White Label Consultancy

Data protection and cyber security *in 2024*

JANUARY 2024

Contents

Introduction

2023 was a busy year within the data protection and cyber security domain. The Court of Justice of the European Union (CJEU) rendered 32 judgments related to data protection. Few of those decisions should be of special interest to companies, such as those related to the right to damages under the GDPR in case of data protection violation. Furthermore, the European Data Protection Board (EDPB) released a number of informative guidance documents, and several data protection authorities published their own guidelines to support businesses in implementing data protection programs. Some of the most important EDPB guidelines have been on data subject rights, such as right of access, personal data breach notification procedure under the GDPR as well as guidelines for identifying and avoiding deceptive design patterns. National DPAs released practical guidelines on technical security measures that companies should implement to secure personal data during data processing activities. A number of these guidelines were also translated by White Label Consultancy last year to make them more usable to a wider audience. These types of guidelines are very timely and should be carefully reviewed by companies as last year, a number of major companies suffered serious cyber incidents due to a lack or inadequate cyber security measures. The latest CJEU judgment according to which the disclosure of personal data or unauthorized access to personal data through a cyberattack by a cybercriminal can put an obligation on the controller to compensate the data subject for non-material damages, whereby non-material damage can also include fear experienced by a data subject about a possible misuse of personal data by third parties as a result of an infringement of the GDPR.

It is expected that 2024 will also bring many new developments that organizations should be aware of. For example, emerging artificial intelligence-based technologies also pose a serious threat to the cyber security domain as such technologies can be used for harmful cyber operations. Also, new legal acts related to both data protection as well as cyber security will be adopted or enter into force this year. This blog post will look into what organizations can expect both in data protection and cyber security.

1 Data protection in 2024

1.1 Trends in the European Union

At the beginning of last year, the European Commission published its plan to carry out another major review of the applicability of the GDPR. This will be the second review and is due in May 2024. The previous one took place in 2020, two years after the GDPR entered into force. While in 2020 the European Commission found that new amendments do not need to be made, the outcome of the second review might lead to some proposals for changes with regard to GDPR enforcement.

Data protection authorities will continue investigating the use of tracking technologies and issue guidance documents for the use of artificial intelligence. For example, Norwegian and Dutch data protection authorities have already explicitly stated that this year, they will put more focus on unlawful tracking practices through cookies as well as Facebook pixels. Increasing enforcement practice was exercised also by the Spanish data protection authority throughout last year and it will most definitely continue also this year. Data protection authorities are doing a lot of cooperation when it comes to enforcement and thus the fact that certain authorities have announced their plans should be seen as an indication that also other EU/EEA authorities will follow the path.

Another continuous big debate to continue in 2024 in the data protection domain concerns the new "Pay or Okay" module, which Meta enabled for its Facebook and Instagram platforms. The case goes back to Meta's behavioural advertising practice, which was subject to various litigation at the Court of Justice level as well as enforcement actions by data protection authorities. Meta's new "Pay or Consent" solution is currently being assessed by numerous data protection authorities in cooperation with the European Data Protection Board (EDPB) and the latter is supposed to rule on the matter in the coming months.

The end of 2023 was pivotal for artificial intelligence. Even though in December the European Parliament and the Council of the European Union reached a provisional agreement on the AI Act, which is the first comprehensive legal act to regulate artificial intelligence, it is expected that we will witness the formal adoption of the agreed final text in spring 2024. Once enacted, there will be a grace period for organizations to adapt to the new legal requirements and implement the measures required by the AI Act and the formal entrance into force will take place in 2026.

Spring of 2024 will be an important period for the data transfers between the European Union and the United States of America. Namely, in July 2023, when the European Commission adopted its adequacy decision on the European Union - the United States of America Data Privacy Framework, it published a timeline showing the process of the adoption of the new framework starting from 2022. The timeline highlighted that in spring 2024, the European Commission will carry out the first periodic review of the Data Privacy Framework.

At the end of November 2023, the Council of the European Union approved the Data Act. Data Act constitutes a new regulation on harmonised rules on the fair access to and use of data. As White Label Consultancy highlighted in one of its earlier blog posts, this act aims not just to protect data but also to ensure its accessibility and interoperability. Data Act addresses personal and non-personal data related to the performance, usage, and environment of connected products,

a significant expansion over the GDPR's scope. The act got published in the EU Official Journal in December and thus, by now, has entered into force.

On the 1st of November 2022, the Digital Markets Act entered into force. The Digital Markets Act is another European Union law that aims to enhance the fairness and contestability of the markets in the European Union digital sector. This law has an objective to identify large digital platforms that provide core platform services, "gatekeepers" on the market, and those gatekeepers will then be subject to concrete strict obligations and also certain prohibitions. The companies falling under the gatekeeper status are mostly the largest digital companies operating in the European Union market. The identified gatekeepers are given six months to get their operations into compliance with the Digital Markets Act requirements or they will face fines. The Digital Markets Act will continue to be very relevant for some major digital platform service provider companies as the European Commission is continuously expanding the gatekeepers list, and more and more companies are identified as gatekeepers. Thus, companies that might reach the threshold should already proactively make sure that they comply with the Digital Markets Act.

The European Commission shall continue working on the draft principles related to the voluntary cookie pledge initiative. In December 2023, the EDPB also provided the European Commission with its feedback on the principles and made several proposals for a change. The voluntary cookie pledge initiative is supposed to have a significant impact on the way cookies are used and installed on websites.

In March 2023, the EDPB launched its 2023 coordinated action, which was focused on the designation and position of data protection officers (DPOs). The coordinated action involved 26 data protection authorities throughout the whole European Economic Area as well as the European Data Protection Supervisor. The EDPB aims to make the report public during the first plenary session of the following year. In October, the EDPB also announced that in 2024 it will be focusing on the implementation of the right of access by controllers and for that, a new coordinated action will be launched.

1.2 Data protection beyond the European Union

1.2.1 Kingdom of Saudi Arabia (KSA) Data Protection Law

On the seventh of September 2023, the Saudi Data & Artificial Intelligence Authority (SDAIA) published its Implementing Regulations to the KSA Personal Data Protection Law (PDPL) and on the 14th of September, PDPL entered into force. The KSA PDPL together with the Implementing Regulation to the PDPL and the regulation on personal data transfers outside the KSA together form a comprehensive federal data protection regime of KSA. This new legal framework marks an important milestone for the KSA data protection field. Although the law entered into force in September 2023, it has a 12-month statutory grace period. Thus, the organisations concerned have until the 14th of September 2024 to become compliant.

1.2.2 UAE Data Protection Law Updates

As announced during one of the latest DIFC Data Protection Talks by the DIFC Commissioner's Office, in 2024 there will be a significant focus on adequacy decisions for data transfers. More specifically, DIFC will carry out a complete review of the UK adequacy decision. Furthermore, other existing adequacy decisions might be reviewed and reissued. 2024 might also bring some new adequacy decisions, however, no further information is known about that. In addition, the DIFC Data Protection Law will be amended with an aim to further develop and support regulation 10, i.e. the regulation of personal data pro-

cessing through the use of autonomous and semi-autonomous systems.

It remains to be seen what will happen with the UAE Data Protection Implementing Regulations. Following KSA´s recent adoption of the regulations, UAE may follow suit and draft the implementing regulations this year, but at the time of writing, there is no official announcement on this.

1.2.3 Data protection reform in Australia

In September 2023, the Australian Government published its response to the Privacy Act Review Report. In the publication, the Australian Government fully agreed with 38, partially agreed to 68 proposed amendments, and noted 10 proposals of the 116, which shall give the Privacy Act (Cth) significant reform in 2024. Such legislative amendments would positively impact privacy and data protection in Australia, as there have not been any major amendments since the 1980s. The Attorney-General's Department will lead the next stage of work, including the development of legislative amendments.

The proposed legislative amendments will benefit all aspects of society including individuals, businesses, and the government. The proposed amendments mainly relate to strengthening privacy laws to ensure the collection, use, and disclosure of people's personal information is reasonable. Reforms will ensure Australians can be more confident that their personal information is being protected appropriately and that action will be taken where businesses fail to manage personal information appropriately. For businesses, the privacy reforms will provide greater clarity on how to protect personal information, thus improving trust and fostering greater international competitiveness. For the government, the reforms will bring strengthened enforcement options and measures to enhance the effectiveness of Australia's privacy regulator.

Finally, the legislative amendments will give greater enforcement powers to the Office of the Australian Information Commissioner (OAIC) and expand the scope of orders the court may make in civil penalty proceedings, and empower the courts to consider applications for relief made directly by individuals.

Beyond the legislative amendments and reform, the Attorney-General's Department will also be focusing on non-legislative reform, with a key initiative being the introduction of the Children's Online Privacy Code.

All proposed reforms directly build on the commitment to prioritise privacy and data protection as outlined in the 2023-2030 Australian Cyber Security Strategy.

1.2.4 The United States of America (US) State privacy laws

This year, the US will see an entrance into force 8 new state privacy laws. At the end of March, the **Washington My Health My Data Act** will enter into force. This is considered an important piece of legislation that will contribute to regulating health data at the state level. My Health My Data Act regulates very strictly the collection, processing, and sale of consumer health data. This law is also novel as it allows a private right of action in case of violations. At the same time, **Nevada Senate Bill 370** will enter into force. It is a comprehensive health privacy law, that will put in place strict requirements regarding the collection, use, and sale of consumer health data. The bill will prohibit the collection and sharing of such data without the consumer's freely given and affirmative consent. The bill also provides a prohibition for the sale of consumer health data without the consumer's written consent.

On the 1st of July, 4 US state privacy laws will enter into force – the **Texas Data Privacy and Security Act (TDPSA), Oregon Consumer Privacy Act (OCPA), Colorado Privacy Act „universal opt-out" mechanism** and **Florida Digital Bill of Rights (FDBR).**

The TDPSA establishes transparency and disclosure obligations on controllers conducting business in Texas which are consumed by residents of Texas. The law applies also to the controller, who

processes personal data himself or is engaged in the sale of personal data and controllers, which are not small businesses in accordance with the US Small Businesses Administration. TDPSA, however, has some exemptions about applicability, such as not applying to state government entities, nonprofit organisations, higher educational institutions, etc.

Oregon Consumer Privacy Act (OCPA) has similarities to the privacy law of Texas as it also puts transparency and disclosure obligations on the controller, who conducts its business in Oregon or produces services or products, that are targeted to the residents of Oregon. The law applies to the controller that goes under the aforementioned definition and who controls or processes personal data of not less than 100,000 Oregon residents, excluding personal data controlled or processed solely to complete a payment transaction or controls or processes personal data of not less than 25,000 Oregon residents and derives more than 25 percent of its gross revenue from the sale of personal data.

Colorado Privacy Act "universal opt-out" mechanism constitutes a universal opt-out mechanism according to which, the consumers will be vested with rights to opt out of the sale of their personal data as well as the processing of their personal data for targeted advertising. The organisations to which the Colorado Privacy Act applies must enable the consumers to opt out of such practices through the universal opt-out mechanism.

Florida Digital Bill of Rights (FDBR) is another comprehensive US state privacy law. Even though this state privacy law is mostly similar to those of other states, it still differs slightly due to its high jurisdictional threshold. According to the scope of the FDBR, it applies to controllers who have an annual global revenue of more than $1 billion and derives 50 percent of their global gross annual revenue from the sale of advertisements online, operate a consumer smart speaker and voice command service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation or operate an app store or digital distribution platform with at least 250,000 different software applications for consumers to download and install. Considering these limitations, it this law will be more important for bigger tech companies and most other businesses will not be subject to its scope. In addition to the earlier mentioned state privacy laws, on the first of October, two more privacy laws enter into force – the Montana Consumer Data Privacy Act and minors-related provisions of the Connecticut Act concerning Online Privacy, Data, and Safety Protections.

Montana Consumer Data Privacy Act will impose specific transparency and disclosure obligations on a controller, who conducts its business in Montana or produces services or products, that are targeted to the residents of Montana and a controller that controls or processes personal data of not less than 50,000 Montana residents, excluding personal data controlled or processed solely to complete a payment transaction or controls or processes personal data of not less than 25,000 Montana residents and derives more than 25 percent of its gross revenue from the sale of personal data.

The Connecticut Act concerning Online Privacy, Data, and Safety Protections is Connecticut's new state privacy law, which aims to amend the current Connecticut Data Privacy Act to provide more protection for health and minors' personal data. According to the timeline, most of the provisions will enter into force on the first of October 2024, however, the provisions requiring media platforms to unpublish or delete certain minors' accounts will enter into force on the first of July 2024. According to new provisions, social media platforms will be under obligation to unpublish or delete the social media accounts of minors in case such a request is made by the minor or the minor's legal guardian. This means that social media platforms will need to also create such mechanisms to enable the filing of the mentioned requests.

2 Cyber security developments in 2024

2.1 NIS 2 Directive

In July 2016, the Directive on the Security of Network and Information Systems (NIS) entered into force. This directive is an EU-wide cybersecurity-related legislation established to increase cyber resilience across the whole EU through specific regulatory measures. More specifically, the directive strengthened the cyber security capabilities on a national level, enhanced collaboration between states, and implemented cyber security in organisation by default. On the 16th of January 2023, the NIS 2 Directive entered into force. This is a sequel to the NIS Directive. The objective of the NIS 2 Directive is to boost cyber security in the EU and keep up with the evolving digitalisation and address more effectively the threats posed on the cyber security landscape. The directive shall increase the preparedness of the member states, further enhance the cooperation between states through setting up a cooperation group, and increase the maturity of cyber security across the sectors, which are vital for the economy and society as a whole. According to the agreed timeline, the states have until the 17th of October 2024 to adopt and publish the measure to comply and transpose the NIS 2 Directive. The measures need to be applied by the 18th of October 2024 and from the same day, the NIS Directive will be repealed.

2.2 The Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554

DORA is an important cyber security regulatory framework addressing operational resilience and cyber security maturity in financial services. DORA foresees the businesses to implement cyber security in its core business activities. The regulation establishes legally binding rules for information communication technology risk management, incident reporting, and third-party risk management. Although most deadlines of DORA will come in 2025, it is in 2024 that the firms must develop their roadmaps with regard to the implementation of the operational resilience framework. In accordance with DORA requirements, the financial services providers will need to be compliant with the new DORA requirements by Q4 of 2024.

Financial entities and third-party ICT services providers will have until the 17th of January to comply with DORA since that is when the enforcement starts.

2.3 European Union Cyber Resilience Act (CRA)

On the 30th of November 2023, the European Parliament and the Council of the European Union reached a political agreement on CRA, which the European Commission proposed in September 2022.

The CRA will be an important legislation in the European cyber security landscape as it will be the first of its kind in the world. The Cyber Resilience Act will require that all products put on the European Union market to be cyber secure. It will also complement existing legislation, specifically the NIS2 Framework, which was adopted in 2022. The CRA seeks to harmonise rules and standards when bringing to market products or software with a digital component. It hopes to establish a framework of cybersecurity requirements that govern the planning, design, development, and maintenance of such products, with obligations to be met at every stage of the value chain. Finally, the CRA creates an obligation to provide a duty of care for the entire lifecycle of

such products. As in 2023 only a political agreement was reached, it is expected that it will finally adopted no earlier than in the second half of 2024. This will mean that the new requirements set forth by the regulation will be applicable in 2027 and the obligation to report incidents and vulnerabilities in 2026.

3 Key Takeaways

2024 will be also a very busy year both in data protection, but also in the cyber security field. Numerous judgments are expected from the Court of Justice of the European Union, furthermore, a number of data protection authorities will publish their decisions in some cases related to major social media companies about topics like data transfers and behavioural advertising. Also, a lot of states in the United States of America will have their data protection laws come into force. Similarly, there are a lot of data protection legislative developments also in other jurisdictions. In addition, the cyber security domain will see the repeal of the NIS Directive with the NIS 2 Directive and this will bring additional obligations for companies.

3.1 Some possible action items for companies

Review your cookie banners and other tracking technologies

Whenever companies are using cookies or other types of tracking, they need to have in place cookie banners, which should inform users about the use and types of cookies as well as their purposes. Companies should also have a clear overview of the types of cookies and whenever necessary request consent from the users.

EU companies should evaluate their data subject request procedures

Throughout 2024, the European Data Protection Board will be focusing on the implementation of the right of access by controllers. For that, a coordination action will be launched. Thus, companies should carry out a critical review of their data subject request procedures. The companies should see if they have in place needed documentation on data subject requests and if roles and responsibilities are organised.

Companies engaging in business activities in the United States of America should keep an eye on emerging state privacy laws

The United States of America has in 2024 eight new state privacy laws coming into force. This can have significant implications for the data processing activities of companies that carry out business also in the United States of America. Thus, these companies should review their business activities and data protection framework to stay compliant with new possible obligations.

Enforcement of the Kingdom of Saudi Arabia Data Protection Law begins

Last year saw the entrance into force of the data protection law of the Kingdom of Saudi Arabia. In light of the start of the enforcement of this law in September 2024, the companies should start

carrying out data mapping, if they already have not yet. Furthermore, companies should have in place data protection policies, procedures, and privacy notices to ensure that data protection and security standards are met. Similarly, necessary security controls have to be implemented.

Companies engaging in business activities in Australia should follow the review of the Australian Privacy Act

The exact details of the changes with regard to the Privacy Act (Cth) are not yet known. However, it can be stated that many of the legislative reforms will relate to enhancing privacy and data protection, whilst also increasing enforcement powers. In light of this, the Australian government has published "Overview of Cyber Security Obligations for Corporate Leaders" detailing governance obligations to assist in the management of risk and response to cyber incidents.

Organisations, which are providers of essential or important services should prepare for the compliance of NIS 2 Directive

The mentioned type of companies needs to carry out due diligence against their technology partners. More specifically, cybersecurity-related processes have to be reviewed and vendor risk assessments evaluated. Moreover, a holistic assessment has to be done on security controls.

Contact

hello@whitelabelconsultancy.com
+45 71 74 74 54

NORWAY

Main Office Oslo

+47 4141 2168

Fjordalléen 16
0250 Oslo

DENMARK

Copenhagen Office

+45 71 74 74 65

Dampfærgevej 27
2100 København Ø

POLAND

Warsaw Office

+48 515 07 99 77

Ul. Marszałkowska 58/15
00-545 Warszawa

UNITED ARAB EMIRATES

Dubai Office

+971 50 4536616

Dubai World Trade Center
Dubai

White Label Consultancy

Data protection and cyber security *in 2024*

JANUARY 2024