which is not new in the privacy world, of how do you get all this information across in a way that's clear and concise and understandable to the end user.

So, this is something that we're continuing to work on because I think it's something that is going to be a challenge over an a number of years to come, but what we do is we really utilise the fact that we have been a market research company and we have a unique position where we've got an ability to communicate with our research participants quite often, and in different ways. Rather than just having all our information on a privacy notice which, of course, we do, we have other ways of talking to people about what we're doing with the data, when we have collected it, and to tell them about what rights they have.

What do organisations need to be aware of regarding the management of third parties with respect to data sharing and transfers?

I think all organisations need to do some form of due diligence exercise, and that will depend on the size of your organisation and the resources you've got at hand. There are a couple of key questions that I always ask at the start of those processes to help navigate how it's all going to run. The first one is fairly obvious and it's 'what data is involved in and how it's being used.' And that will allow you to do a mini risk assessment to understand what sort of resources you need to bring into the process, so do you need to bring in someone from information security, do you need to bring in someone from legal or corporate governance.

Then, the second question is, what role will each of the organisations involved have. So, are we talking about two data controllers or a data controller and a data processor. And the answer to that is not always clear cut and sometimes the organisations involved have a different interpretation, so it's really important to get that sorted out right at the start, because once you've got the answer to that you are naturally going to be able to know what contracts you need to put in place, including any safeguarding of data transfers and also, you need to be able to understand what practical implications there will be for each of the organisations under the agreement.

Stay tuned for the new 'The Art of Privacy' video series coming soon to OneTrust DataGuidance

Oman: Latest developments in data protection and cybersecurity

Oman does not currently have a standalone data protection law. Whilst Oman's Constitution (Royal Decree No. 101 of 96) recognises an individual's right to confidentiality in all forms of communication, it does not recognise the right to privacy as a fundamental right beyond this. Alice Gravenor, Senior Associate at PwC Legal Middle East, analyses the patchwork of laws and regulations that constitute Oman's legal protection framework in the absence of a constitutional right to privacy or general data protection legislation and discusses all the latest regulatory developments aimed at strengthening Oman's privacy regime.

Establishment of the Cyber Defence Centre

In June 2020, the Sultan of Oman, His Majesty Sultan Haitham Bin Tarik, issued Royal Decree No. 64 of 2020 ('the Decree') establishing the Cyber Defence Centre. Although very short, the Decree represents one of the latest developments concerning the data protection and cybersecurity landscape in Oman.

Article 1 of the Decree states that a body by the name of 'The Cyber Defence Centre' will be set up and that such centre will report into the Oman Internal Security Service ('ISS'). The Decree is brief and does not go much further than stating that bylaws and decisions necessary for the implementation of such a system will be issued by the Head of the ISS, and that anything contrary to the Decree and the system it implements is hereby repealed.

Development of a draft data protection law

The Oman Information Technology Authority ('ITA') announced in 2017 that it was developing a data protection law ('the Draft Law'). However, the Draft Law remains a draft without a clear indication of when it will come into force. It was speculated that if approved and signed into law, the Draft Law will grant powerful rights to individuals in Oman, enabling them to exercise levels of control over their personal data equivalent to the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), for example by giving individuals the right to:

- object to the processing of their personal data;
- demand access to any personal data about them held by any organisation in Oman;
- demand that any mistakes in this data are corrected; and
- demand that this data is completely erased if they wish.

The ITA went as far as to hold public consultation sessions to discuss the Draft Law and seek feedback from members of the public on its contents, but limited further developments have since occurred.

In July 2020, the State Council held its eighth ordinary session of the first annual sitting for the seventh term where it discussed the 'Personal Data Protection Draft Law', noting the importance of the Draft Law in light of the ongoing technological developments and digital challenges.

Hon. Dr. Rashid bin Salim bin Rashid al Badi, Committee Head of the Legal Committee of the Council, stated that the Draft Law contains 35 Articles divided into five Chapters as follows:

1. Definitions and general provisions;
2. Tasks and powers of the Ministry of Technology and Communications;
3. Rights of individuals with regards to their personal data;
4. Obligations of the controller and processor handling the processing of personal data; and
5. Penalties for violating the provisions of the law.

Despite providing previously unknown detail on the Draft Law, no reports on the timelines for promulgation of the Draft Law have been reported.

A limited number of other laws in Oman relate to the use of personal information and cybersecurity, however these are certainly not the equivalent of bespoke data protection laws such as the GDPR.

The Cyber Crime Law

The Cyber Crime Law (Royal Decree No. 12 of 2011) seeks to address a wide array of illegal activities involving a computer device, computer system, or network. It considers various acts as cybercrimes and sanctions violations of such acts with robust penalties in the form of imprisonment and fines.

The Cyber Crime Law also contains limited provisions with respect to personal data protection, including making it an offence to violate the privacy of individuals using technology. It does not however impose any obligations on those who collect personal data.

The Electronic Transactions Law

The Electronic Transactions Law (Royal Decree No. 69 of 2008), which is based largely on the UN Model Laws relating to e-commerce and electronic signatures, contains limited provisions relating to the processing of personal data. It does, however, include some requirements relating to the obtaining, retention, and dissemination of personal data. However, the Electronic Transactions Law only applies to transactions performed between parties who have agreed to perform their transactions electronically and therefore its narrow data protection provisions do not apply to those who collect personal information outside the scope of the Electronic Transactions Law .

Sectoral laws

Limited data protection and cybersecurity provisions can also be found in a number of sectoral laws across the telecommunications, financial, and healthcare industries.

- Under Resolution No. 113 of 2009 issuing Regulations on Protection of the Confidentiality and Privacy of Beneficiary Data issued pursuant to Royal Decree No. 30 of 2002, following the written approval of a customer, a telecom service provider ('TSP') is permitted to share customer personal data with any of its subsidiaries or with other companies. Under such circumstances, the TSP is obliged to guarantee not to use customer data for any purpose other than the specified purposes and within the permissible limits. It is not clear whether this would include sharing the data with third parties outside of Oman and therefore consequently permit a cross-border transfer of such data.
- The Banking Law (Royal Decree No. 114 of 2000) contains certain limited provisions covering the protection of customer information in the banking context. All licensed banks, including their directors, officers, managers and employees are prohibited from disclosing customer information without the customer's consent, unless required to do so under Oman law or instructed to do so by the Central Bank of Oman.
- The Healthcare Law (Royal Decree No. 75 of 2019) contains provisions surrounding the disclosure of patient information. It is stated that patient information must not be shared with any person until the patient has provided their written consent to do so. Limited exceptions exist to this rule such as where disclosure is required to share relevant patient information with health insurance companies.

Given the latest developments concerning data protection and cybersecurity in Oman, with the issuance of Royal Decree No. 64 of 2020 establishing the Cyber Defence Centre, and the latest discussions concerning the Draft Law, it seems Oman has data protection and cybersecurity firmly on the agenda, and that further development in this area is likely in the coming months.

Alice Gravenor Senior Associate

alice.gravenor@pwc.com

PricewaterhouseCoopers Legal Middle East LLP

WEBINAR

Key takeaways: Japanese privacy laws and the impact of the new amendments

Since 2005, the Act on the Protection of Personal Information ('APPI') in Japan has been amended twice. The first amendment was enacted in 2015 with the changes coming into force in 2017, and the latest Amendments were introduced in June 2020. It is expected that the current Amendments will come into force no later than June 2022. This webinar looks at the practical impact of the new Amendments. Atsushi Okada, Partner at Mori Hamada & Matsumoto, provides a detailed analysis of the APPI, and looks at specific changes to data subject rights, cross-border transfers, and data breach reporting.

Data subject rights

Data subject rights have been expanded under amendments to the APPI. In comparison to the current law, data subjects can now exercise their rights in response to a severe data breach, if their personal data no longer needs to be processed, or if their 'rights or legitimate interest' are likely to be affected. However, as our speakers point out, companies should be aware that certain exceptions apply. For example, a request can be refused if it would result in huge expense, or if an organisation can provide alternative means to protect the interests of the data subject.

Data retention period

Organisations should note that short-term data will now be subject to access requests from data subjects. Under the existing law, any data which was to be erased after six months was not 'Retained Personal Data' and therefore not subject to data subject requests. The amendments abolish this rule, and data subjects can exercise their rights regardless of the retention period.

Mandatory breach reporting

Whereas under the current law organisations should 'duly make an effort' to report a breach to the Personal Information Commission ('PPC'), and it is recommended that the affected data subjects be notified, this was not mandatory. The amendments will mean organisations will be required to report a data breach to the PCC, and to data subjects if the rights and interests of subjects are infringed.

Penalties

The 2020 amendments will bring about some significant changes to penalties. In comparison to the GDPR, there are no administrative fines, however criminal penalties have been increased. For example, the charge for submitting a false report is now 500,000 yen (approx. €4,000). Additionally, the penalty for violating an order from the PCC can bring fines of 100 million yen (approx. €800,000).

Cross-border transfers

There are stricter requirements on cross-border transfers. In short, a data subject needs to be more informed on where their information is going, how it is being handled, and most importantly, how it is being protected. Organisations should be aware of relevant safeguards and security measures, they must obtain consent from data subjects, and integrate any changes into a privacy policy.

How OneTrust DataGuidance helps

OneTrust DataGuidance™ is the industry's most in-depth and up-to-date source of privacy and security research, powered by a contributor network of over 500 lawyers, 40 in-house legal researchers, and 14 full time in-house translators. OneTrust DataGuidance™ offers solutions for your research, planning, benchmarking, and training.

OneTrust DataGuidance offers a GDPR Benchmarking tool, which includes California, Brazil, Thailand, Russia, Japan, and which is currently being expanded to include Australia as well as China. The tool assists organisations to understand and examine core requirements under each law in order to determine their consistency for gap analysis and assessment, and contribute to the development of global compliance programs.

OneTrust DataGuidance solutions are integrated directly into OneTrust products, enabling organisations to leverage OneTrust to drive compliance with hundreds of global privacy and security laws and frameworks. This approach provides the only solution that gives privacy departments the tools they need to efficiently monitor and manage the complex and changing world of privacy management.

Watch this webinar on demand and catch up on all OneTrust DataGuidance webinars through the new resources portal on www.dataguidance.com

ONETRUST
LGPD FAST TRACK

Get Your Implementation Up and Running in 24 Hours

- Same day DSAR implementation
- Simple setup with pre-completed workflows
- Certification and training
- LGPD setup guide and implementation webinar

OneTrust

PRIVACY, SECURITY & GOVERNANCE

Implement Today

Brazil: LGPD entry into force and approval of ANPD structure

The President of Brazil, Jair Bolsonaro, promulgated, on 17 September 2020, Law No. 14.058/2020 which validated Provisional Measure 959/2020, resulting in the entry into force of the LGPD on 18 September 2020. Bolsonaro had 15 business days to validate Conversion Bill 34/2020, which was passed by the Senate of Brazil on 25 August 2020 and had rejected provisions passed by the Chamber of Deputies, which sought to postpone the entry into force of the LGPD to 31 December 2020.

On 26 August 2020, Bolsonaro also signed Decree No. 10.474 of 26 August 2020 ('the Decree') which approved the regulatory structure and the framework of the positions of the Brazilian data protection authority ('ANPD').

Alan Thomaz, Partner at AT Advogados, told OneTrust DataGuidance, "In 2018, the LGPD was approved and set to come into force in February 2020 and after a few legislative developments, moved to August 2020. In addition, the ANPD Authority was created, and the administrative sanctions of the LGPD were postponed to August 2021. In 2020, Provisional Measure 959/2020 was intended to postpone again of entry into force date of the LGPD to May 2021. In Brazil, such measures enter into force and take effect immediately but must be voted within 120 days or become void. Provisional Measure 959/2020 regulated two different subject matters (i.e., the payment of social benefits in the context of COVID-19, and LGPD's entry into force date) which was found to be a flaw within the legislative process, as each subject matter has to be voted in an independent provisional measure.

Nevertheless, on August 25, 2020, the House of Representatives voted such provisional measure, changing the postponement date from May 2021 to 31 December 2020, and right after on 26 August 2020, the Senate approved the part of the provisional measure that regulates the benefits related to COVID-19, but acknowledged the flaw, invalidating the part of provisional measure regulating the LGPD."

Expected actions by ANPD

Under the Decree, the ANPD is tasked with, among others, ensuring the protection of personal data, developing relevant guidelines, investigating and enforcing against violations of data protection, as well as promoting cooperation actions with data protection authorities from other countries.

Furthermore, the Decree provides details on the appointment of members of the ANPD, as well as

administrative and internal procedures for the functioning of the ANPD. The Decree will come into force on the date of publication of the appointment of the ANPD's executive director in the Federal Official Gazette.

In 2018, the LGPD was approved and set to come into force in February 2020 and after a few legislative developments, moved to August 2020. In addition, the ANPD Authority was created, and the administrative sanctions of the LGPD were postponed to August 2021

Thomaz continued, "The Decree is intended to change the administrative structure of the executive branch, by creating and moving specific positions of government employees, and defining the roles of each position in ANPD's internal structure. Now, Bolsonaro must indicate the individuals who will assume such positions created in the ANDP. I believe that the first actions to be taken by the ANPD would be issuing further regulation in pending topics of the LGPD (e.g. international transfer of data and data protection impact assessments). Also, the ANPD should dedicate its efforts to guide organisations that intent to obtain a minimum level of adequacy to the LGPD."

LGPD enforcement

The delay of entry into force of the sanctions' provisions of the LGPD to August 2021 does not necessarily mean that there would be a grace period for organisations. Thomas concluded, "Individual or class actions are still possible, and any preliminary court order or injunctive relief may impose penalties and require organisations to take specific actions to comply with the LGPD (e.g. stopping a marketing campaign or the offering of a product or service). Therefore, companies that have not dedicated specific efforts to obtain minimum adequacy to the LGPD may be exposed.

Achieving compliance with the LGPD is a complex process, but, as a rule of thumb, organisations should focus at least on reviewing highly intrusive practices, observing data subjects' rights (such as transparency and access), and implementing organisational and technical measures to avoid data incidents."

Nikolaos Papageorgiou Lead Privacy Analyst
npapageorgiou@onetrust.com

Comments provided by:
Alan Thomaz Partner
at@alanthomaz.com
AT | Advogados, So Paulo

France: Managing requests from authorised third parties

The French data protection authority ('CNIL') published, on 10 July 2020, a practical guide ('the Guide') and a collection of common procedures ('the Procedures') to help organisations in dealing with requests from authorised third parties involving transmission of documents and/or information which may include personal data. In particular, CNIL highlighted that companies receiving such requests from an authorised third party may encounter difficulties when attempting to reconcile the obligation to respond to authorised third-party requests and their duty to comply with personal data protection and confidentiality requirements. The Guide comprises of sections on identifying an authorised third-party request, on verifying the source of the request and the scope of the request, and on ensuring secure transmission when data controllers transmit documents or information by the data controller to the authorised third party. The Procedures supplement the Guide by providing more detail on the specific procedures which are frequently encountered with respect to authorised third-party requests involving, jurisdictional queries, administrative queries, economic surveys, and social, work and health surveys. This Insight focusses on the Guide, analysing the main requirements and recommendations outlined by CNIL.

Identifying authorised third-party requests

In terms of authorised third parties, the Guide specifies that authorities may have the power, by virtue of legislation or other applicable regulations, to request specific documentation from data controllers. In addition, Article 4(9) of the GDPR specifies that the concept of 'recipient' encompasses actors which are likely to receive such documentation in relation to fact-finding missions in accordance with EU or Member State law. In relation to this, the Guide specifies that 'authorised third parties' should be distinguished from other recipients of information acting outside the scope of fact-finding missions, for instance in the context of requesting access to administrative documents or the exercise of a data subject's right to access information.

After outlining the actors which would fall under 'authorised third-parties', the Guide explains steps for identifying requests originating from authorised third parties. In this regard, the Guide specifies that if a data controller receives a request for the transmission of personal data, the following steps are recommended:

- Ensure that the request is based upon a legislative provision which is currently in force: if the request mentions a specific provision, verify this provision, or, in cases where the request does not mention a specific provision, ask the organisation making the request to confirm that they are acting in accordance with a legal provision and to specified said legal provision.
- Verify that this organisation making the request is acting, at the time of their request, as an authorised third party. Therefore, data controllers must not merely rely on contextual information, such as the phrasing of the request or the nature of the body making the request.

Verifying authorised third-party requests

The Guide outlines three main rules data controllers need to follow when receiving requests for the transmission of personal information to the organisation:

1. Verify the source of the request, i.e. the organisation making the request.
2. Verify the scope of the request, i.e. what information is requested and whether excess data is requested.
3. Respect professional secrecy and the right of communication.

These are explained further below.

Source of the request

The verification of the request is a two-fold procedure consisting of:

- legal verification (i.e. ensuring that the organisation making the request is actually mentioned in the legal provision); and
- practical verification (i.e. ensuring that the request

received by the data controller actually originates from the authority or public body mentioned).

Methods of verification specified in the Guide include checking that the postal address provided matches with the official address published by the authorised third party in its website, contacting the data protection officer ('DPO') of the organisation making the request, and checking that the domain name of the email address corresponds to that published on the website of the organisation.

Scope of the request

The Guide specifies that authorised third parties must abide by the limitation of information and data they can request as provided under the relevant regulations. In addition, the Guide notes that the data controller must ensure that:

- the data transferred to the authorised third party is covered by the provisions the authorised third party relied upon; and
- the information collected before transmission to the third party does not contain personal data 'in excess,' i.e. data not requested by the authorised third party. In relation to 'excess' data, the Guide specifies that, in cases where the request does not require the transmission of personal data, the data controller must consider limiting their response until the data requested is anonymised.

Professional secrecy

The Guide highlights that, in responding to an authorised third-party request in respect of which there is no provision for waiving one or more professional secrets, the organisation must be opposed to professional secrecy. In light of this, the Guide specifies that, before invoking professional secrecy, the data controller must ensure that the following two conditions have been met:

- Does the access request relate to information protected by professional secrecy? In this respect, the data controller is responsible for identifying the rules providing for such professional secrecy. However, the Guide notes that in cases where there is no specific provision for professional secrecy, the data controller may still be subject to professional secrecy.
- In cases where the request is related to information protected by professional secrecy, does the organisation making the request benefit from a legislative provision allowing the waiver of the professional secrecy? In this respect, the Guide notes that the absence of explicit provisions allowing the waiver of professional secrecy does not mean that an authorised third party is not entitled to the benefit of such waiver and that case law has shown that information which would be protected by professional secrecy was still transmitted to authorised third parties because such transmission was a necessary consequence of the provisions applicable to the third party (such as the specific mission entrusted to a third party by virtue of legislation).

Secure communication requirements

The Guide outlines recommendations to ensure the secure communication of information which is not in a material form (e.g. not as paper documents or in another material form).

The Guide highlights that the data controller has an obligation to ensure an adequate level of security of data by implementing procedures, such as the use of encryption, of online exchange platforms that comply with state-of-the-art security standards, and of two separate transmission channels for sending separately the encrypted document and the decryption key.

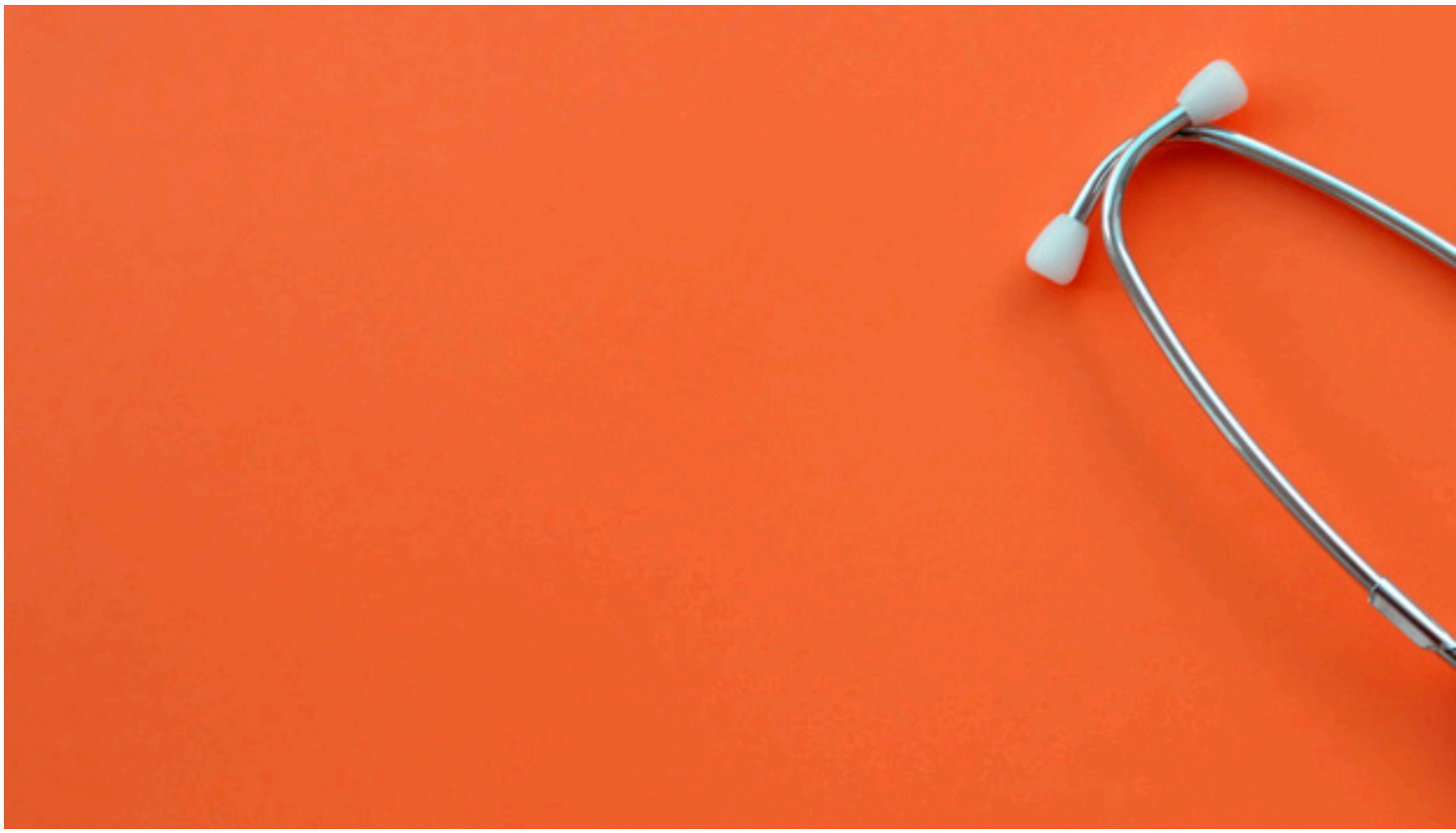
In addition, the Guide notes that if an organisation wants to oppose the authorised third party's request, the organisation must document any relevant element to justify its decision. The Guide also states that, depending on the applicable provisions, there are remedies when a request is rejected, such as an appeal.

Moreover, the Guide notes that information transmitted in the context of authorised third party requests can be retained if the processing:

- is justified on the basis of a specific and legitimate purpose in line with Article 5(1)(b) of the GDPR;
- affects data that is strictly limited to what is necessary for such purpose;
- does not occur for a period surpassing the time limit necessary for the achievement of such purpose; and
- is subject to appropriate security measures.

Lastly, the Guide strongly recommends the adoption of a policy for managing authorised third party requests, which should be shared with recipients of information or people responsible for dealing with such requests.

Suzanna Georgopoulou Privacy Analyst
sgeorgopoulou@onetrust.com



India: Government announces launch of National Digital Health Mission

The Prime Minister of India, Narendra Modi, announced, on 15 August 2020, the launch of the National Digital Health Mission ('NDHM'), with the aim of leveraging the power of technology to create a healthier India. The NHDM is part of the Government of India's initiative to develop and improve its healthcare system by increasing the use of data, information, technology, and infrastructure services. The NHDM seeks to benefit from emerging technologies such as artificial intelligence, Internet of Things, blockchain, and cloud computing to provide additional opportunities for facilitating a more holistic digital health system, that can increase the equitable access to health services, improve health outcomes, and reduce costs.

Earlier in 2017, the Government of India had launched the National Health Policy 2017, with the intention to create a digital health technology ecosystem and improve the efficiency, transparency, and patients experience in healthcare across the public and private sectors. In July 2019, the Ministry of Health and Family Welfare released the Draft National Digital Health Blueprint ('the Blueprint'), followed by a final report issued in November 2019. Similarly, the Blueprint aimed to establish and manage digital health data and the infrastructure required for data exchange, promote the adoption of open standards by all actors of the national digital health ecosystem, create a system of e-health records based on international standards, and establish data ownership pathways.

Scope

Matthew Chacko and Aadya Misra, Partner and Associate respectively at Spice Route Legal, highlighted that the NDHM introduces "the creation of specific actors [for instance] you may now see 'health data fiduciaries' or healthcare providers who are required to use software that will enable them to create health records and share it with users and 'health information users' ('HIUs') or entities that require patients' data. HIUs will be required to register with an infrastructure registry under the NDHM."

The NHDM aims to develop a strong mandate to ensure adoption across both public health and private ecosystems and help achieve the vision of interoperability within the health sector, with an emphasis on accessible and shareable health records. The NDHM strategy overview highlights that each healthcare provider creates health data for patients during every encounter, which commonly includes a diagnostic report, a discharge summary, prescriptions, and clinical notes. The NDHM will require healthcare providers to share a digital copy of any health reports being physically shared with the patients to enable the creation of longitudinal health records.

A system in line with data protection legislation

The Blueprint aimed to implement concept of data protection in all aspects of digital health data processing. The notions of Privacy by Design, electronic consent, anonymisation, de-identification, and encryption, among others, were

already presented as requirements to ensure the security of personal data. In the same vein, the NHDM implements principles of personal data protection which are in line and consistent with the upcoming privacy legislation. Under the NDHM, aggregated health data will become part of the National Health Analytics architecture, and shared in a way which is designed to be compliant with the provisions of the Personal Data Protection Bill, 2019 ('the Bill').

The NDHM will require healthcare providers to share a digital copy of any health reports being physically shared with the patients to enable the creation of longitudinal health records

Chacko and Misra noted, "the NDHM seeks to introduce interoperable digital health standards and systems in India, with a focus on security and privacy of health records. Most of the data protection principles in the NDHM are based on [the Bill]." In addition, and similarly to the Blueprint, the NDHM introduces the concept of anonymisation. Chacko and Misra added, "[the NDHM would] categorise health data into personal data and non-personal data, the latter of which would include aggregated information and datasets where personal identifiers have been removed."

Patients consent and control over health data

Similarly, to the Blueprint which introduces electronic consent framework and consent management to ensure the privacy on personal health data, the NDHM places consent at the centre of health data exchange between organisations. The NDHM will implement a federated health records management exchange system that will enable patients to access and share their information with appropriate consent and complete control of the record. The following elements, among others, will be part of the design of the system:

- owned by the individual, all records and their component will be owned and controlled by individuals;
- health lockers, in which patients will have the choice to store a copy of their records;
- consent-driven sharing, with the adoption of an appropriate digital consent management framework, as well as the implementation of options to revoke consent;
- 'forget my data' which will provide patients with the right to request health providers to delete their health data; and
- grievance, users will be provided with options to complain about the misuse of their personal health data.

Chacko and Misra outlined some of the key aspects of the NHDM, including, "the introduction of a centralised personal health record system which would enable patients to maintain and view their individual and consolidated health records." Moreover, the NHDM seeks to increase the importance of consent with regards to personal health data. On this point, Chacko and Misra noted, "there is a drive to create a user consent-based architecture. Apart from requiring users' consent to share health data, the initiative also includes issuing health IDs to patients and introducing 'health lockers' or digital platforms for users to store data. IDs will be linked to data consent managers. [...] All health data that is exchanged would be upon users' consent and in a prescribed manner. This process draws interesting parallels with the exchange of information in the financial sector through the use of account aggregators, a process that is regulated by the Reserve Bank of India."

Mona Benaissa Privacy Analyst
mbenaissa@onetrust.com

Comments provided by:
Mathew Chacko Partner
mathew@spiceroutelegal.com
Aadya Misra Associate
aadya.misra@spiceroutelegal.com
Spice Route Legal, Bangalore

5 MINUTES WITH...

Odia Kagan

Odia is a Partner and Chair of GDPR Compliance & International Privacy at Fox Rothschild LLP, a national US based law firm with 27 locations across the US. Odia combines her in-depth knowledge of data protection regulations and best practices with her keen understanding of emerging technologies to provide clients with practical advice on how to deploy their products and services, and engage third-parties in compliance with data protection laws.

Tell us a bit about your job role and how you have progressed in your career?

In my role I provide companies with personalised, pragmatic actionable advice on how to structure their products and services in a way that is compliant with data protection laws. I work with a few key industries including: manufacturers and providers in the automotive industry, and companies with complex data use issues in the data analytics/adtech/media space. Having said that, I've been fortunate to work with a cross section of hundreds of companies of different sizes and across different industries which gives a lot of variety and a broad insight into the problems that many companies are facing.

I started my legal career as an officer in the Israeli Defense Forces JAG corps. That was my last position in the public sector or as a litigator... Since then I had worked in law firms. In 2008 I moved to the US and have been practicing law in Philadelphia ever since, focusing on data privacy and technology.

What alternative job would you have if you had not gone into law?

This is a tough question because I had decided that I would go into law when I was 3 years old and have not regretted it ever since! I took my first law class in 3rd grade and my major in high school was Legal Studies...

If I were to pick another job I would say – a creative in an advertising agency. I am a fan of shopping, cosmetics, fashion magazines, and interior design and spend time enjoying fashion advertisements, many of which are a form of art, wit, and creative flare. I like the idea of being creative, and using my understanding of the market conditions, and people's needs and problems, to help a client figure out the best way to present their product or services and to craft the right message. Those are all aspects of my job in data protection counseling.

What is something you love about your job, and what is something you do not love?

The fact that it is like solving a complex 3D puzzle with facts and laws being the puzzle pieces. I like being able to solve problems and find a way to 'yes' which enables the client to move forward in a way that mitigates their risk. Saying 'you can't do this' is easy. It's harder to find a way to actually be able to do this, and allow innovation to co-habitate with data protection. In my daily work I need to keep up with ever changing laws, and be able to figure out how they actually apply in practice to unique factual situations.

Entering time, and reviewing invoices....are not a joyful time in my day. But - invoices and entering time are the lawyers' form of accountability. Just like we repeatedly express to clients how important accountability is under GDPR or CCPA even though keeping up with policies and procedures is mundane – so are attorneys duty bound to produce accurate and transparent invoices and bills.

Where is your favourite place on earth?

My top favorite places are: the grand lobby of the Raffles hotel in Singapore; walking down the central business district of Chicago; the inside of a well-stocked Sephora; and the recliner in my bedroom, under a fuzzy blanket watching a movie with my family.

Who would play you in a film about your life?

Julia Roberts I hope. I need to do a few more cool things to get her attention!

What is your favourite book?

Definitely 1984 by George Orwell. It was powerful and disconcerting and, of course, a staple for understanding privacy and data protection. I was also very influenced by his other book, Animal Farm. The injustice stayed with me for weeks after reading it. The book 'Growth Mindset' by Carol Dweck changed my life and taught me to look at things as a starting point for change rather than as a foregone result. And finally – I am a big fan of the 'Shopaholic' series by Sophie Kinsella and other and romantic comedy literature by Jane Green, Marian Keyes and others.

What is some advice you would give to others starting off in your industry?

- Be curious and knowledge hungry. This is a super fast-paced area of the law and you could walk to make coffee and suddenly a big guidance is issued that changes everything (true story).
- Find the area of the practice that speaks to you and that you can relate to. This is universally true but specifically for a legal career that is very demanding from a time investment perspective. If you are going to spend the vast majority of your time working, or thinking about work, it might as well be something that inspires you, or challenges you, or that you care so much about that you can't drop the amended-version-of-CCPA-regulations-because-you-have-to-know-what-happens-at-the-end (also maybe true story...)
- Don't be afraid to step out of your comfort zone or, as the sign on my wall says "Do one thing every day that scares you."

Who is your inspiration?

My grandmother, Esther Vinnik. When asked what is the one thing she would take with her to a deserted island she said "An apartment building complete with all the tenants." She was very brave, determined, tenacious, witty, and an out-of-the-box thinker. She was a person who had a lot of hardships in her life – long exile in Siberia under dire conditions, inability to go to university to study her profession of choice (which was the law), moving to a foreign country (Israel) in her 40s, and starting from scratch – but was never bitter, and never lost her optimism, her joy, her drive to help people, and her deep connections with friends and the community.

Odia is a regular contributor for OneTrust DataGuidance, read her latest Insight article discussing the Schrems II Case on the DataGuidance platform today

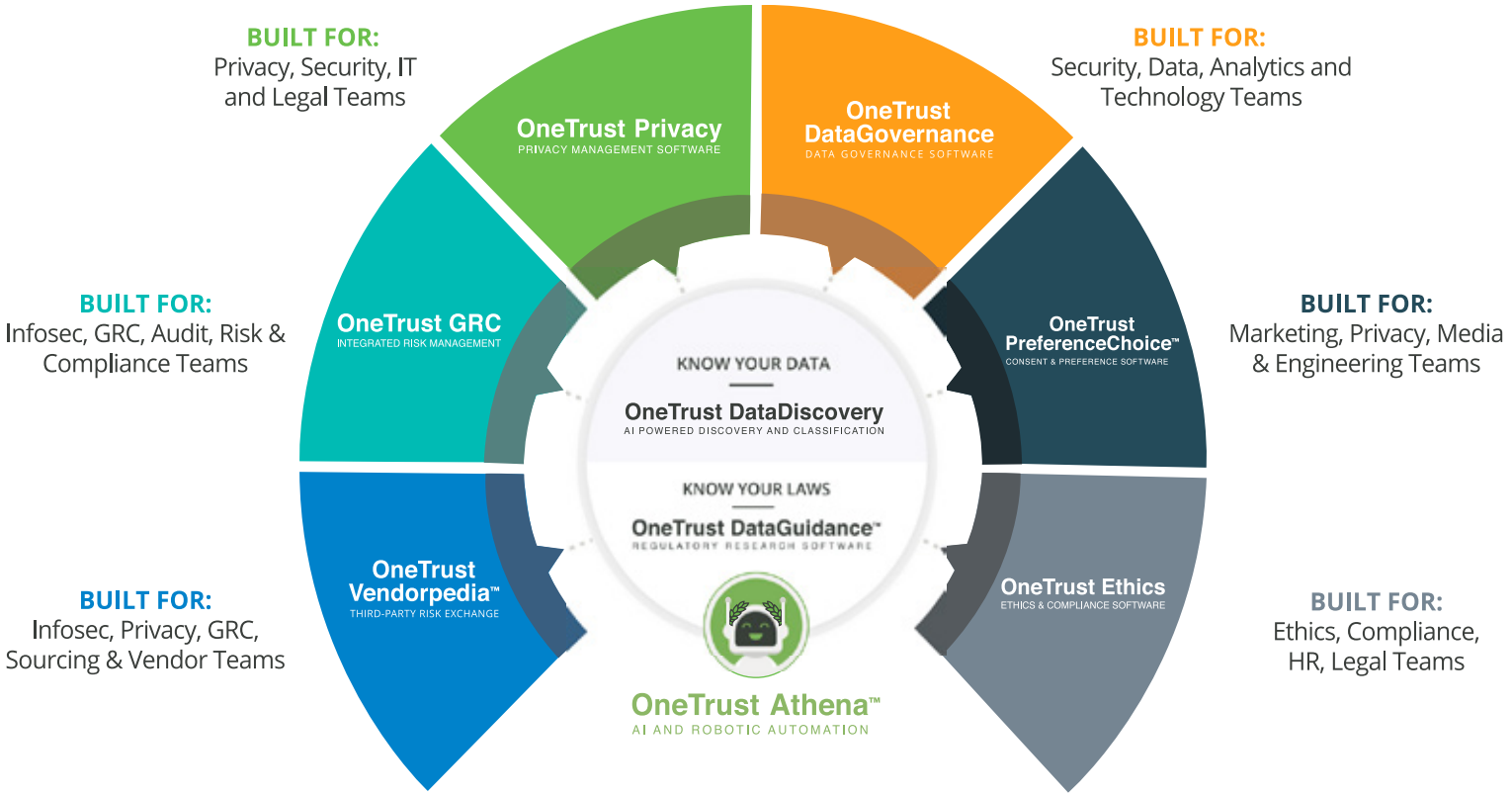
OneTrust

PRIVACY, SECURITY & GOVERNANCE

Be a More Trusted Organization™

The #1 Most Widely Used Platform to Operationalize

Privacy, Security & Governance



Trusted by 6,000 Customers, Both Big and Small

aetna™ Allianz Akamai Marketo ORACLE vevo Steelcase randstad

Interested in what OneTrust can do for your business?

WATCH A DEMO

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

Website: www.dataguidance.com

Email: DPL@onetrust.com