Volume 6, Issue 1
January 2024
dataguidance.com

DATA PROTECTION LEADER

Ideas shaping privacy, published by OneTrust DataGuidance™

PRIVACY GOVERNANCE CHALLENGES FOR 2024

EU AI ACT

Answering questions about next steps and how organizations can prepare

EMPLOYEE ENGAGEMENT

Exploring how to build a successful data protection employee engagement program

GRC PRACTICES FOR AI

Discussing how to incorporate safety, security, and privacy into AI

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.

Natalija Bitiukova, Ikea
Natalija Bitiukova is a Global Data Privacy Lead working for IKEA Retail (Ingka Group). She also serves on the board of the Lithuania-based non-profit organization Human Rights Monitoring Institute (HRMI) and is a co-chair of PrivacyConnect Copenhagen Chapter. Natalija has researched the implications of online manipulation and data misuse for democratic processes and has contributed to the study commissioned by the European Parliament (LIBE) on the impact of propaganda on the functioning of the rule of law in the EU.

Dr. Carlo Piltz, Piltz Legal
Dr. Carlo Piltz accompanies and advises national and international clients in questions of data protection, IT security, and IT law. Carlo supports compliance and legal departments as well as internal data protection officers in day-to-day business as well as in complex cases and contract negotiations. Carlo also works as an external data protection officer. Carlo's passion is also administrative law and he has successfully completed the theoretical training to become a specialist lawyer for administrative law. Carlo was invited to the respective parliaments as an expert for both the new version of the Federal Data Protection Act and the Berlin State Data Protection Act.

Alexander Weiß, Piltz Legal
Alexander has been working as a lawyer at Piltz Legal since 2022 and advise clients on data protection, IT security and IT law. In addition, he also advises on new European digital laws, such as the Cyber Resilience Act, the Data Act or the AI Act. Alexander came into contact with digital legal issues during his studies at Humboldt University in Berlin, which he completed in 2017 with a focus on intellectual property law. From 2017 to 2019, Alexander worked as a research assistant at an internationally oriented multidisciplinary business law firm in the area of legal tech and the digitalization of law. During his legal clerkship at the Higher Regional Court in Berlin, completed in 2022, he was able to gain further experience in data protection and IT law at several companies and law firms.

Alex Sharpe, Sharpe Management Consulting, LLC
Alex is a long-time (+30 years) Cybersecurity, Governance, and Digital Transformation expert with real-world operational experience. Alex has run business units and has influenced national policy. He has spent much of his career helping corporations and government agencies create value while mitigating cyber risk. This provides him a pragmatic understanding of the delicate balance between Business realities, Cybersecurity, and Operational Effectiveness. Alex has been recognized as a thought leader in Business Strategy, Cybersecurity, Risk Management, National Security, and the Cloud.

Lisa Fitzgerald, Lander & Rogers
Lisa Fitzgerald is a partner in the Corporate practice at Lander & Rogers and co-head of the firm's Digital Economy practice. In addition to general commercial, corporate and regulatory work, Lisa specialises in technology, media, telecommunications, privacy, cyber security and intellectual property rights. Lisa's practice covers all aspects of technology, media, telecommunications, data, privacy and intellectual property rights, with a focus on emerging technologies, data services and cyber security.

Keely O'Dowd, Lander & Rogers
Keely is a Senior Associate in Lander & Rogers' Digital Economy practice, specialising in technology projects, intellectual property, privacy, and cyber security. Keely advises on a broad range of technology transactions, including IT procurement, outsourcing, and software licensing, as well as privacy and cybersecurity compliance and data protection matters.

Image production credits
Cover / page 4 image: KS BioGeo/ Signature collection / istockphoto.com
Page 6-7 image: Ramberg / Signature collection / istockphoto.com
Page 8-9 image: blackdovfx / Signature collection / istockphoto.com
Page 12-13 image: Wirestock / Essentials collection / istockphoto.com
Page 16-17 image: Adam Calaitzis/ Essentials collection / istockphoto.com
Page 20-21 image: MicroStockHub / Signature collection / istockphoto.com
Page 24-25 image: NicoElNino / Essentials collection / istockphoto.com
Page 26 image: tigristiara / Essentials 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

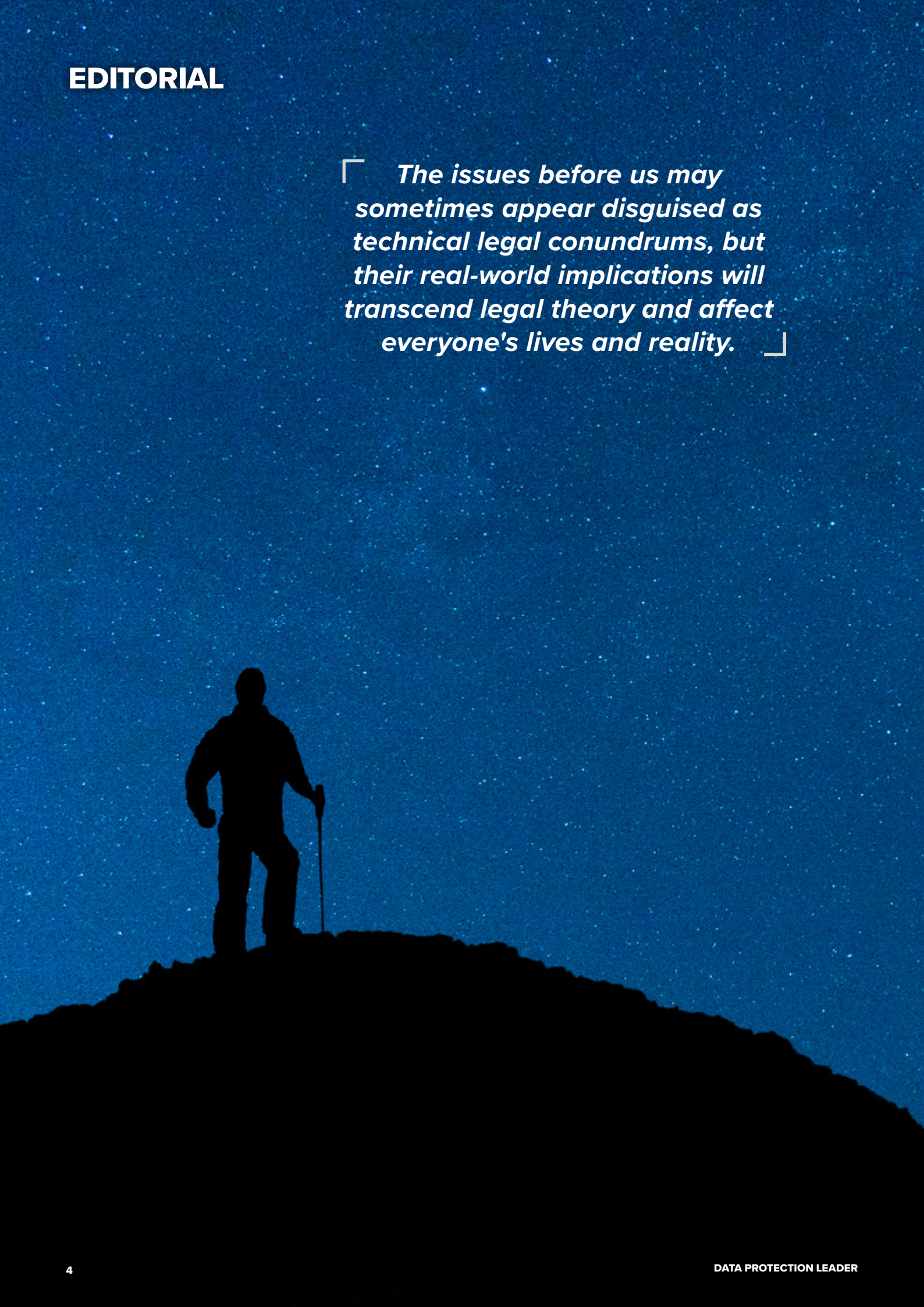
Managing Editor **Alexis Kateifides**
akateifides@onetrust.com

Editorial Lead **Victoria Prescott**
vprescott@onetrust.com

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

CONTENTS

EDITORIAL



The issues before us may sometimes appear disguised as technical legal conundrums, but their real-world implications will transcend legal theory and affect everyone's lives and reality.

Editorial: Privacy governance challenges for 2024

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

2024 is set to be a year of significant change. Geopolitical change. Technological change. Social change. While change can, of course, be an opportunity to do things better and that should be our constant aspiration, the changes ahead will bring considerable challenges - many outside our control and some within our control. Those of us working in data protection, privacy and cybersecurity will find ourselves at the forefront of this process and face some real tests of knowledge and good judgment. The issues before us may sometimes appear disguised as technical legal conundrums, but their real-world implications will transcend legal theory and affect everyone's lives and reality. Here are some of the big challenges that we are going to have to tackle:

Justifying evolving data processing activities

As uses of data become more creative and ambitious, finding a justifiable legal basis for that processing will be a constant and elusive exercise, particularly given the increasingly restrictive interpretations of "contractual necessity" and "legitimate interests". We will need to operate within the boundaries set out by courts while continuing the debate with policy makers and regulators.

Narrowing role of vendors as processors

The growth and creativity in the uses of data for things like machine learning and product improvement are testing the role of service providers as humble processors like never before. The instinctive thinking may be to move into a controllership situation where those service providers become masters of their own data processing activities, but this brings with it some challenging situations to overcome given the lack relationship with data subjects. Therefore, exploring the boundaries of what a processor can do with data while still being a processor will be a constant task.

Weaponization of rights

In a world where polarization is the order of the day, relying on data subjects' rights as a tool to fight wider causes, which may have little to do with the protection of data is an obvious reality. Regulators will be a victim of this trend as much as organizations acting as controllers. The question will be how to ensure that data protection rights are properly honored without diminishing their crucial value.

Hostility towards automated decision-making

When the Court of Justice of the EU (CJEU) takes a particularly strict view on a data protection issue, you know this is going to attract the regulators' attention. The recent CJEU jurisprudence on automated decision-making that significantly affects individuals is bound to do exactly that precisely at the time when this type of practice grows exponentially. Expect a toughening of approach on any uses of technology that may be seen as blind reliance on the "computer says no" doctrine.

Regulators becoming legislators

A particular growing trend in the US facilitated by various state privacy laws, will likely amplify the effect of emerging legislation in this space. From California to New Jersey and beyond, we are going to see local regulators adopting a creative approach to their function and passing their own home-made regulations. Just being up to speed with these new rules will be a job in itself, let alone complying with them.

Global data flows in an increasingly autocratic world

The EU-U.S. Data Privacy Framework may have taken off some of the immediate pressure affecting Transatlantic transfers of personal data, but the hard core interpretation of Schrems II has not gone away. Apply that thinking in today's context of autocratic leaders and governments seeking unrestricted access to data and the picture is not pretty. Are we heading towards an environment of generalized distrust on the global sharing of data? That is a question that we will be grappling with for the foreseeable future.

Mastering DPIAs

Judging by how privacy regulators are approaching pretty much every investigation, having a solid and compelling story to tell as demonstrated by a well-reasoned DPIA is an absolute priority. In practice, that means deploying a system that spots when to do a DPIA and being as robust as possible in the assessment itself. The importance of DPIAs as a tool to identify data protection risks and address any weaknesses cannot be overemphasized. Those who master the art of doing DPIAs will be the true privacy gurus.

Transition of privacy accountability towards AI governance

And then, the biggest topic of our time: AI. All signs seem to indicate that privacy and data protection professionals are going to end up taking a leading role in managing AI regulatory compliance. This is a new area of governance which appears so close and yet so far from the issues we are used to dealing with. Many transferable skills will need to be applied to a completely new set of requirements. The challenge here is truly served.

So as the year progresses and the shaky reality of the world engulfs us, each of us will play a significant role in getting these issues right. And while there is always room for debate and the positions may not necessarily be aligned, we must remember that it is in everyone's interest to find a workable path to these challenges. Extreme positions in any debate are usually the loudest but hardly ever the correct or most helpful ones. The greater our dose of responsible pragmatism in addressing the privacy governance challenges in front of us, the greater our chances of success will be.

EU: The AI Act is here - what now?

Dr. Carlo Piltz Partner
carlo.piltz@piltz.legal
Piltz Legal, Berlin

Alexander Weiß Associate
alexander.weiss@piltz.legal
Piltz Legal, Berlin

What are the next steps for the draft EU AI Act now that trilogue discussions have concluded? Is the Act still at risk of not becoming law?

Until recently, the European Parliament and the European Council were in the so-called trilogue. In these negotiations, representatives of the two institutions worked out a joint legislative proposal with the mediation of the European Commission. A draft text was recently published. This draft must now be adopted by the Parliament and the Council and can then be published in the Official Journal.

On February 2, 2024, the Committee of the Permanent Representatives of the Governments of the Member States to the European Union (Coreper) approved the final draft of the AI Act. The AI Act must now be formally adopted by the Council and the European Parliament.

If the final stages of the legislative process proceed as planned, the AI Act is likely to enter into force in summer 2024. In principle, the AI Act would then become fully applicable 24 months later in 2026.

It is currently still unclear whether the Member States will approve the draft. At least a qualified majority is required, which means 15 states with a population of at least 65%. In France for example, the approval is not certain.

If the Member States do not give their approval, a new attempt would only be possible in the next legislative period after the European elections in June. This would probably cause a delay of at least one year.

What will be the impact of the provisions on foundational models for organizations?

Contrary to the draft version of the European Parliament that contained provisions regarding foundation models and defined these as an AI system model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks, the final draft does not contain stipulations concerning this term anymore. However, the final draft of the AI Act contains the term 'general purpose AI model' in Article 3, paragraph 1, point 44b, meaning an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This is likely to include services such as ChatGPT.

The providers of such systems are subject to extensive obligations. For example, providers must maintain comprehensive technical documentation and shall ensure that users are informed that they are interacting with an AI system or a general purpose AI model. A privilege and thus an exception to these obligations only applies in the case of free and open source licenses, provided that these

models do not present a systemic risk. Providers of the latter systems are subject to extended obligations, such as ensuring an appropriate level of cyber security. Such systems are also monitored by the European Commission, which shall entrust the implementation of these tasks to the AI Office. *Inter alia*, the Commission can request documents to prove compliance and in some cases even request access to the AI model, and take measures, e.g., implement mitigation measures or restrict the making available on the market, withdraw or recall. Fines of 3% of the worldwide annual turnover for the preceding financial year or €15 million can be imposed on providers of general purpose AI models for breaches of the relevant regulations.

What do organizations need to be aware both in terms of the entry into force of the AI Act and the oversight and enforcement of it?

As soon as the AI Act is published in the Official Journal of the European Union, the regulation will enter into force on the twentieth day following its publication. After 24 months, the regulation shall apply.

However, some provisions will apply earlier. For instance, Title I and II (General provisions and prohibited Artificial Intelligence practices) shall apply after six months of the entering into force. *Inter alia*, provisions regarding High Risk AI and General Purpose AI Models will apply from 12 months following the entry into force. The classification rules for high-risk AI systems and corresponding obligations in the AI Act shall apply from 36 months following the entry into force. The AI Office will be drawing up so-called Codes of practices covering obligations for providers of general-purpose AI models and of general purpose models presenting systemic risks. According to Recital 60t of the AI Act, these tools should represent a central tool for the proper compliance with the obligations.

With regard to sanctions, Article 71 of the AI Act stipulates that authorities may impose fines or other penalties such as warnings and non-monetary measures. The penalties provided for shall be effective, proportionate, and dissuasive. Vis-à-vis sanctions, the AI Act only provides a basic framework. However, the exact implementation is left to the member states.

Article 71 of the AI Act includes the following provisions:

- Fines of up to €35 million or 7% of a company's global turnover generated in the previous year can be imposed for breaches of the obligation in Article 5 of the AI Act (Prohibited Artificial Intelligence Practices).
- €15 million or 3% of the worldwide annual turnover for the preceding financial year can be imposed for violations of other obligations under the AI Act.
- False information to authorities is fined with €7.5 million or 1% of the previous year's global turnover.

Besides the sanctions described, natural and legal persons have the right to complain to the relevant market surveillance authorities in case of infringements of the AI Act's provisions.

What can organizations do now to prepare for the Act?

We recommend that all companies that use AI or launch AI on the market familiarize themselves with the provisions of the current draft. The AI Act will in some cases have a significant impact on the design of digital business models, the drafting of contracts, (e.g., for SaaS services with AI elements) and information obligations.

In particular, companies must check whether the systems used can be considered as AI and therefore fall under the AI Act. Another decisive factor is whether the company's own AI systems are to be classified as high-risk AI, as the most comprehensive obligations apply in this regard. *Inter alia*, many AI systems from the HR sector are considered high-risk AI (e.g., CV sorting software for recruitment processes).

In order to ensure that the obligations of the AI Act can be fulfilled, the creation of corresponding test processes and the recruitment of the necessary personnel resources should already be started now.

It should also be expected that the legal requirements will be further developed, optimized, and possibly even corrected. In this respect, legal developments in this area should continue to be monitored even after the AI Regulation comes into force.

International: Establishing GRC practices for AI

Alex Sharpe Principal
alex@sharpellc.com
Sharpe Management Consulting LLC

Introduction

Artificial intelligence (AI) can potentially revolutionize and disrupt how we work and live. While AI only recently gained mainstream attention, it is decades old, with the term 'artificial intelligence' going back to the 1950s. Like so many other emerging technologies, we have a technology-driven problem that technology alone cannot solve. We craft our value creation strategy, governance, and risk management approach by understanding how AI is different and how traditional governance, risk management, and compliance (GRC) practices are applied.

What makes the governance of AI different?

The answer lies in how AI is different. Once we understand how AI is different, we can craft governance programs that promote innovation and create value while ensuring safety, security, and privacy.

At its core, AI is software usually running on very specialized hardware. But it is not software like we traditionally think of software. With traditional software, we code formulas and procedures to perform specific tasks: mostly if-then-else statements, hand-coded formulas, and procedures.

With AI, we create a 'model' that we feed lots of data to 'train the model.' We code these models to tell the model what we will give it (input) and what we will be asking it to do. For example, 'Mr. Model, we will feed you lots of images with cars. Please figure out what a car is so you can identify those with cars when I give you images in the future.' These models effectively mimic human behavior.

Once trained, we input data either as a question or a request for an action to be accomplished, blocks of data to be summarized, classified, or to generate new data.

Traditional software is static once developed unless deliberately changed, usually involving a defined process under change control. Traditional software can be inspected. AI is constantly evolving as it is used and cannot be inspected.

As the model is used, it adapts (learns) and evolves based on experience and how it is tuned.

For example, feeding a model many images containing cars teaches it to identify cars. Feeding a model lots of text can teach it proper sentence structure. These models are almost always single-use. A model trained to identify cars in images cannot convert voice to text or find cancer cells in an x-ray.

The life cycle of an AI application can be generally decomposed into two broad phases: ***training*** and ***inference***. During the training phase, the model is developed and fed specially curated data called the ***training data***

to produce a trained model. The inference phase begins when the model is trained. During the inference phase, users input data (e.g., query), and the trained model produces output called inferences. References can be either a ***prediction*** or the ***completion of a task***. Quite often, a confidence level, in the form of a percentage, is provided with the inference so the user can make an informed decision.

Some governance-related items exist on the border between training and inference. For the sake of simplicity, we will not focus on where they belong, but rather, how they get addressed.

Experience shows it is best to assess risk and develop governance programs by looking at the training and inference phases across each of the elements:

- the model;
- the people (developers, data scientists) who build and maintain the model;
- the data used to train the model;
- the data inputs to the model;
- the output;
- the users; and
- the infrastructure.

How does the risk equation change?

How we view risk regarding AI fundamentally differs in two key ways. First, we look at how things tend to go wrong. Second, the integrity leg of the confidentiality, intelligence, and availability (CIA) triad becomes increasingly more critical.

AI creates new risks and new dimensions to existing risks while amplifying others. For example, the insider threat in an AI world is amplified.

When it comes to managing risk, Dr. A. Prabhakar, Director of the Office of Science and Technology Policy (OSTP) and the former Director of the Defense Advanced Research Projects Agency (DARPA), said it best:

"When we look at what's happening with AI, we see something compelling, but the technology is still quite limited. The problem is that when it's wrong, it's wrong in ways that no human would ever be."

Would our model trained to recognize cars, identity older models? Would it mistake a child's toy for a car? We do not know how to inspect these models yet. These models are constantly changing. Even if we could inspect, would the model we inspect today be in production tomorrow? In addition to extensive testing, the most common (and the lowest cost) mitigation is to keep humans in the loop.

An almost comical example is the reported instances of AI creating fake legal cases that have made their way into court documents. These are called Hallucinations and are most common in generative AI. Unfortunately, there are more life-threatening and impactful situations like false diagnoses. The simple act of checking output goes a long way. Naturally, the more impactful the outcome, the more oversight is warranted.

As AI is increasingly used in decision-making, safety, and security, the risk and the motivation for bad actors to influence increases.

> ***AI is a technology-driven problem that cannot be solved by technology alone. It requires a combination of technology, people, process, and organization.***

Consider the creation of a sandbox for the more experimental and riskier use cases to contain the blast radius when things go wrong. Many organizations are limiting the use of different forms of AI to select groups until they get a better handle on the situation. Whether for a sandbox or restricted use, the guardrails can be strengthened as you figure them out before full-scale rollout.

Confidentiality, integrity, availability

Information security (INFOSEC), cybersecurity, and privacy historically focus on ensuring only authorized users are given access to information (i.e., confidentiality). To a lesser extent, we also concentrate on providing systems and data that are available when needed (i.e., availability). Until AI, integrity has mostly been the concern of fraud and, to a lesser extent, devices, especially medical devices. AI increases the importance of the integrity leg of the CIA triad.

As AI is driven by the model, the data, and ongoing usage, our governance models need to focus not only on confidentiality and availability but also on the integrity of the component, the operation of the model, and monitoring the output.

Incorporating AI into existing GRC practices

The way scientists and developers categorize models does not lend itself to developing governance programs, assessing use cases, or communicating with stakeholders, shareholders, and users. Scientists and developers use terms like 'deep learning,' 'fuzzy logic,' and 'reactive machines.' The rest of us discuss categories like machine learning, neural networks, and generative AI. Product vendors use product names. Unfortunately, a clean taxonomy does not exist, and a lack of common terminology hinders our ability to communicate reliably.

> ***As AI is increasingly used in decision-making, safety, and security, the risk and the motivation for bad actors to influence increases.***

Efforts by standards bodies and industry bodies are developing a common taxonomy with agreed-upon language. Until then, we can craft our governance programs around deployment models and modalities driving toward specific use cases.

Deployment models range from most to least controlled: on-premises custom-built models using our proprietary data are totally under our control. Publicly available products with AI embedded within them are the most out of our control. In between is a range driven by your sector and value creation strategy.

Modalities is a fancy way of categorizing the output type: text, code, images, voice, video, and the like.

As we craft our programs, policies, and controls, we need to look at the traditional factors of likelihood and impact through the lens of both the modality and the deployment model. AI embedded in an office productivity tool to check spelling, grammar, and punctuation presents a different risk than a custom-built application used for making medical diagnoses.

Basic blocking and tackling

This is where traditional security practices, applied to AI, can have an immediate impact.

The guiding principles underlying Zero Trust are directly applicable to AI governance. While the Cloud Security Alliance (CSA) has pieces in the works that view AI through the lens of Zero Trust, they are not yet available. In the meantime, you can review Zero Trust Guiding Principles[1].

Data scientists and the producers of models are not known for their security practices. They are scientists. Often, data scientists are overprivileged and high-value targets – a very risky combination. Many people who build the models (and the model's components) struggle to believe somebody would actively engage to alter data or muck with the model.

Many models do not have access control features as we see in enterprise applications, let alone logging or monitoring. Near term you will most likely need to provide these protections outside of the model in the supporting infrastructure.

Establish a working group

AI is a technology-driven problem that cannot be solved by technology alone. It requires a combination of technology, people, process, and organization. A working group or at least a steering committee needs to be formed. In a perfect world, it would be part of a board committee. At the very least, it needs to be chartered by the board to have proper authority. It needs to be multi-disciplinary across the organization with representation from the business units, legal, compliance, HR, risk, and the like.

Corporate policies

Corporate policies need to be updated. A dedicated AI policy is more than likely required. Given the large-scale adoption of publicly available tools, especially generative AI tools, updates to existing Acceptable Use Policy(s) (AUP) are probably the most pressing. Many organizations prefer an addendum versus a wholesale rewrite of the AUP. While updating policies, it is important to recognize the specific needs of the different modalities and service delivery models.

Identity and Access Management

Extend Identity and Access Management (IAM) practices to the data scientists and model developers. The concept of least privilege, separation of duties, and role-based access control will go a long way. Be sure to control access to the training data, the model - especially for those who can make changes -, and users.

Anyone who can affect the data, modify the model, or perform maintenance should be treated as a highly privileged user. They should have separate logins for their official roles and as regular employees. Practices for highly privileged roles, like system administrators, should be applied to your AI team.

Model integrity

More than likely, the model does not come with built-in access controls, so the controls will need to be built around the model. The integrity of the model must also be protected. The model needs to be protected to retain its CIA, especially for mission-critical applications.

When it comes to integrity, it is essential to prevent unauthorized changes and detect them. Organizations are using cryptographic hashes and digital signatures to detect changes and foster configuration management.

Training data

Training data drives the model. It is at the heart of everything you do with AI. The source of the training data (provenance) must be known, and the integrity of the data must be maintained. It must be stored in a way that restricts access, protects its confidentiality, and cannot be changed in an undetectable way (integrity). Digital signatures are an excellent way of detecting unauthorized changes.

It is important to recognize that if the model becomes corrupted (benignly or maliciously), it may need to be retrained. Confidence in the training data's integrity is critical to confidence in the model.

Knowing the value of AI is driven by the data can result in too much data being collected and retained, placing you at the risk of getting sideways with privacy, legislatures, and regulators.

Knowing the value of AI is driven by the data, adversaries, especially APTs and

Nation States, are even more inclined to steal (and manipulate) your data.

Awareness and training

Three new groups require tailored AI training – data scientists, model developers, and users.

The awareness of data scientists and model developers needs to be enhanced to understand the malicious and accidental threats to the data and the model.

Users are to be trained on corporate policies and resources, along with the need to be skeptical of any output. Making users aware of the need not just to take output at face value but to be on the lookout for both inadvertent errors like hallucinations and malicious attacks like deep fakes is vital. Providing users with basic instructions and contact information on how to proceed is incredibly useful.

Deep fakes and influence operations

Adversarial AI, especially with social engineering attacks, is on the rise. Tailored training for relevant roles like help desk personnel, systems administrators, executive support staff, and accounts payable is recommended.

The Cybersecurity and Infrastructure and Security Agency (CISA), the Federal Bureau of Investigations (FBI), the National Security Agency (NSA), and the UK's National Cybersecurity Center have excellent resources[2345].

Logging and monitoring

Logging and monitoring features and functions are likely not inherent to your model or data sets. They will need to be provided through the supporting infrastructure.

Logging and monitoring will need to be developed for event detection, traceability, and incident response. More likely, your organizations have standards in this space. It is best to start there and look towards viewing those through the lens of AI.

Role of AI Bill of Materials

Much like a traditional Bill of Materials (BoM), an AI BoM provides a detailed inventory of all components of an AI product – the components within the product, how it was trained, cautions, and instructions. Just like a BoM tells us what is on a truck or a Software BoM (SBoM) maps out third-party software in a product, an AI BoM provides insight.

An AI BoM is like a list of ingredients and nutritional information on food products.

While the standard(s) for AI BoMs are evolving, it is clear they have two primary purposes. First, an AI BoM provides transparency so you can make informed, risk-based decisions. Second, when something goes wrong, and it will, the AI BoM provides insight so you can assess the impact, determine the next steps, contain, respond, and correct.

It is only a matter of time before we learn of a component embedded in an AI product, like we saw with Log4J, that we need to assess before determining the next steps. An AI BoM provides transparency, reduces confusion, and accelerates the timeline. In a perfect world, an AI BoM will also provide instructions.

Anyone looking to use a product will benefit from an AI BoM. Anyone building a product will foster adoption and gain credibility by providing an AI BoM. Given the shift of liability from customers to product vendors and service providers globally, as evidenced by the National Cybersecurity Strategy[67] and Security by Design and Default[8], it is only a matter of time before AI BoMS are demanded by customers, regulators, and legislatures.

Closing

AI has great potential. Like any disruptive technology with great potential, we are best served by incorporating safety, security, and privacy into our value-creation strategy. AI is different. Understanding how it is different is the key to not only creating value but also our risk mitigation.

1. *See: https://cloudsecurityalliance.org/artifacts/zero-trust-guiding-principles/*
2. *See: https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats*
3. *See: https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF*
4. *See: https://www.ic3.gov/Media/Y2023/PSA230605*
5. *See: https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure*
6. *See: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*
7. *See: https://www.dataguidance.com/opinion/usa-three-rs-us-national-cybersecurity-strategy*
8. *See: https://www.cisa.gov/securebydesign*

Meet a DPO:
Natalija Bitiukova, Global DPO at IKEA

Tell us about yourself and your role.
I hold the position of the Global Data Protection Officer at IKEA (Ingka Group). My role is multifaceted, encompassing two key dimensions. I inform and advise the business on data protection matters and I also monitor businesses' compliance with the data protection law and our internal privacy commitments.

I lead a small team of senior Global Data Protection Officers assigned to different parts of our multinational business, including Global Functions, IKEA Retail and Ingka centres. We work closely with our Global Cyber Security & Privacy team which provides day-to-day operational support and enablement to Ingka Group teams and our network of local Information Security & Data Privacy Leads in different countries.

No two days in the world of data protection are alike, and that's what keeps this role fascinating. My days are a dynamic mix of diverse tasks. I might begin by engaging with our marketing department, providing privacy insights into their annual strategy. Later, I could find myself analyzing a new privacy law in India, drafting a Data Protection Officer opinion on a cutting-edge digital initiative, and culminating the day with a training session. The ever-changing landscape ensures that it's never a dull moment.

What drew you to working in data protection and privacy?
The nexus of law and technology has always intrigued me, and my journey through this intersection has taken various forms. My career commenced as a human rights lawyer, focusing on research and litigation across different human rights domains, including criminal justice, victims' rights, non-discrimination, freedom of expression, and the right to privacy. Later, my path led me to Brussels, where I worked at the European Data Protection Supervisor and focussed specifically on the questions of online manipulation. Subsequently, I transitioned my expertise into the business world, first as a consultant and later as a legal counsel and DPO. Even though I deal with complex business cases on a daily basis, I continuously return to the core of the fundamental right to privacy and the fundamental rights framework as a whole.

What are the key privacy compliance areas that are top of mind for you right now for your program?
At the moment, several key privacy compliance areas are taking centre stage in our program. Embedding data privacy controls and leveraging privacy-enhancing technologies for our data-driven digital products is one of our top priorities. Additionally, we are closely monitoring evolving data protection and data-related regulations worldwide, such as the Digital Personal Data Protection Bill in India and the upcoming AI Act in the EU, to ensure our program aligns with the latest legal requirements. Lastly, we are committed to fostering a culture of privacy within our organization, and innovating in training and awareness space to make privacy learning more tailored to the needs of different business areas.

What are the key elements of your privacy program? Is it based on particular laws/standards/frameworks? How has it evolved over time?

Our privacy program is founded on a combination of international data protection laws, industry standards, and best practices. Historically, the General Data Protection Regulation was one of the core tenants of our programme, but it has evolved significantly over time, reflecting the ever-changing privacy landscape and emerging privacy requirements and their interpretation around the world. This evolution is crucial to stay agile and adaptive in the face of emerging technological and regulatory changes. Key elements of our programme are across three main areas:

1. Processes. Comprehensive data protection policies and procedures, privacy by design assessments (encompassing LIA, TIA, DPIA, etc.) and privacy control framework.
2. People. A robust central privacy organization supported by a network of dedicated privacy leads across Ingka Group's markets.
3. Technology. Utilization of privacy management suit and solutions to track and measure our maturity and progress towards privacy goals.

Which other business functions do you regularly interact with, and why?

At IKEA, 'togetherness' is one of our core values so, naturally, cross-functional collaboration is key in ensuring the success of our privacy program. I frequently engage with various business functions, including group digital, data and product teams, data and analytics, and marketing. These interactions are essential because data touches every aspect of our organization and are striving to embed privacy considerations at all levels - strategic, tactical and operational. Leadership from the top and cohesive effort is vital for effective privacy management.

What are your thoughts on the rapid pace of change within data protection and privacy? Are there any recent developments that have been of either personal or business interest?

The rapid pace of change within data protection and privacy is both exhilarating and challenging. It keeps us on our toes, but it also offers opportunities for innovation and better protection of individuals' data. Recent developments, such as the emergence of comprehensive state-level privacy laws in the US, the Digital Personal Data Protection Bill in India and discussions on AI legislative initiatives across the world, have been of significant interest to our business. Personally, I also found particularly interesting the recently adopted European Sustainability Reporting Standards (ESRS) which now legally mandate proactive disclosures on the ESG matters and specifically reference data privacy on numerous occasions. I am also looking forward to the outcomes of the EDPB's coordinated enforcement of the role of DPOs. All these initiatives emphasize the important role of personal data protection, necessitating a proactive and adaptable approach.

What advice would you give to others looking to maintain and evolve their privacy programs?

To those seeking to advance their privacy programs, I'd offer the following advice:

- Stay informed, stay alert: Continuously monitor not only legislative but also technological changes worldwide Being aware of emerging privacy trends and staying informed about legal and technological developments is essential when providing informed and all-rounded advice to your stakeholders.
- Engage and learn: Foster strong relationships and open lines of communication with key stakeholders across your organization. Learn from your stakeholders, and create opportunities Privacy is a team effort, and collaboration is essential.
- Monitor and measure: As the saying goes, "If it cannot be measured, it cannot be managed." Understanding your position in your privacy management program and articulating the business value it brings will elevate you as a trusted partner.

What do you think the biggest challenge facing the data protection industry at the moment is? Will this change over the next 5 years?

The biggest challenge facing the data protection industry right now is technological advancement in the AI space presenting novel privacy challenges and, in parallel, the increasing complexity of the data-related regulatory landscape. For instance, think of EU's alphabet soup of digital acts, such as DMA, DSA, Data Act, Data Governance Act, AI Act and similar. A number of these laws require establishing internal 'digital' compliance teams, mirroring the demands placed on DPOs under GDPR. This requires serious consideration of how future privacy governance and management models will look like and what capabilities privacy function 2.0 will need to put in place. At the same time, we as a community should be investing in our own knowledge development, understanding of the underlying technology and being able to bridge to translate these regulatory requirements into practical advice. Staying agile and proactive in the face of these challenges will be instrumental in the industry's continued success.

INFOGRAPHIC

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

GDPR Fine Enforcement: Q4 2023 Report

October 1, 2023 - December 31, 2023

Quarterly Enforcement Highlights

Total Fines Issued

20,832,532 €

Largest Singular Fine

10,000,000 €

Garante fines Axpo Italia €10M for concluding unsolicited contracts containing incorrect personal data

Most Enforcements

39

Spain

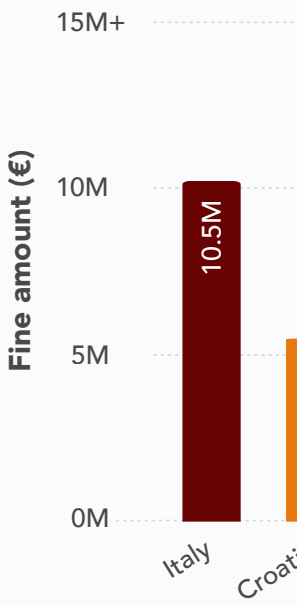
accounted for 43% of enforcements with 39 total

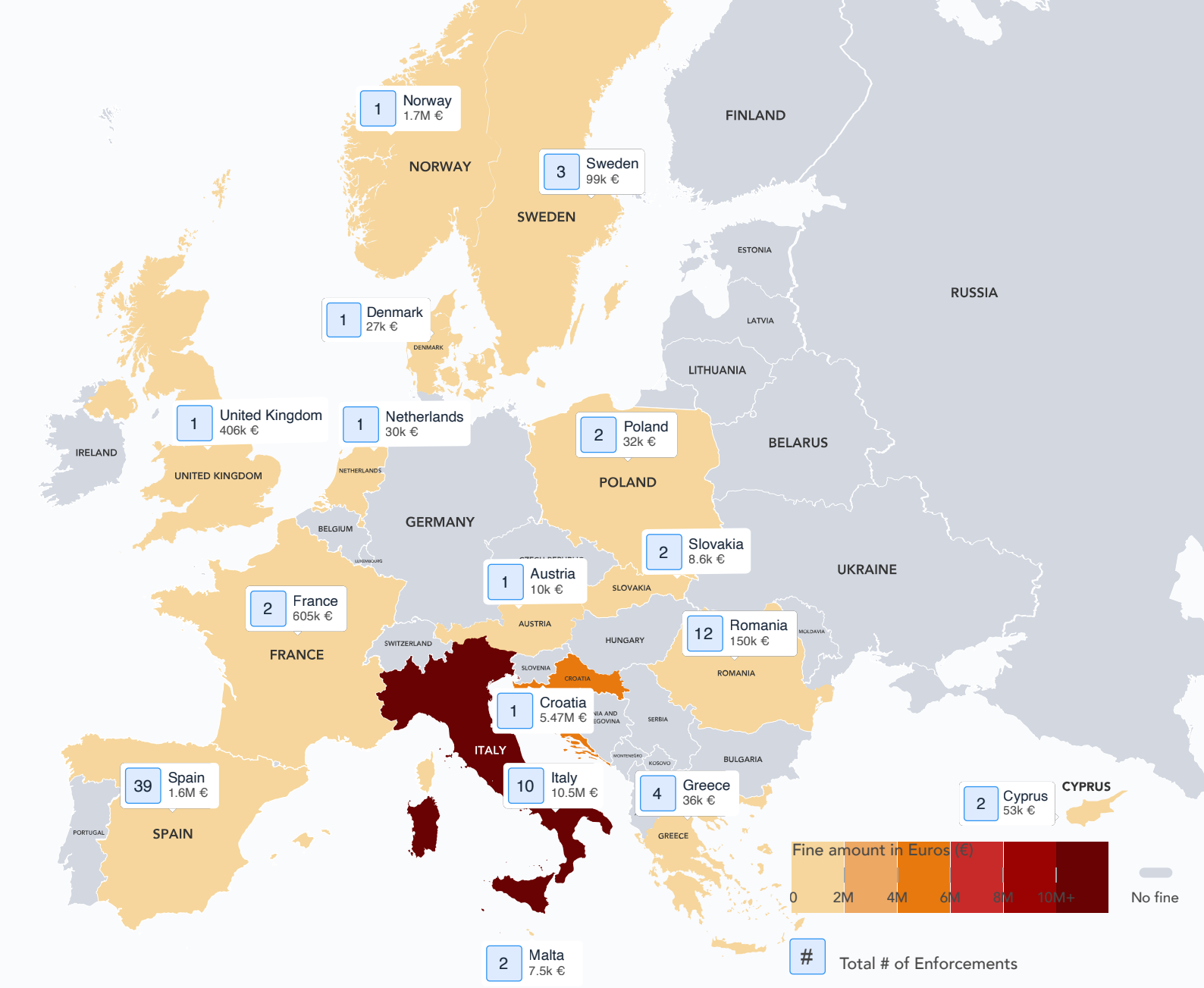
Most Frequently Enforced

Principles relating to processing

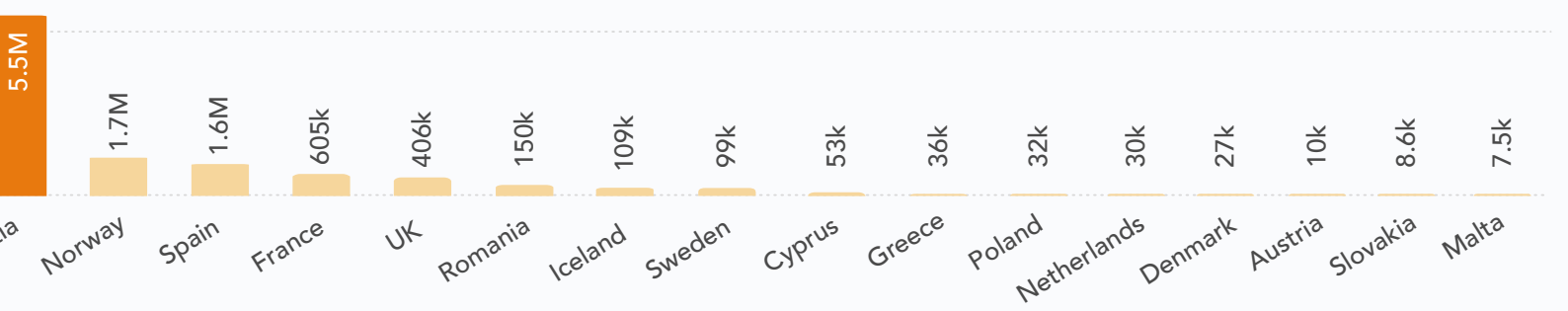
accounted for 29% of all enforcements issued

Fine Amou



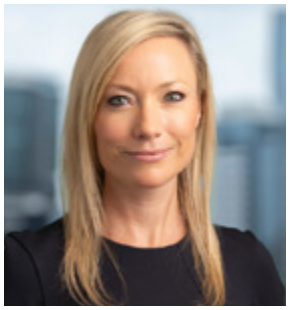


nts by Jurisdiction



Country profile: Australia

Sweeping reform and greater regulatory action on the horizon



Lisa Fitzgerald Partner
lfitzgerald@landers.com.au
Lander & Rogers

Keely O'Dowd Senior Associate
kodowd@landers.com.au
Lander & Rogers

This article was written on September 25, 2023. The Australian Government has since published its response to the Privacy Act review on September 28, 2023.

During 2022-2023, Australian organizations suffered the most serious and pervasive data breaches in the nation's history. Some if its largest corporates all suffered major, malicious, and seemingly systematic cyber-attacks.

These data breaches were a catalyst for Australian organizations, regulators, and policy makers to sharpen their focus not only on the adequacy of privacy and data protection laws, data governance, and cybersecurity risk management, but their relationship with directors' duties under Australian law.

Consequently, we are witnessing the development of an increasingly complex privacy and data protection regulatory landscape due to recent privacy law changes, further reforms on the horizon, and a multi-regulator environment with overlapping regulatory remit. We explore these developments in this article.

Recent privacy law changes

In response to the Singtel Optus Pty Ltd and Medibank Private Limited data breaches, the Australian Government swiftly passed the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Act) (the Amending Act). The Amending Act was introduced into the Parliament of Australia on October 26, 2022 and received royal assent on December 12, 2022. The Amending Act implements the most significant reforms to Australia's privacy laws since the commencement of the Notifiable Data Breaches scheme in 2018.

The Amending Act amended the Privacy Act 1988 (Cth) (the Privacy Act) by:

- expanding the extraterritorial reach of the Privacy Act;
- significantly increasing penalties for serious or repeated interferences with privacy;
- strengthening the Notifiable Bata Breaches scheme;
- introducing new information sharing powers for the Office of the Australian Information Commissioner (OAIC) and the Australian Communications

and Media Authority (ACMA); and
- enhancing the powers of the OAIC to investigate and resolve privacy breaches.

The increase in penalties for serious or repeated privacy breaches is intended to incentivize businesses to take strong privacy and cybersecurity measures to protect personal information they hold and to reflect community expectations. Penalties have been increased from AUD 2.22 million (approx. $1.4 million), to the greater of:

- AUD 50 million (approx. $32 million);
- three times the value of any benefit obtained through the misuse of information; or
- if the value of the benefit cannot be determined, 30% of an organization's domestic turn over in the relevant period.

The Amending Act fast-tracked a number of aspects from the Australian Government's Privacy Act Review, undertaken during the previous two years. Australia is currently waiting to see what further proposals from the Privacy Act Review will be implemented by the Australian Government.

Privacy Act review

On February 16, 2023, the Attorney-General's Department published the Privacy Act Review: Report 2022 (the Report). The Report is the final product of the Attorney-General's Department wide-ranging two year consultation and review of the Privacy Act. The review considered whether the Privacy Act and its enforcement mechanisms are fit for purpose in an online environment and digital economy. The Report contains 116 proposals aimed at strengthening the protection of personal information, the control individuals have over their information, and to better align Australian privacy laws with global standards.

The Report's proposals address a wide range of themes and issues, with some notable changes including enhancing privacy protections, removing a number of longstanding exemptions, regulating de-identified information, introducing a higher standard of privacy protection to be 'fair and reasonable,' and introducing a direct right of action for privacy breaches.

Significantly, the Report proposes the removal of the small business exemption and employee records exemption from the Privacy Act. These exemptions are a unique feature of Australian privacy laws. In most cases, organizations with an annual turnover of up to $3 million do not have to comply with the Privacy Act. Likewise, organizations do not have to comply with the Privacy Act when engaging in an act or practice directly related to a current or former employment relationship between an employer and employee and the employment record held by the organization relating to the employee. These exemptions are one of a number of reasons why Australia has not received an adequacy decision by the European Commission under the EU's General Data Protection Regulation (GDPR).

The next evolution of Australian privacy laws is on the horizon and the wide-reaching changes are anticipated to soon become law, potentially by the end of 2023

If the Australian Government adopts all, or the majority, of the proposals set out in the Report, this will represent the most fundamental change to Australian privacy laws since the introduction of the Privacy Act in the 1980s. In some cases, the proposed changes will place Australia's privacy laws above the standards required under the widely regarded 'gold star' standards of the GDPR.

Organizations doing business in Australia or with Australians will need to significantly change their data collection and handling practices if the major Privacy Act Review proposals are adopted.

Multi regulator environment

Adding to an increasingly complex privacy landscape, organizations

conducting business in Australia must also deal with a multi-regulator environment. Organizations and boards will need to prioritize privacy, data protection, and cybersecurity and resilience, or otherwise risk facing regulatory scrutiny from multiple angles.

The OAIC, ACMA, Australian Competition and Consumer Commission (ACCC), Australian Securities and Investment Commission (ASIC), and the Australian Prudential Regulation Authority (APRA), each have a keen interest in organizations' privacy, data protection, and cybersecurity compliance practices in Australia.

Each regulator brings a slightly different lens to privacy, data protection, and cyber issues. All regulators have a range of enforcement tools to monitor and enforce compliance with privacy and related laws.

It is evident that Australian regulators are stepping up and signaling a willingness to scrutinize organizations' privacy, data protection, and cyber practices like never before. Regulators will take action to enforce compliance, if necessary, given the heightened cyber risk and data breach environment we face in Australia and globally.

In a recent speech, ASIC Chair, Joe Longo, stated:

For all boards, cyber security and cyber resilience have got to be top priorities. If boards do not give cyber security and cyber resilience sufficient priority, this creates foreseeable risk of harm to the company and thereby exposes the directors to potential enforcement action by ASIC based on the directors not acting with reasonable care and diligence[1].

ASIC's stricter enforcement approach is a clear warning to corporate Australia that cybersecurity must be a board priority, and a failure by company directors to take cybersecurity seriously will invite regulatory scrutiny.

Organizations and boards will need to prioritize privacy, data protection, and cybersecurity and resilience, or otherwise risk facing regulatory scrutiny from multiple angles

Cybersecurity is increasingly referred to as a foreseeable risk of harm to a company and its stakeholders, from its employees to its customers and supply chain. The failure of a company's cyber risk management framework to adequately cover risk could be in breach of a director's duty of reasonable care. Boards must view cyber risk as any other risk in the business, such as workplace health and safety, and must take reasonable steps to mitigate risk that are practical and proportionate to the business.

The Australian Information Commissioner also recently renewed calls for organizations to prioritize privacy and data security practices. Upon the release of the OAIC's latest Notifiable Data Breaches Report, the Information Commissioner stated the "OAIC expects organizations to have robust and proactive procedures in place to protect the personal information they hold"[2].

Privacy and cybersecurity is undoubtedly a governance issue. If something goes wrong, boards should be in a position to demonstrate the reasonable steps they took to prepare and manage privacy and cyber risk. Otherwise, affected individuals will allege breaches of duties and regulators will have a less sympathetic ear for those boards that do not have a privacy and data governance framework in place to manage and protect personal information.

What lies ahead

The Australian privacy and data protection landscape is complex. Existing laws create a tapestry of laws that continues to evolve over time. The next evolution of Australian privacy laws is on the horizon and the wide-reaching changes are anticipated to soon become law, potentially by the end of 2023. All organizations that collect personal information as part of their business practices in Australia need to be on high alert and start preparing for impending changes to the Privacy Act.

In an environment of vast and onerous privacy law changes, heightened regulatory oversight and scrutiny, and ever-evolving cyber threats, effective privacy and data governance is now non-negotiable. If staying on top of changes to the Privacy Act is not a key priority for all organizations operating in Australia and if this does not form part of all organizations' privacy governance practices in the second half of 2023, regulators are unlikely to show leniency or restraint in the exercise of their enforcement powers. It would be wise to take stock and start a privacy uplift program now.

1. *Address by ASIC Chair Joe Longo at the Australian Financial Review Cyber Summit, September 18, 2023, Marconi's illusion: What a 120-year-old magician's trick can teach us about cyber preparedness (published 18 September 2023), see: https://asic.gov.au/about-asic/news-centre/speeches/marconi-s-illusion-what-a-120-year-old-magician-s-trick-can-teach-us-about-cyber-preparedness#!page=1&type=speeches*
2. *OAIC, Ongoing vigilance in data protection measures essential, (published 5 September 2023), see: https://www.oaic.gov.au/newsroom/ongoing-vigilance-in-data-protection-measures-essential*

GUIDE

AI Playbook

Understand your obligations and harness the power of artificial intelligence

Get to know global AI regulations

Empower AI system developers

Ensure responsible AI adoption

Get the guide

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Want to raise the bar? Don't trivialize employee engagement

Based in Copenhagen, Tim Clements is Business Owner of Purpose and Means. As a consultant assisting data protection leaders align their programs with business goals and strategies, an Official Training Partner of the IAPP, and a member of IAPP's Faculty, Tim shares his insights and experiences in building a data protection employee engagement program.

Data protection is all about people. Personal data - data about people - an extremely broad concept where context and timing are often critical. To truly work with data protection, understanding this fundamental concept is essential. In my experience, companies often pay lip service to explaining the complexities of 'personal data' - more on this later.

Data protection is all about people - the employees in your company. The people who you as a Data Protection Leader need to rely on to live up to principles and expectations which are articulated in your data protection policies.

This duality requires greater focus than many companies currently provide and by investigating time and effort, the compliance bar can be raised. It's about making data protection living and breathing in the functions, departments across the company, especially where core processing of personal data is taking place.

Data protection is a team sport

Data protection should not be solely the preserve of a legal or compliance department. For a start, those departments often come under 'corporate functions' which to some employees represent 'overhead' or 'not where business value is generated.'

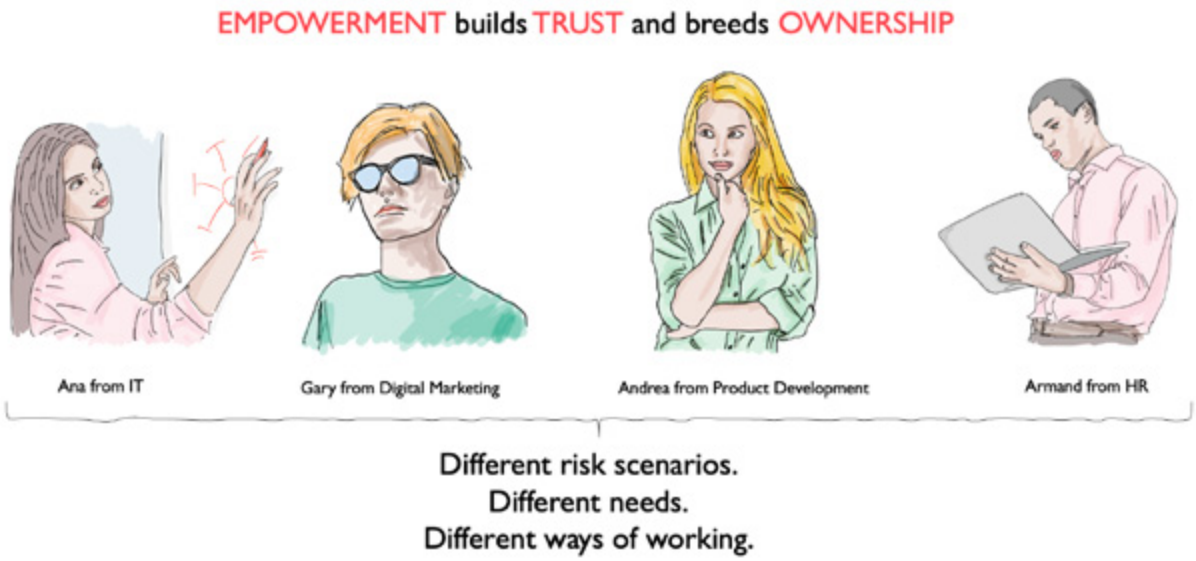


Image: Purpose and Means

Also, these departments traditionally do not have large budgets, which means data protection efforts may be limited. If you want to see where the budgets are large in many companies, look at where the technology is deployed. For example, digital marketing, the digital platform, business development, etc.

Data protection must therefore disseminate itself across the company recognising that a multitude of competences have important roles to play in any data protection team.

Using a football analogy, if data protection is treated solely as a legal issue, you'll be fielding a team of goalkeepers; you'll defend your goal with all your might, but you probably won't score many goals. So, just like any team sport, data protection requires difference competences on the field.

The potential is enormous

Employee engagement is still an area I often see trivialised. There are various levels of engagement. Unfortunately, rolling out generic eLearning across the company is common, with an intention of ticking a box rather than embedding competences and knowledge.

Generic eLearning is problematic, as is any generic education and training. If the material is not aligned with your organisational policies and procedures, it can be counter-productive; employees become confused, disinterested and certainly no wiser.

So where to begin to address this important issue, because the potential to improve employee engagement is huge.

And for the sake of clarity, when I mention employees, I also include management and leadership as these are two extremely important groups you need to engage with in different ways than your average employee.

Policies are a good place to start, but...

Data protection policies are a good starting point, assuming they have been written in a proper way. And what do I mean by 'proper way'?

Data protection policies exist in your company among a raft of other policies, e.g. finance policies, HR policies, IT policies, etc.

When talking 'policies', we must always remember the target audience - your employees. Unfortunately, some policy writers forget this, especially in data protection, by writing them in a language the average employee finds difficult to understand i.e. legalese, with many abstract terms and concepts included.

If your company has engaged with a third party to write your policies – which could be an external law form or consultancy - you may have experienced this problem, especially if they have not invested time in understanding the business context, reviewing existing policies and talking with other policy owners across the company.

As mentioned, data protection does not exist in isolation, and should not.

A key task before drafting policies is to identify existing policies that are related or potentially overlapping. This 'harmonization' exercise is critical. It will help avoid potential conflicts between a statement in a data protection policy and a statement in say, an IT policy. Your policy says one thing, and the IT policy says another.

Another harmonization consideration is overlapping content. You'll end up wasting your employee's precious time if you are duplicating statements across policies. Harmonization is a must-do activity.

Also, applying the business context is vital. Employees will not see themselves in the policies if they are generic and lack the context of your company.

Writing, maintaining, and ownership of data protections policies really should be an internal task. If you are about to refresh a set of policies created a few years ago by an external company, consider keeping things internal this time round.

Distinguishing stakeholder groups

Once you have your policies written in a proper manner that reflect what data protection is to your organization and include all the required statements in relation to the applicable laws and regulations, then you need to determine the method you'll disseminate the policies to the various groups of employees.

Just circulating a link to the policies on your policy portal is not sufficient. Even though you may point to a clause in your employees' employment contracts along the lines of "employees are expected to read and understand all company policies..." we need to help employees with this - help them live up to this expectation.

Some departments may see this task easier than others. In a legal or compliance department, it's probably a given that employees will carry out this task, without question.

In a UI/UX team, or a team in digital marketing, the situation will be far different.

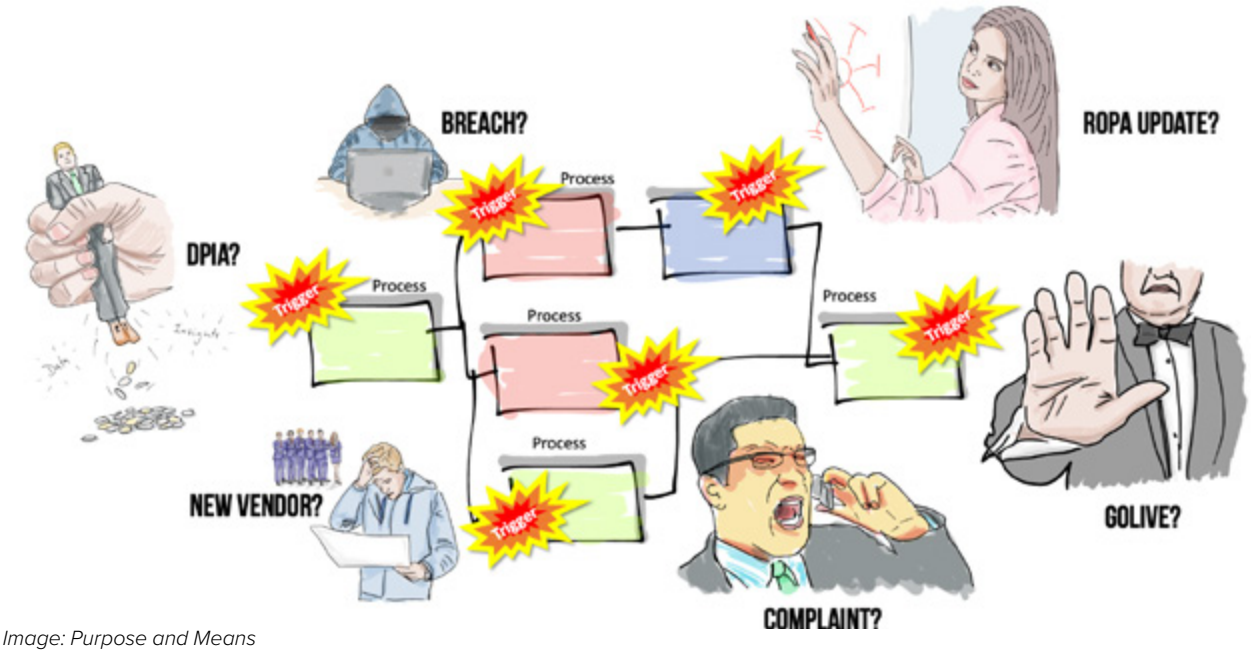


Image: Purpose and Means

If you are looking to engage with employees across your company it can be useful to take a walk around your buildings one day. Wander around the different functions and departments in your company and observe.

Observe the differences in ages, perhaps nationalities, look at how people dress, their jewellery, their tattoos, nose rings etc. Although you may be aware of your 'company culture', we're talking sub-cultures here. These will be typically informal, and slightly below the surface but are extremely useful in understanding to determine your own employee engagement strategy.

The approach you need to use to effectively engage with your colleagues in the HR or finance department will probably vary to those in the digital marketing team. For example, finance often are fine following detailed procedures, whereas your digital marketing colleagues may be motivated by colourful, highly visual one-pagers. To effectively engage with your employees, you need to meet them where they are, rather than they meet you on your terms.

A key task therefore is to map out all stakeholder groups - remember to include your leadership and management - and to determine their engagement and information needs and the approach you'll take. Education, training, awareness, briefings, etc., taking into account any cultural nuances - simply asking different teams about their own contextual - and accepted - ways of working will reveal some valuable insights for you.

Empowerment builds trust and breeds ownership

If you want to take things to another level, consider empowering employees to develop their own procedures or ways of working. You'll need to provide them with some basic data protection education about fundamental concepts and work with them to ensure they link them to their context.

Educate them in basic risk management, ensuring they fully understand the difference between 'risks to the fundamental rights and freedoms of individuals' and 'compliance risks' by providing lots of examples of real-life incidents involving problematic processing or unintended consequences of processing.

Facilitate the discussions about the risks they see in their processing context and help identify the measures needed to treat the risks.

The teams then need to document their own ways of working and once they have done that, they are more likely to take ownership of something they've created themselves. Once you reach this point, there's a strong chance they'll also maintain the documents, educate, and train their colleagues, new employees and so on. This will take away pressure from you and ultimately reduce the number of data protection issues that get forwarded to you by default because you represent 'data protection.'

The result of this will be data protection considerations embedded deep into the 'processing engine rooms' of your company.

Realistically, this is where the responsibilities and considerations must belong. This is where the contextual processing knowledge and expertise resides.

How can a Data Protection Leader understand the ins and outs of all applicable laws and regulations, manage the data protection programme of work, and have a deep knowledge of all processing scenarios?

Delegation and empowerment will help spread responsibilities.

Yes, this approach will more time and will effort in the short term, but if you intend to stay in your role for a while, you'll see the longer-term benefits.

The importance of 'operational triggers'

Once you have disseminated your policies into ways of working, or procedures, work instructions or whatever you call it in your company, you can't expect employees to remember everything.

Again, you may think that you've informed employees that they need to remember to request the ROPA be updated, or they need to consider a DPIA at the start of a project. You may think it mentioned this in the education you've made for them. But employees are humans and just like us, we often forget things.

One approach to ensure important considerations are not forgotten is to embed triggers in the operational process and procedures of your company. Typically, the processes and operational procedures will be owned by somebody outside of the data protection team. It could someone in IT or technology who is responsible for an IT change management process, or a release management process. It could be the person responsible for portfolio management,

or someone else responsible for the business case process.

To embed your data protection trigger (or control) you'll need to engage with the relevant process owner, explain the scenario and risk and then agree the work that is required. Don't underestimate this task. It can take time to update process documentation, as well as communication and education activities - this will be typically the responsibility of the process owner.

Re-framing data protection

A key element of an engagement strategy is the perception of 'data protection' itself. If you don't actively frame this in the right way, employees will make up their own minds about the importance of your role - adding value or getting in the way. If you've framed data protection around 'avoiding fines and penalties' or 'to be compliant' that's not always the phrase that will resonate with, say a CMO or a data scientist.

Again, there's a huge opportunity to frame data protection beyond 'compliance' and once adopted should underpin all engagement activities you have with employees. This can be as simple as a short statement/ slogan in your email signature, to ensuring all presentations have one slide that mentions your statement - and ensure that all your decision making, and engagement reflects this.

You're competing for the attention of employees

Consider twisting the perception of data protection in your materials - get inspired by how companies project their brands to get your attention. Remember, employees are inundated with messages from across your company. You are competing for their attention with your peers. You need to devise ways that will make your messages and materials unmissable and eye-catching. If not, all the effort you make in writing the material may be a complete waste of your time if nobody reads it.

How can you make your engagement stand out, and memorable? How will you present at the next Town Hall? What will you say at the next department meeting? What about the poster campaign for the Data Protection Day event? The All Hands meeting? There's no easy answer, but if you start thinking along the lines of 'being different', you'll be putting yourself at an advantage compared with your peers who'll continue to dish out the same old material!

Your engagement roadmap

A useful group to build relations within your company are your internal communication colleagues. Often, they can provide you with an overview of various communication channels and tools that you may be able to get access to.

This will help you ensure that you're not just relying on employees seeing your emails, or posts on the company's intranet.

Once you have your policies and other content, and you have your stakeholder groups identified and their information, education, and training needs, then you can start putting together your engagement roadmap.

Your roadmap should outline a cadence of engagement activities. Employee engagement is like a ball - to need to make it bounce and keep it bouncing to keep people engaged and build passion for data protection. Make the activities varied and often.

Once the ball stops bouncing, it loses momentum and that's something you must avoid in your work.

Personal data

As mentioned at the beginning of this article, in my experience, companies often pay lip service to explaining the complexities of 'personal data' yet it is a huge opportunity to get employees interested and passionate about data protection.

When engaging with employees, I sometimes prefer to talk 'data about people' using lots of examples that articulate the broadness, complex and contextual nature of this term, especially when things go wrong. And I'm thinking more about unintended consequences of processing and unintended use cases, rather than data breaches.

If in your work, you recite the GDPR definition and give a few examples of identifiers like name, email, government issued ID, postcode, etc., then there's great potential for you to exploit the fact that all employees will be able to relate to their own personal context outside of work and use lots of 'what if' examples with themselves, their family and friends.

Also, if employees do not fully understand the complexities of personal data, then it will be very difficult for you to lift your work in say, building a ROPA, considering DPIAs and so on. I see the root cause of poor quality DPIAs is often as a result of employees not understanding this highly important term.

Once employees are comfortable with the term and can use their imagination in various processing contexts then you're on the road to spreading passion about data protection.

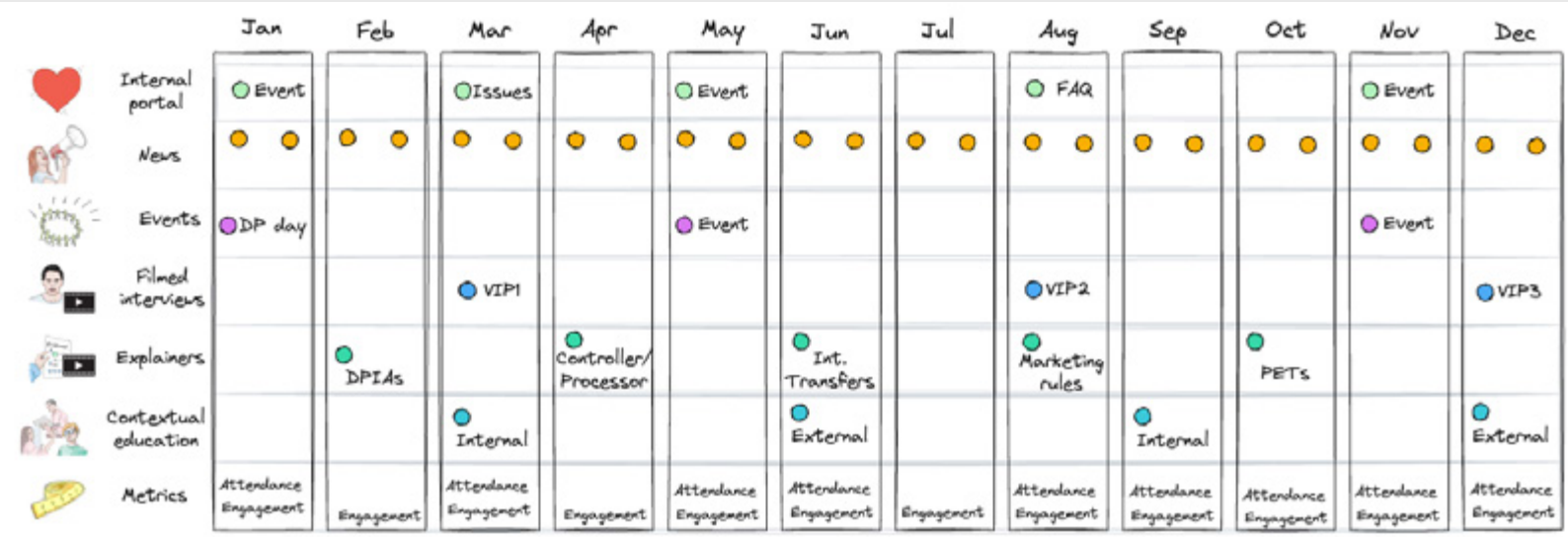
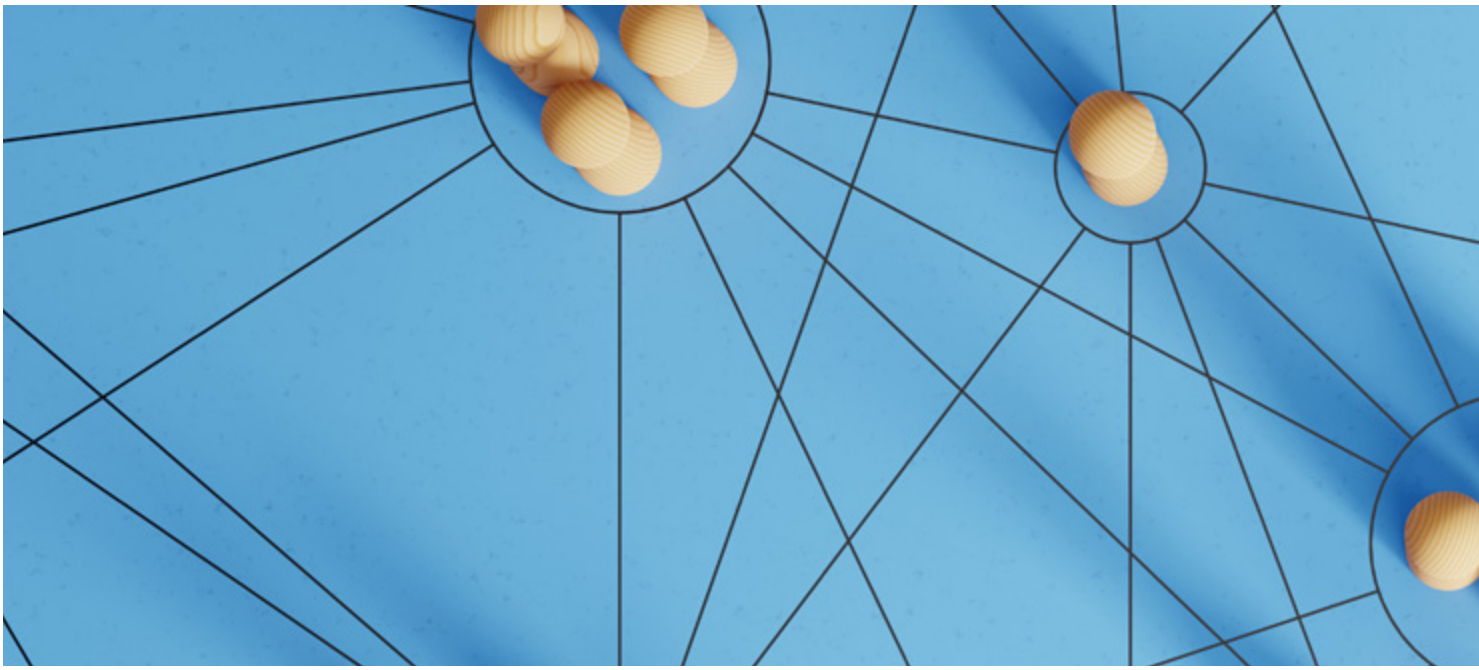


Image: Purpose and Means



International: Does your organization need a Trust Office?

Andrew Clearwater Chief Trust Architect
aclearwater@onetrust.com

Instead of 'business as usual,' organizations should focus on building trustworthy products through processes and people

Trust isn't just about doing what's required, but doing what's right.

But who defines what is “right” when it comes to your business? What is the north star guiding your organization's decision making?

For us at OneTrust, it was an organic progression born from our need to manage risk in our privacy and security functions. While the company was founded in 2016, we weren't able to immediately sit down and say ‘this is what Trust means to us, and here's how we're going to pursue it.'

How'd we get here?

We set out to build software that would help companies around the globe follow and adhere to appropriate privacy regulations for their specific industry and geographic locations. As we grew, however, it was imperative we implement and adhere to specific frameworks for our own privacy and security programs.

So OneTrust began earnestly building its Trust Office by pulling in the proper stakeholders who could lead this charge. While I currently serve as the Chief Trust Architect, I started my OneTrust career as the Director of Privacy. I worked alongside our then-VP of security and members of our legal team to create an Integrated Management System (IMS) committee that could take on such a large initiative.

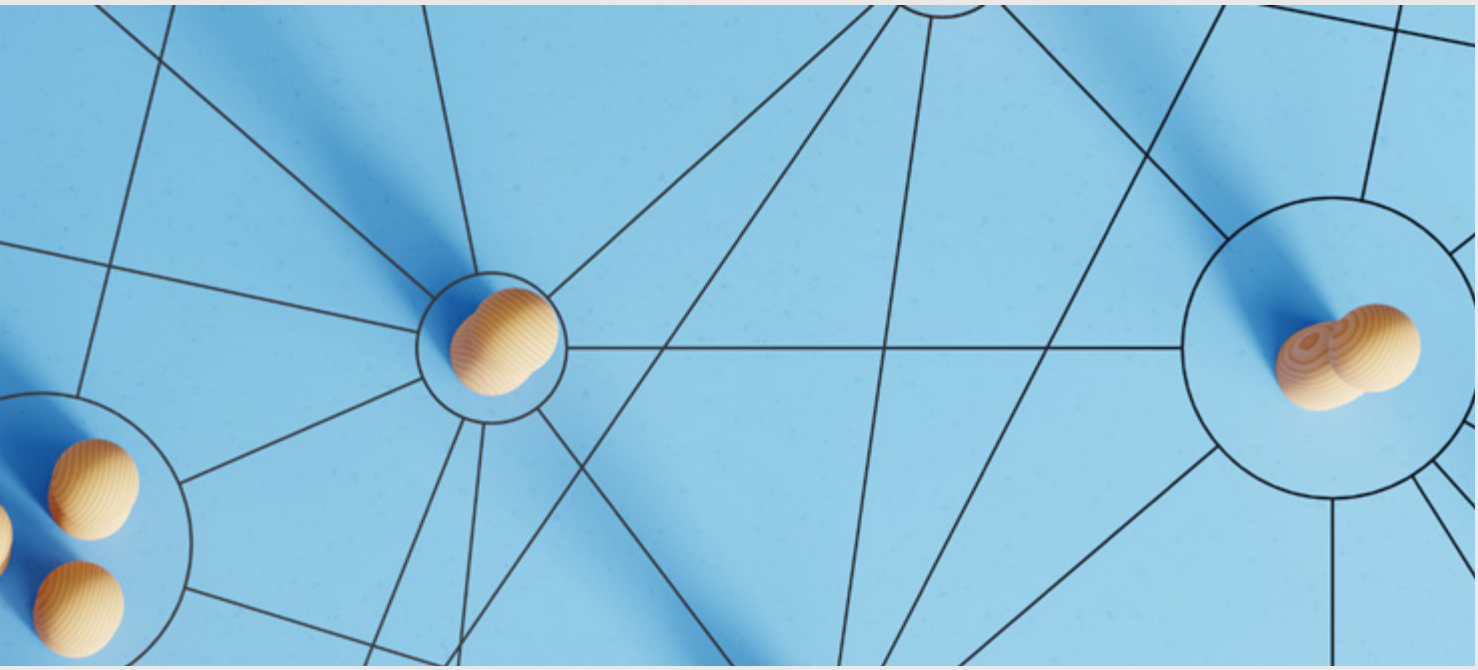
The focus of the committee was to adopt and implement a security framework, with our first audits being carried out against our security controls leveraging ISO 27001 and SOC 2. We soon followed this with ISO 27701 to ensure we managed the processing of personal data appropriately.

As we grew, so did our program implementation in other lines of business, like Ethics & Compliance, as well as Environmental, Social, and Governance (ESG). And this is where that evolution into a trust-based business really presented itself: as we took the proper steps to do what is not just required, but what is right, we built out that same scope of opportunity for our customers through the Trust Intelligence Platform.

If we were going to embark on this journey, why wouldn't we do the same with our customers? What they were looking to accomplish wasn't just a compliance-driven effort. They also wanted to build programs focused on trust and transparency with their employees, customers, partners, and community.

5 building blocks to create a Trust Office

The old saying "easier said than done" rings true here, I know. A couple hundred words about what our company did to begin



the journey to being a trust-based business pales in comparison to the actual time, resourcing, and effort that went into the change. But what I can do is offer five building blocks that could help start this necessary shift.

1. **Evaluate**: As with any business decision, you have to evaluate the situation and determine if there's a reason for the function. In this case, you're asking a question at the macro level: does my organization need a trust office? From there, evaluate the business as a whole and what trust means to your people, processes, and products.

2. **Enable**: Who's in charge of this new undertaking? Create the role(s) and ensure the person or committee taking this on will be enabled with support from the board room and C-suite. Once this is established, communicate this out to both employees and customers that your organization is taking this charge seriously and looking to begin the process.

3. **Develop**: What is the operating model going to look like? What resources are needed to make this happen, and what's the starting point for that? As I mentioned earlier, it was OneTrust's need to adopt integrated management systems driven by ISO standards that then created our desire to build a platform that could do the same for our customers.

4. **Establish**: Now it's time for goal setting. Start small and look at a single year. What are the cross functional aspects that can be determined, and how are those met? What 'wins' are most important in this year-one ramp-up? Determining those benchmarks will create needed landmarks along the way.

5. **Create**: Finally, how can we measure this? As with any business initiative, it needs to be tracked. Beware, however. Don't treat this like run-of-the-mill data gathering, i.e., number of security incidents or other firmographic metrics. Ideally this will be measured in the same way a customer satisfaction rating would be: What's working, what's not, how can improvements be made and redundancies removed? Do our people believe our products and processes exude trust?

Who's doing what?

Using the five building blocks as a guide — and obviously adaptable to whatever your business feels is the best way forward — our Trust Office took shape by collaborating with the following stakeholders and departments who could lend their expertise and insights to this always-on initiative. We created Centers of Excellence (CoE) across specific domains we learned are important to our customers, including:

- **Privacy**: Led by our Data Protection Officer
- **Security**: Led by our Chief Information Security Officer
- **Ethics & Compliance & ESG**: Led by our Chief Ethics & Compliance Officer

Each Center of Excellence brings together a cross-functional group of experts in their domain to:

- Be the expert in their field to help guide our product, marketing, sales, and support teams as we advise our thousands of global customers on their own programs
- Serve the community by sharing resources and best practices on their industry and domain
- Build the best trust program internally using the OneTrust platform

What's the benefit?

The headline of this piece is "Does your organization need a Trust Office?" but it could have been "Why your organization needs a Trust Office." We're biased, of course, but know there's true value in establishing such a program in your organization.

Company leadership is on the hook for serving two stakeholders: employees and customers. Both of whom, of course, deserve honesty and transparency from the brand they're trusting to work with. Our customers helped us understand the deep need to establish a Trust Office, and it's our responsibility to leverage our own Trust Intelligence Platform and uphold the tenets that make us a trust-based business.

And while it seems daunting to embark on such a program — one that will certainly look different for you than it does for us — we can only say that it's a worthwhile investment of time and energy.

Just keep in mind, there is no finish line or final destination on the journey to trust; it's ever-moving and adaptable. Safe travels!

5 MINUTES WITH...

Jordan Crenshaw

Jordan Crenshaw is the Senior Vice President at the U.S. Chamber of Commerce's Technology Engagement Center (C_TEC), where he leads the day-to-day operations of the policy team. Crenshaw also manages the Chamber's privacy working group, which is comprised of nearly 300 companies and trade associations, and is responsible for developing model privacy legislation and principles. Prior to his role at C_TEC, Crenshaw led the Chamber's Telecommunications and E-Commerce Policy Committee, which analyzed federal privacy, cloud computing, broadband, internet, e-commerce, and broadcast policies that impact U.S. businesses. Before joining the Chamber, Crenshaw was an attorney focused on environmental issues and consumer privacy laws. Crenshaw also worked at McGuireWoods, LLP assisting discovery issues for environmental nuisance, TCPA, and other civil litigation. Crenshaw also held roles in the Virginia Senate leadership, the Office of the Attorney General of Virginia, the U.S. Department of Labor Office of Administrative Law Judges, and the National Right to Work Defense Foundation. Crenshaw earned both his undergraduate degree and Juris Doctor from the College of William and Mary. He is licensed to practice law in Virginia and is a Certified Information Privacy Professional (CIPP/US). He, his wife, Molly, and daughter, Charlotte, live in Virginia.

Tell us a bit about your job role and how you have progressed in your career?
I lead the U.S. Chamber of Commerce's Technology Engagement Center, which is the technology policy hub of the organization. The Chamber is the world's largest business federation. Day-to-day, I oversee a team of policy experts who emphasize technology's role in our economy and advocate for rational policy solutions that drive economic growth, spur innovation, and create jobs. The team works across several major issues and emerging technologies including AI, privacy, broadband, drones, and automated vehicles. I accidentally fell into privacy and technology, getting my start in environmental and labor law. In previous roles, I worked on privacy issues and when I saw an opening at the Chamber to be the lead on telecom and data protection issues, I jumped at it. It is an exciting field that will only get more complex and interesting in the years ahead.

What alternative job would you have if you had not gone into law?
If I could do anything outside the law, I would relish the chance to be a novelist or travel writer. Luckily, my career has enabled me to do some degree of both. I get to be a storyteller highlighting the truth of how technology, like AI, is a force of good for the economy and society - even helping small business owners compete with larger entities. My role at the Chamber has also enabled me to see the world - from traveling to London to hold listening sessions on AI policy and South Korea to talk about automation and the law, to visiting all the great state and local chambers of commerce that are the backbone of the U.S. economy.

What do you love about your job, and what do you find challenging?
No day is ever the same. This is both the best and most challenging part of the job. One day I have the opportunity to testify in front of Congress on a hot issue like AI, the next, I am somewhere on the other side of the country with the owner of a coffee shop talking with him about how digital advertising saved his business during COVID. At the same time, news cycles change, businesses have fluid needs, and policymakers may reprioritize issues that require our engagement.

Where is your favorite place on earth?
Anywhere I can be outside, there is good food, or get great shots of the Milky Way with my camera. The American Southwest, Montana, Big Sur, the Florida Panhandle, Spain, and Fenway Park are a few.

Who would play you in a film about your life?
I am a big fan of the first three Indiana Jones and Star Wars movies, as well as the Tom Clancy books, so I'd be honored for it to be Harrison Ford. I will have to settle for a deepfake version of me for now.

What is your favorite book?
Fiction-wise, A Time to Kill. Although in life there are moral truths and most things are black and white, I really enjoyed how the story dove into life's gray areas. My favorite line from the book is when the attorney-protagonist's mentor tells him before a big case, "If you win this case, justice will prevail, and if you lose, justice will also prevail. Now that is a strange case." I sometimes worry we, as a society, have lost the sense of nuance in today's discourse. Sometimes, people can be both right and wrong on a given issue at the same time.

What is some advice you would give to others starting off in your industry?
Test things. Never assume what people are saying in the public square, social media, or on TV is the full story. Investigate things for yourself. Poke holes in legislation and the arguments in a case. Sometimes you will find the legal and policy flaws that others have not, and your clients and members will thank you.

Who is your inspiration?
I have to answer 'who' in the plural. My wife for working both a full-time job and taking care of our daughter when I'm away and making me strive to be the best version of myself. My mom for constantly praying, looking out for, and leading me to my faith. My dad for being a diligent worker as a pilot in the aviation industry for decades. And my eight-month-old daughter, Charlotte, who motivates me to get up in the morning (literally and figuratively).

Interested in Becoming a **OneTrust DataGuidance** Contributor?

Partner with the world's most widely used technology platform to manage privacy, security, and data governance and help organizations be more trusted. Law firms around the world partner with OneTrust DataGuidance because we are committed to and invested in their success.

INDUSTRY EXPERTISE

- Market leader in regulatory intelligence
- Over 20 years' working with Contributors

THOUGHT LEADERSHIP

- Experts in over 300 jurisdictions
- Recognized thought leaders in privacy, security and governance

NO FINANCIAL TIES

- No financial obligations for partnering
- Exclusive discounts to OneTrust DataGuidance

GLOBAL AUDIENCE

- Global customer base
- 1,600 customers

CRITICAL COMPLIANCE TOPICS

- Key privacy and security areas covered
- Ever-growing and changing product to adapt to market need

SUPPORT

- Dedicated Relationship Management Team
- Dedicated Representative support
- Ongoing Partner Collaboration & Resources

Send Your Submissions to: contribute@onetrust.com

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE