WRANGU

What to Expect for Privacy and Data Protection in 2023

By Wrangu

www.wrangu.com

Table of Contents

As we enter 2023 data protection and privacy show no signs of slowing their momentum. Requirements, driven by customer dollars, are getting more complex, technology continues to develop at an incredible rate and regulation shows no sign of becoming easier! So, what are the headlines for 2023?

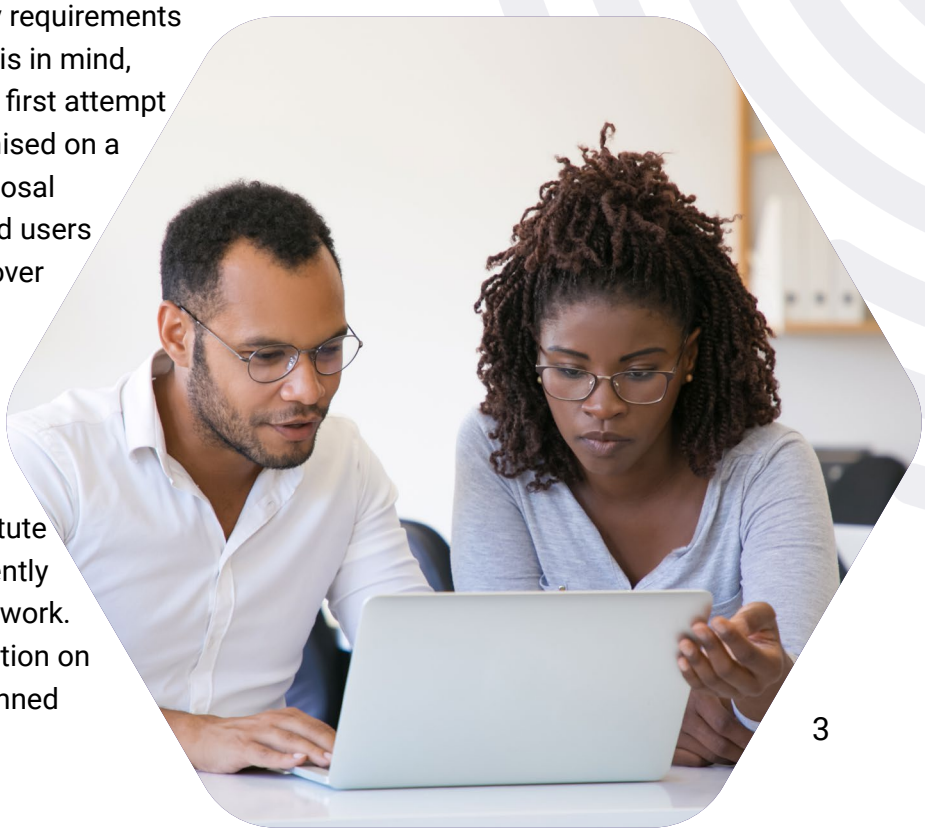
This year has already seen renewed interest in the possibilities of Artificial Intelligence (AI) with excitement around ChatGPT. What implications does AI have for privacy and data protection? Customers, employees, and regulators are driving requirements for sustainable and socially acceptable products and services forcing a transition for most companies sourcing models. The UK will debate whether GDPR should be replaced. Adequacy decisions are being debated with a focus on whether changes enacted by the United States will satisfy the Court of Justice. Expect new state laws in the United States (and a federal law?) along with improved coordination of enforcement efforts in the EU. Let us tackle them one at a time.

Artificial Intelligence

Artificial intelligence has captured the popular imagination for some time but re-exploded with the development of Dall-E, generating digital images from natural language descriptions, and more recently ChatGPT. Concerns over ChatGPT and its consequences have been debated widely, but its popularity is undeniable despite questions over what implications AI might have for privacy and related rights such as autonomy, dignity, jobs, and schooling.

The fundamental issues are well known with particular focus on biased data sets where the data itself is not neutral, fair, or equitable and reflects societal biases creating AI that does the same. Expanded use of AI also creates Due Process issues where machines are making decisions about criminal sentencing, loans, financing for business, scoring for tests, admissions for college and many more areas of an individual's life. This raises questions around recourse and what should it be? Should there be transparent information around judging criteria? Can decisions be appealed and if so to who? Can you appeal a decision before a human judge and is that necessarily better?

AI creates a lot of data protection and privacy questions, but it also has the potential to generate extraordinary benefits, from providing better health care to helping manage climate change. There is always going to be a balance between regulatory requirements and delivered benefits to iron out. With this in mind, the European Union is in the process of a first attempt to establish a regulatory framework premised on a risk-based approach. The regulatory proposal aims to provide developers, deployers and users with clear requirements and obligations over using AI. Regulation of AI is not just happening in Europe. Around the world, countries are acting. Last year the White House published an AI Bill of Rights, China is developing regulations around algorithms, and the National Institute of Standards and Technology (NIST) recently published an AI Risk Management Framework. The UK is also planning a public consultation on its AI National Strategy and there is a planned government whitepaper forthcoming.



Sustainable and Socially Acceptable Products and Services

The response to ESG signals a maturing industry that is looking to regulators to establish standardized metrics and make good on its claims of sustainability. There is an increasing compliance need to gather data and produce reports documenting initiatives arising from new regulations. These requirements provide transparency for all an organization's stakeholders: from the traditional focus on investors and shareholders to include the wider group of employees, consumers, and local communities.

These initiatives are driven by organizations that recognize their role in local communities coupled to the global challenge of climate change. It is also driven by concerns to uphold human rights like privacy and data protection, the right to work and receive fair wages, and diversity initiatives to create a more equitable world. What follows is a brief forecast of the legislative and regulatory landscape.

Upcoming Legislation

Women on Boards Directive

Like most regulatory initiatives, the European Union is leading the way. A decade after the "Women on Boards" Directive was first proposed, the EU Commission adopted it in November 2022 with the aim of improving the gender balance on boards of publicly listed companies. The Directive requires at least 40% of non-executive director positions or 33% of all director positions are held by women by 30 June 2026.

> The Directive requires at least **33%** of all director positions are held by women by 30 June 2026

European Commission's Corporate Sustainability Reporting Directive (CSRD)

In December 2022, the CSRD came into force. The CSRD builds on the prior Non-Financial Reporting Directive (NFRD) extending the scope of covered entities to large companies incorporated in the EU and non-EU incorporated companies that do significant business in the EU. The change will reportedly increase covered entities from approximately 11,000 to 49,000. The CSRD amends and updates the NFRD as well as expanding reporting requirements and specifying both the disclosure format and standards that companies must use. Under the CSRD, organizations must include a dedicated section in their management report covering their impact on sustainability matters as well as the role sustainability plays in the organizations decision making. This information must cover both the organization's own operations as well as its extended value. The CSRD has an extended role out period with the first set of companies already covered by NFRD needing to comply by 1 January 2024.

German Supply Chain Due Diligence Act (SCDDA)

Emphasis on value and supply chains is also taking effect in local member state laws. The most notable is the German SCDDA, which came into effect 1 January 2023. This law covers both environmental and Human Rights impacts throughout an organization's supply chain and applies to both large German and non-German organizations.

The scope of the law is notably broad requiring organizations take a risk-based approach to managing due diligence in its own business practices as well as its direct and indirect suppliers. There is also the requirement to designate a responsible individual like a Human Rights Officer with direct access to the highest levels of an organization. Beyond risk management, there are extensive reporting and documentation requirements creating transparency around operations. The importance of the German law is the broad scope of issues it is intended to address and its basis as the model for the broader EU Directive on Corporate Sustainability Due Diligence expected to be approved in early 2023.

Carbon Border Adjustment Mechanism (CBAM)

Also in December last year, a political agreement was reached on the implementation of CBAM, also known as the carbon border tax. The policy targets the practice of shifting carbon intensive production outside of the EU to countries with less stringent requirements on climate policy. The CBAM adds a cost on embedded carbon emissions generated in the production of certain imports like cement, iron, and fertilisers. The initiative will take place of transitional period beginning in October 2023 where importers will be required to report carbon emissions - though not yet pay a tax on them - with the permanent system phased in during 2026.

Environmental, Social, and Governance (ESG)

In the United States, ESG disclosures remain a voluntary practice undertaken by many companies responding to demand from investors and other stakeholders including customers. The Securities and Exchange Commission recognized the ambiguity that has emerged in documentation and reporting standards and set an ambitious agenda to establish mandatory reporting requirements. In 2022, the agency proposed for public comment a list of requirements related to climate change disclosures and hopes to approve final rules by April 2023. The SEC also indicated an intention to propose a new comment period for disclosure requirements related to Diversity, Equity, and Inclusion.

European Union

The European Union is the regulatory king setting the data protection agenda for the rest of the world. Top of mind is the European Data Strategy and the publication of a suite of complementary regulations. The EU Commission also published a draft adequacy decision for the United States. A major update that will affect an economic relationship valued at $7 trillion.

A major update that will affect an economic relationship valued at **$7 trillion**.

EU-US Data Privacy Framework

In October, the White House released an Executive Order paving the way for the new EU-US Data Privacy Framework (DPF). The new framework includes three components: commercial data protection principles to which U.S. organizations can self-certify, the executive order, and Department of Justice regulations. (Interestingly the principles were originally negotiated while the GDPR was being finalized and still referenced the 1995 Data Protection Directive. Obviously, these references will be updated to refer to the GDPR.)

The executive order requires U.S. intelligence authorities to limit U.S. signals intelligence activities to what is necessary and proportionate adopting language from the Court of Justice's (CJEU) Schrems II decision and is the first of two prominent issues on which the CJEU found the Privacy Shield failed. The executive order is paired with Department of Justice (DOJ) regulations creating a new redress system, including a new Data Protection Review Court to process complaints over the legality of U.S. signals intelligence activities. This is the second core requirement of essential equivalence the CJEU found lacking under the Privacy Shield.

In December, the European Commission launched the process to adopt an adequacy decision to foster data transfers from the EU to the U.S. by publishing its draft adequacy decision. The draft will now go through the full adoption procedure. The European Data Protection Board will issue a non-binding opinion. The commission will then request approval of a committee composed of Member States representatives. Once the Member States approve the adequacy decision, the decision is formally adopted, with a final decision likely in the Spring.

Enforcement Actions

Until now, many have complained that the European Union is a legislative superpower with a weak enforcement record. In 2020, Access Now called the GDPR "a legislative success but an enforcement failure." Into the fifth year of the GDPR, supporters of the legislation and thousands who have filed complaints await to see their data protection rights materialize. There remains slow resolution of cross-border cases, differences in national procedures and practices, and underfunded national data protection authorities.

This message has now reached the institutional level. In May 2022, the European Data Protection Supervisor gathered thousands of experts to discuss a way forward on enforcement. This resulted in new requirements being mandated by the European Commission for supervisory authorities, in line with the launch of a new enforcement review plan to ensure adequate application of the EU General Data Protection Regulation. The European Commission will require all national data protection authorities to file "an overview of large-scale cross-border investigations under the GDPR" every two months which will provide a solid basis for overseeing the supervisory authorities' administration of their duties. This is a notable change and should mean that big cases that have laid dormant will see accelerated investigation and enforcement.

Digital Markets Act and Digital Services Act

The Digital Markets Act (DMA) and the Digital Services Act (DSA) were among the most significant pieces of legislation published last year. The focus is now on implementation for the so-called gatekeepers. These are the biggest tech companies, defined as having a market capitalization of €75 billion or annual turnover of €7.5 billion with 45 million monthly end users in the EU and 10,000+ annual business users. The law is intended to drive a more fair, open, and contestable market and provide for hefty fines in the case of a violation. Look for this going into effect this Summer.

DMA applying to companies with annual turnover of **€7.5 billion** with **45 million** monthly end users in the EU and 10,000+ annual business users.

The DSA provides rules for online intermediaries offering network infrastructure such as internet access providers, hosting services, and online platforms. Among a lengthy list of new obligations will include transparency reporting, risk management obligations, crises response, external auditing, and transparency for online advertising. In addition, there will be an outright ban on ads targeted to children.

Cyber Security Regulations

There has been a flurry of new laws introducing minimum security requirements and risk-based management. These laws tend to be sector specific meaning a lot of them must be passed and take effect. In September 2022, the European Commission proposed the Cyber Resilience Act designed to introduce minimum levels of security requirements for connected products, effectively regulating the market for the Internet of Things. The law is intended to prevent manufacturers from bringing products to market when they are aware of potential cyber-security vulnerabilities. This stems from the shocking example in 2017 of a German doll that could be easily hacked to speak to children. Still open is to what extent software components will be regulated on the law.

In 2023, NIS2 will replace the EU's existing cyber-security law, the NIS Directive. It applies to organizations across different sectors ensuring that networks and systems they use to deliver services and conduct their business maintain a high level of cyber-security. NIS2 will interplay with the Cyber Resilience Act setting out the cyber-security requirements. NIS2 entered into force January 16th and will apply from 2025.

The Digital Operational Resilience Act (DORA) is a new framework for management of digital risks in financial markets ensuring resilient operations in the financial sector seeking to avoid incidence of severe operational disruption from cyber security and information and communications technology. The law went into effect in January this year with an implementation period of two years applying from 2025.

Data Act

The Data Act is a big file on the EU policymakers' table likely to be finished this year. The Data Act is part of the overall European strategy for data complementing the Data Governance Regulation. The Data Act intends to create the conditions for a fair and innovative data economy with rules making it easier to use and access data generated in the EU across all economic sectors. The new law is divided into three main strands regulating how businesses and consumers can access data generated on local devices (i.e., cell phones and laptops), it empowers public bodies to obtain privately held data under certain conditions, and rules around interoperability making it easier for customers to switch between cloud service providers.

The intention of the Data Act is to ensure fairness in the digital environment, stimulate a competitive data market, and open opportunities for data-driven innovation by making data more accessible. To do this, end users are empowered to access and use their data for their own means as well as measures rebalancing negotiating power for small and medium sized enterprises (SMEs) to prevent abuse of contractual imbalances. Questions linger over whether some SMEs should be exempt, how to deal with trade secrets, and how data sharing will work.

ePrivacy Regulation

Discussions over the ePrivacy Regulation have been ongoing for years. Originally, it was intended to be published alongside the GDPR, however while the GDPR enforcement matures, the ePrivacy Regulation lingers in regulatory purgatory. Eventually, the ePrivacy Regulation will replace the ePrivacy Directive updating regulation of confidential electronic communications, some forms of metadata, spam, and cookies.

Under the previous Czech presidency of the EU, there were intense informal exchanges between the EU Commission and Parliament trying to push the regulation forward. Unfortunately, discussion hit an impasse when attention turned to law enforcement access for electronic communications and under what conditions. Member states want law enforcement access to be a rule while EU lawmakers prefer it as an exception. This is a long-standing grievance with no easy solutions.

United Kingdom

Digital, Culture, Media and Sport poised for new attempt at data protection reform

A crucial tenant of the post-Brexit National Data Strategy aimed at unlocking the value of data to secure "a pro-growth and trusted data regime" is the Data Protection and Digital Information Bill. The Bill was laid before the UK Parliament on 18 July 2022. The bill proposing amendments to various UK legislation including the UK's incorporation of the GDPR in domestic law (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003.

Due to changing administrations, the Bill's passage through the legislative process was paused in September 2022 to allow for further consideration balancing the UK's seemingly precarious adequacy decision. Work on the bill seems to again be gaining steam and consultation on the stalled bill is expected to begin soon.

US Adequacy Decision

Brexit entitled the UK to issue its in adequacy decisions and the UK and U.S. have been in ongoing discussions over the last two years. The test for adequacy under the UK GDPR requires a final decision from the Secretary of State that they are satisfied that UK data protection standards are not undermined when personal data is transferred to another country. In October 2022, the UK's Secretary of State highlighted progress being made by both countries toward a UK adequacy assessment.

When the UK left the EU there was concern that if the UK were granted an adequacy decision by the EU the UK might then turn around and give the US an adequacy decision permitting a work around of onward transfers from the EU to the UK and onward to the US. An adequacy decision from the UK, current projections are in early 2023, is made easier by the publication of the EU's own draft adequacy decision.

United States of America

State Laws

In the U.S. it is the year of state privacy laws. The CPRA amendment of CCPA took effect in California at the start of 2023 with an expanded scope to cover employee and business contacts, introduced a category of sensitive data, and created new data subject rights. Enforcement also shifted from the Attorney General to the California Privacy Protection Agency. With this new mandate, there is likely to be expanded enforcement. The Virginia Consumer Data Protection Act also took effect on 1 January. Colorado and Connecticut's laws will go into effect on July 1 and Utah from December 31. In addition, there are several active proposals in states across the country.

A game changer would be a privacy law with a private right of action like Illinois' Biometric Information Privacy Act (BIPA). BIPA allows private citizens to bring lawsuits against companies for violating the law. For this reason, BIPA is probably the most influential privacy law in the U.S. The American Civil Liberties Union, a revered civil liberties organization, is supporting several state proposals replicating BIPA's private right of action in democratically controlled states.

Federal Privacy Law: The Debate Continues

There were moments in 2022 when it seemed a federal privacy law would inevitably be passed, but here we are, still waiting. As more states enact or look to enact state privacy legislation, one wonders if the United States is approaching a tipping point where the federal government will just leave it to the states to regulate in this area. In the last Congress, one of the main challenges to getting federal privacy legislation was getting the House to bring it to vote. This was because the person responsible for calling a House vote, House Speaker Nancy Pelosi, is from California. A state that has broadly objected to the pre-emption of its own ground-breaking privacy law, CCPA as amended by CPRA.

The midterm elections brought a new party into power meaning Nancy Pelosi is no longer the Speaker. While the new Speaker, Kevin McCarthy is also from California. He is on the record supporting a pre-emptive federal privacy law and may bring it to the House floor at some point for a vote. The Senate is a much more difficulty balanced. In committee, Maria Cantwell has opposed the passage of the law as it was proposed and the main champion on the republican side has been replaced by Ted Cruz. However, if voted out of the House, there will be pressure on the Senate not to prevent the law as a once in a generation opportunity.

Conclusion

As always, there is a flurry of activity and change in the privacy and data protection space as regulators struggle to catch up with the explosive growth and innovation in the technology sector.

If you or your company is facing challenges from the expanding privacy and data protection regulatory landscape. Let us help you implement these necessary steps within your organization.
Please feel free to get in touch with our experts.

WRANGU

CONTACT US!

Website: www.Wrangu.com
Email: Hello@Wrangu.com