White Label Consultancy

EU Digital Regulations

June 2024

In 2024, businesses will need to navigate a changing landscape of data protection and cybersecurity regulations. Below, we present a list of key European Union (EU) digital regulations to monitor, along with a brief explanation of their implications.

Table of Contents

Part I. Cybersecurity

1. NIS2 Directive

Overview

The Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive *(NIS2 Directive)* (NIS2) is the new EU legislation governing cybersecurity. Importantly, the NIS2 Directive is the official successor of the Network and Information Security (NIS) Directive, which was introduced in the EU in 2016.

The NIS2 has the primary objective of instilling a new common high-level approach for cybersecurity across the EU and increasing the overall level of cybersecurity in the EU. NIS2 also requires EU Member States to increase the cyber resilience of public and private entities operating in critical sectors. This makes the NIS2 Directive one of the most important cybersecurity-related legal acts in the EU. It puts forward specific measures regarding cybersecurity risk management and establishes obligatory reporting requirements for several highly critical sectors.

The NIS2 Directive entered into force on 16 January 2023. However, the EU Member States have until 17 October 2024 to transpose NIS2 into national law and provide the necessary publication. Thus, the NIS2 Directive will be applicable and enforced starting 18 October 2024.

The upcoming discussion gives an overview of the NIS2 Directive, highlights the changes it brings, and puts forward several action items for companies.

Applicability

Previously, the NIS Directive categorised entities as essential services providers and digital services providers, whereas NIS2 splits entities under essential sectors or important sectors.

Whereas under the previous NIS Directive, it was up to the EU Member States to decide what entities fall under the covered categories, the NIS2 Directive directs that the categorisation will be based on the size of the entities. Hence, medium-sized and large entities will be covered within the scope of the new directive.

Furthermore, NIS2 widens the scope with regard to sectors falling under the two categories mentioned above. For example, the Directive will extend cybersecurity obligations to (i) the EU reference laboratories (in the meaning of Regulation (EU) 2022/2371 on serious cross-border threats to health); (ii) manufacturers of certain medical devices (in the meaning of the Regulation 2022/123 on the reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices); (iii) basic pharmaceutical products; and (iv) entities carrying out research and development activities of medicinal products.

The NIS2 Directive develops requirements related to entities operating in approximately 18 sectors. These sectors are divided into two categories – essential sectors and important sectors. Notably, the obligations under the NIS2 differ depending on which category the

organisations fall within. For example, fines for non-compliance are higher if you are classified as an essential sector.

- The category of essential sectors includes Energy, Transport, Finance, Public Administration, Health, Space, Water Supply (drinking & wastewater), and Digital Infrastructure, including cloud computing service providers and ICT management providers.

- The second category of important sectors includes organisations from the following sectors: Postal Services, Waste Management, Chemicals, Research, Foods, Manufacturing (medical devices and other equipment), and Digital Providers (social networks, search engines, and online marketplaces).

In accordance with EU law, NIS2 applies to entities with fewer than 250 employees and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million. However, exemptions exist, such as entities deemed as providing critical infrastructure and services to the government. The categorisation also defines the level of supervision of compliance with the requirements stemming from the NIS2 Directive as well as the sum of fines, which can be issued in case of infringements.

Key Points

The Council of the EU stated in 2022 that the NIS2 Directive will set the baseline for cybersecurity risk management measures and reporting obligations across all sectors that are covered by NIS2. This means putting forth guidance for such entities on handling and addressing cyber threats.

Within the NIS2, there are four new organisational requirements that organisations must implement throughout their business entities.

1) Risk Management;
2) Corporate Accountability;
3) Reporting Obligations; and
4) Business Continuity.

In relation to risk management, Article 21 states that essential entities must ensure they take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems, and there must be adequate measures instilled to minimise the impact of an incident. Article 21 takes a holistic approach, and requires the protection of not only, the network and information systems, but also the physical environment of such systems.

To comply with the new Directive, organisations must take measures to minimise cyber risks. These measures include incident management, stronger supply chain security, enhanced network security, better access control, and encryption.

The NIS2 Directive also expands the duty of care and imposes stricter reporting requirements for cybersecurity incidents. This essentially implies that, contrary to the previous NIS Directive, every cybersecurity breach must be reported to the relevant authority regardless of the impact of the breach on the organisation's operations.

Contained within Article 23, under the new Directive, reporting has been divided into three phases:

1) The initial phase is notification which requires that authorities be notified without undue delay and in any event within 24 hours of becoming aware of

the significant incident. The notification shall provide information on whether the cyber incident is believed to be the result of unlawful or malicious acts, or if it might have a cross-border impact.

2) The initial notification is being followed by a follow-up notification. This means without undue delay and in any event within 72 hours of becoming aware of the cyber incident, follow-up information must be provided giving further details about the incident, its severity and its impact.
3) Lastly, there is the final report obligation, which requires the entity to provide not later than one month after the submission of the follow-up incident notification a report that has a detailed description of the cyber incident, the type of threat or root cause behind the incident, information about the measures applied and where applicable, the possible cross-border impact of the incident.

Enforcement and Fines

The NIS2 Directive brings significant administrative fines for violations of its obligations, the amount of which varies depending on the categorisation of the entity.

For organisations designated as essential entities, the administrative fines can reach up to EUR 10 million or at least 2% of the total annual worldwide turnover in the previous fiscal year of the undertaking to which the essential entity belongs, whichever is higher.

On the other hand, important entities can be subject to administrative fines of up to EUR 7 million or at least 1.4% of the total annual worldwide turnover in the previous fiscal year of the undertaking to which the important entity belongs, whichever is higher.

Next steps

Where the NIS2 Directive is applicable, the following obligations must be implemented:

Management should have a clear understanding of the requirements of the Directive and the risk management efforts. Specifically, it has a direct responsibility to identify and address cyber risks to ensure ongoing compliance with the requirements. Thus, as part of the organisations' ongoing obligations, management must ensure they have updated knowledge of the Directive and should engage in regular training. This is a specific requirement contained within Article 20 of the Directive.

Since the reporting requirements have changed (as described in more detail in the above paragraph), organisations must accordingly update internal processes to ensure proper reporting to authorities.

Risk management processes and policies must be implemented throughout the organisation. This includes incident management, improved supply chain security, network security, access control, and encryption.

It is also required that organisations consider business continuity in the event of a cyber incident, which can include system recovery, emergency procedures and the establishment of a crisis response team.

2. Cyber Resilience Act

Overview

On 30 November 2023, a political agreement was reached on the *Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for*

products with digital elements and amending Regulation (EU) 2019/1020 (*Cyber Resilience Act)* (CRA). The CRA builds on the EU's Data and Cyber Strategies and forms an important part of the upcoming EU certification schemes, e.g. the EU Cloud Services Scheme and the EU ICT Products Scheme.

The CRA will be an important legislation in the EU cybersecurity landscape as it will be the first of its kind in the world. It will regulate various products with a digital component, which are being used in daily life. The CRA puts forward requirements that all products placed on the EU market need to be cyber-secure. It will also complement existing legislation, more specifically the NIS2 Directive.

The CRA seeks to harmonise rules and standards when bringing to market products or software with a digital component. It aims 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.

The CRA was approved by the European Parliament in March 2024 and is expected to be adopted by the Council. This will mean that the new requirements will become applicable in 2027 and the obligation to report incidents and vulnerabilities in 2026.

Applicability

The CRA applies to all operators involved in the lifecycle chain of products with a digital element. This covers manufacturers, importers as well as distributors. The CRA also applies extraterritorially, meaning it applies to entities both inside and outside of the EU, in so far as they import, place, or distribute their products with digital elements on the EU market.

The CRA applies to products with digital elements, which in the meaning of the act means software or hardware products, which are intended to be used to connect to a device or network and remote data processing solutions, which are necessary for the products with digital elements to function. Furthermore, the act also covers hardware or software components of such products, which are placed on the EU market.

The CRA classifies products with digital elements into the three main categories below, depending on the risk level associated with the product:

- Default category – products, without critical cybersecurity vulnerabilities. Examples of products falling into the default category are smart speakers and word processors. These products will be subject to a "self-assessment" conducted by the manufacturer.

- Critical category:
    - Class I – products that either (i) primarily are meant to perform functions critical from the cybersecurity of other products, networks or services, or (ii) perform a function, which poses a significant risk of adverse effects in terms of intensity and ability to control, disrupt or cause damage to a large number of other products or the health and safety of a large number of individuals through direct manipulation. Products falling into class I of the critical category shall be subject to a standard harmonised form assessment,

i.e., a European standard form developed by an officially recognised European Standards Organisation or third-party assessment to show compliance with regulatory obligations. Third-party assessments shall be conducted by an officially recognised notified body based on the criteria set out in the CRA. It is the task of the EU Member States to appoint these notified bodies, and the European Commission will keep an updated list of them.

- Class II – products, which provide a critical cybersecurity function and can significantly affect a larger number of products belonging to this category.

It is important to note that the CRA includes exemptions. More specifically, products that are already subject to existing cybersecurity regulations – such as Medical Devices Regulation, Automotive Type Approval General Safety Requirements, Regulation for Products Affected by Aviation Rules, and EU Directive for Marine Products – are exempt.

Key Points

The CRA stipulates cybersecurity requirements towards respective software and hardware products with a digital element. More specifically, the manufacturers of such products need to put in place appropriate cybersecurity measures across the whole product lifecycle, e.g. starting from the design phase and development stage throughout the commercialisation stage in the EU market. Importantly, the manufacturers are obliged to implement essential cybersecurity requirements mentioned in Annex I of the CRA.

The manufacturers are required to conduct assessments to identify and address cybersecurity risks. Products with known vulnerabilities cannot be placed on the EU's market. The products that are placed on the market must feature access controls to prevent unauthorised access. Moreover, manufacturers need to establish procedures for handling vulnerabilities and incidents. They must understand how to address, document, and implement measures related to vulnerabilities.

Additionally, manufacturers are required to perform regular conformity assessments to verify their products comply with the CRA requirements. These products must also undergo a distinct conformity assessment as mandated by the European Health Data Space (EHDS) Regulation.

Enforcement and Fines

The enforcement will be conducted by EU Member States. According to the CRA, administrative fines for violations can reach up to EUR 15 million or 2.5% of a company's annual worldwide turnover.

Next steps

While the European Parliament has already adopted a provisional version of the final text at its plenary meeting on 12 March 2024, the CRA still requires formal adoption by the Council. Organisations that are covered under the CRA should already be conducting comprehensive maturity assessments to determine their current maturity status. It is recommended that these organisations also perform cybersecurity assessments on their products, evaluate third-party risks, and

measure their practices against international cybersecurity standards.

3. Digital Operational Resilience Act

Overview

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU (DORA) was formally adopted in November 2022. It will enter into force on 17 January 2025. The DORA is a crucial regulatory framework within the EU aimed at enhancing operational resilience and cybersecurity maturity in the financial sector. It mandates that businesses integrate cybersecurity into their core activities.

DORA sets forth legal requirements for managing information communication technology (ICT) risks, reporting incidents, and managing risks associated with third-party services. Specifically, DORA imposes obligations on the security of networks and information systems for organisations in the financial sector and extends these obligations to third parties providing ICT services. In principle, DORA seeks to standardise and strengthen existing requirements concerning ICT governance, incident reporting, and risk management measures. This represents a unique regulatory approach in the EU, which has previously addressed ICT risk management through broader directives and guidelines without a wide-reaching regional focus. A primary goal of DORA is to harmonise how ICT risk management is regulated across the financial sector, moving away from the current system where EU Member States regulate these risks individually.

While most of DORA's deadlines are set for 2025, financial firms are required to develop their implementation for the operational resilience framework in 2024. According to DORA's provisions, financial services providers must comply with the new requirements by the fourth quarter of 2024.

Additionally, both financial entities and third-party ICT services providers have a compliance deadline of 17 January 2025, when enforcement of DORA begins.

Applicability

The DORA applies to a wide range of financial institutions and entities, including credit institutions, investment companies, trade repositories, investment managers, crypto-asset service providers, and crowdfunding service providers. It extends the scope of the existing EU laws that already regulate these entities within the financial sector.

Additionally, DORA imposes obligations on third-party communication providers deemed critical by major financial regulatory bodies such as the European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and other EU financial authorities. The determination of a third party's criticality involves assessing factors such as the potential impact of financial services in the event of a large-scale incident and the type and significance of the organisations and companies that depend on these third parties.

DORA, primarily focused on ICT and cybersecurity, is structured around five key pillars. These pillars outline specific requirements to enhance the overall digital operational resilience of the financial sector. The pillars include:

- Governance,
- Risk management,
- ICT-related incident reporting,
- Digital operational resilience testing, and
- Information sharing.

Under DORA, organisations within its scope are required to establish a comprehensive ICT risk management framework. This framework should enable them to identify, assess and monitor various ICT-related risks effectively. Additionally, DORA specifies requirements for contracts with third-party ICT service providers, ensuring these agreements address relevant regulatory expectations.

A key goal of DORA is to standardise incident reporting obligations across the European financial industry to streamline how ICT-related incidents are reported. This standardisation aims to improve consistency and efficiency in handling such incidents. Moreover, DORA seeks to enhance communication and cooperation between EU Member States, fostering a more unified approach to digital operational resilience. It also mandates that organisations regularly test their ICT systems and continuously monitor and implement mitigating measures against risks posed by third-party providers, ensuring ongoing vigilance and responsiveness to potential vulnerabilities.

Key points

Financial institutions will be obliged to carry out mapping and testing of their critical business services, IT systems and relevant processes with the purpose of identifying any possible risks and managing the identified risks.

Financial institutions will need to establish and adopt effective and functional cybersecurity measures to be able to address and mitigate different types of cyber and data breach incidents. Organisations must build a risk management framework by design and default into their daily business activities.

Financial institutions are under an obligation to establish and maintain robust governance to be able to build up operational and cyber resilience. In addition, with the establishment of governance, financial institutions must also appoint personnel who will be responsible and accountable for the maintenance of governance.

Financial institutions must carry out regular testing and reviews of their resilience plans and make sure that personnel are properly trained.

Enforcement and Fines

Under DORA, EU Member States are required to develop rules for administrative penalties and remedial measures that can be applied in cases of DORA violations. The penalties and measures implemented should be effective, proportionate, and dissuasive. For example, entities classified as critical may be subject to administrative fines amounting to 1% of a covered entity's daily turnover for up to six months.

Next steps

The rules established by DORA entered into force on 16 January 2023. Organisations and financial entities within its scope have until 17 January 2025 to prepare and achieve compliance with DORA requirements. It is essential for these organisations to begin implementing the necessary measures to enhance their maturity in managing ICT-related risks. A highly recommended approach for these entities is to conduct a comprehensive gap assessment to identify areas that require additional work and

investment. Understanding existing weaknesses and areas needing further development is crucial for entities to position themselves better with respect to DORA's requirements.

Part II. Data Regulation

4. Data Act

Overview

The *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828* (Data Act) is aimed at enhancing the EU's data economy. It seeks to make data, particularly industrial data, more accessible and usable to foster data-driven innovation and improve data availability across the EU. The Data Act sets out clear rules on data usage and sharing, with the aim of ensuring fairness in the allocation of data value among stakeholders.

Applicability

The Data Act primarily impacts businesses that deal with data generated from connected products ranging across multiple sectors, including:

- vehicles,
- lifestyle gadgets,
- home appliances,
- medical devices, and
- more, which are part of the IoT and capable of gathering and sharing data.

The Data Act impacts all who handle, share, or utilise product data, including the providers of related services. It also impacts data holders who make data available within the EU, as well as data recipients in the EU. The manufacturers of connected products and providers of related services, regardless of their location, are subject to the Data Act if the products are marketed in the EU.

Of note, micro, small and medium-sized companies are exempt from some obligations.

Separately, the Data Act mandates providers of data processing services, such as cloud and edge, to facilitate customer switching, ensuring transparency, support, and minimal disruption during the transition.

Key Points

The Data Act covers the following main contexts:

a. Mandatory data sharing

Data-driven businesses must be on the lookout because the Data Act will require providers of connected products or related services to allow access to the (non-)personal data generated by their products and share it with third parties.

The Data Act simplifies data sharing. In B2B (business to business) and B2C (business to consumer) scenarios, it mandates:

- clear design,
- pre-contractual information, and
- clear user rights and data holder's obligations ensuring easy access to product/service data, including metadata.

Fairness in data sharing between businesses is required and must be supported by fair and non-discriminatory terms and protection against unilaterally imposed contracts. In B2G (business to government) interactions, public sector bodies will largely rely on requests for data on "exceptional need" to respond to public emergencies. Requests must be justified and protection measures for data specified. Data holders, except micro and small enterprises, must provide necessary

data free of charge. Other requests, such as for public interest tasks like official statistics production, may entail compensation to cover the costs of anonymisation or technical adaptation.

b. Enhanced service switching

Separately, the Data Act mandates data processing service providers to ensure seamless customer switching. Key obligations include:

- informing customers about switching procedures and limitations,
- clearly defining contractual terms related to switching,
- offering technical assistance for functional equivalence in new services and smooth transition, and
- initially imposing reduced switching charges which will be prohibited after three years.

Providers must also disclose the jurisdiction of their infrastructure and measures to prevent unauthorised governmental access or transfer of non-personal data that conflicts with EU law.

Enforcement and Fines

The Data Act aims for "effective, proportionate, and dissuasive" penalties for violations to ensure compliance. It requires EU Member States to implement rules on penalties and notify the European Commission of such rules by 12 September 2025.

Additionally, the Data Act prescribes that the current data protection authorities may, within their scope of competence, impose GDPR-level fines for infringements of the obligations laid down in the Data Act.

Next steps

The Data Act officially entered into force on 11 January 2024, but most of its obligations will apply from 12 September 2025. Businesses should begin preparing already by reviewing their current data handling practices to align with the new rights and obligations and incorporating compliance into business strategies.

To guide businesses through the new Data Act, the European Commission aims to release recommended model contractual terms for data-sharing contracts. These terms will offer guidance on reasonable compensation and the protection of trade secrets. Additionally, the European Commission plans to suggest non-binding contractual clauses specifically for cloud computing arrangements between service users and providers. To facilitate this, an expert group has been formed, tasked with drafting these terms and clauses, aiming to present their recommendations by autumn 2025.

5. Digital Services Act

Overview

Among the new EU digital regulations, the *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)* (DSA) is expected to introduce updated consumer protection rules in the online environment. Under the principle of "what is illegal offline should be illegal online", the new rules establish a framework for accountability, ensuring that online service providers are held responsible for their content moderation practices in the digital space. Regulation of online services has been long overdue, with the last major legislative

change in e-commerce happening around 20 years ago. The new rules are essential for establishing clear and fair standards.

Applicability

The DSA applies to companies providing digital services to both individuals and legal entities in the EU, irrespective of the company's location. Regulatory requirements vary based on the company's size and the type of services they offer. Companies that display and distribute user-generated content to the public, such as social networks, are subject to the most stringent regulations under the DSA. Overall, the DSA categorises regulated companies as follows:

- Mere conduit services: these are providers of communication networks, such as internet access providers.
- Caching services: they also provide communication networks but temporarily store data solely to enhance the efficiency of onward transmission of data (e.g. content delivery networks).
- Hosting services: these services store data upon a user's request, such as cloud services or web hosting companies.
- Online platforms considered a subset of hosting services: these platforms distribute user-generated content to the public (e.g. online marketplaces, app stores, collaborative economy platforms, social networks).
- Very Large Online Platforms (VLOPs): this category includes online platforms with over 45 million users in the EU, facing the highest level of regulation.

Key Points

Key aspects of the DSA include the mandatory removal of illegal content, such as IPR infringements or dangerous goods or misleading ads, by online platforms swiftly after being notified by a trusted flagger. Online marketplaces will also need to implement the "know your business customer" principle to trace their traders, and to refrain from the use of dark patterns that manipulate user behaviour online. These measures are part of a broader set of obligations.

The common requirements applicable to all regulated companies include:

- acting on orders against illegal content,
- implementing updated terms and conditions that clearly explain any content moderation activities and relevant complaint procedures in plain and age-appropriate language,
- publishing yearly reports on content moderation efforts, with the specific information required varying based on the type of provider.

At the end of 2023, the European Commission launched a public consultation to prepare templates for the annual transparency reports required under the DSA. However, the initiative is not finalised yet, with the planned adoption of Implementing Regulation providing templates in 2024.

Enforcement and Fines

Penalties for failing to comply can amount to up to 6% of a company's annual worldwide turnover. Enforcement at the national and EU level is expected, accompanied by substantial fines. Companies are overseen by national regulators and coordinated by a Digital Services Coordinator in each EU Member State. VLOPs fall under the jurisdiction of the European Commission. The DSA establishes a new European Board for Digital Services to aid in uniform enforcement.

Next steps

As of 17 February 2024, the DSA is fully applicable. All companies must determine whether they are covered by the scope, and in which category their services fall, e.g., intermediary, hosting service or online platform. As a minimum starting point, companies need to (i) update their systems to effectively identify and remove illegal content in compliance with the DSA requirements, and (ii) revise their terms and conditions (T&Cs) to ensure they are clear about content moderation activities and relevant complaint procedures.

6. Digital Markets Act

Overview

The *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)* (DMA) introduces rules for platforms that act as "gatekeepers" in the digital sector, with the aim of preventing them from imposing unfair conditions on businesses and end users and at ensuring the openness of digital services.

Applicability

The DMA applies to companies that are designated as gatekeepers for one or more of the "core platform services" (CPSs) listed in the DMA. A pre-defined set of CPSs covers e.g. online search engines, app stores, and messenger services. The gatekeepers:

- have a strong economic position, significant impact on the internal market, and are active in multiple EU countries,
- have a strong intermediation position, meaning that they link a large user base to a large number of businesses,
- have an entrenched and durable position in the market, meaning that their position has been stable over time.

Key Points

The DMA establishes clear and far-reaching ex-ante obligations for gatekeeper platforms, as well as prohibitions of certain activities. These have significant implications not only for the gatekeeper platforms themselves but also for "business users" or those using the gatekeeper's CPSs for the purpose of providing goods or services to end users.

Some of the obligations of gatekeeper platforms under the DMA are:

- refrain from using non-public data generated by business users in the context of its CPS, to compete against the business users on the platform,
- rank their own services or products, as well as third-party services or products, in a non-discriminatory way,
- give third-party service providers access to the same hardware or software features, as are available to, or used by that gatekeeper,
- give business users access to data generated in the context of the CPS, including data on engagement.

Gatekeeper platforms are not allowed to treat their products and services more favourably than those offered by third parties on their platform. In addition, gatekeeper platforms are not allowed to track outside end users for targeted advertising, absent effective consent.

Enforcement and Fines

Fines for non-compliance are significant and may equate to up to 10% of the company's total worldwide annual turnover or up to 20% in the event of repeated infringements. In case of systematic infringements of the DMA obligations by gatekeepers, additional remedies may be imposed after a market investigation. Such remedies will need to be proportionate to the offence committed. Non-financial remedies can also be imposed as necessary, including certain behavioural and structural remedies, such as the divestiture of parts of a business.

Next steps

Notably, gatekeepers have six months from the date of the European Commission's decision to designate them as a gatekeeper to fully comply with their DMA obligations for each of their designated core platform services.

The EU originally designated six gatekeepers; however, this list has recently expanded. Gatekeepers now include:

- Alphabet,
- Amazon,
- Apple,
- Booking.com,
- ByteDance,
- Meta,
- Microsoft.

7. AI Act

Overview

On 13 March 2024, the European Parliament passed the *Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* (AI Act). The AI Act is the world's first comprehensive legal act, which regulates Artificial Intelligence (AI). The AI Act establishes specific requirements and rules for the use and development of AI.

The objective of the AI Act is to provide those developing and deploying AI with clear requirements and obligations regarding specific use cases of AI. In addition, the purpose of the AI Act is to ensure that the AI systems which are deployed and used in the EU respect fundamental rights, foster innovation within the AI domain and develop the EU's single market in the AI field.

The AI Act has divided AI systems into three different risk categories: unacceptable risk, high risk, and low risk. Systems that create and can create an unacceptable risk, such as social scoring run by governments, are prohibited. High-risk applications, on the other hand, include critical infrastructures that might put the health and life of citizens at risk, safety components of products, and various essential private and public services, such as credit scoring systems. High-risk applications are subject to specific legal requirements. The last category of AI applications includes those which are not explicitly prohibited or listed as high-risk.

Applicability

According to the AI Act, the regulation applies to:

- Providers placing on the market or putting into service AI systems, or placing on the EU market general-purpose AI models, irrespective of whether those providers are established or located within the EU or in a third country.
- Deployers of AI systems that have their place of establishment or are located within the EU.

- Providers and deployers of AI systems that have their place of establishment or are in a third country where the output by the AI system is used in the EU.
- Importers and distributors of AI systems.
- Authorised representatives of providers which are not established in the EU.
- Product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark.

The AI Act defines AI systems broadly, encompassing a wide range of technologies and systems. As a result, a significant number of organisations are likely to fall within the scope of the regulation.

Key Points

General-purpose AI models which come with system risks will be subject to more stringent obligations. This means that for such AI models, there is a need to conduct model evaluations. Furthermore, the model must be analysed with regard to cybersecurity to ensure that possible risks are mitigated.

According to the AI Act, providers of general-purpose AI models are under an obligation to establish and maintain technical documentation of the respective models. The information must include documentation for those providers that integrate such general-purpose AI models into their AI systems and publish an overview of information which has been used to train the model. Furthermore, providers of such models must also adopt a policy regarding EU copyright law.

Public bodies, as well as private entities providing public services, such as banks, government, hospitals, and insurance providers, who deploy high-risk AI models, are under an obligation to carry out fundamental rights impact assessment. The assessment must include an overview of processes where such AI systems are to be used and an overview of the categories of natural persons and groups who are likely to be affected by these AI systems. Additionally, it is required that information be provided regarding the duration for which the AI system will be operational, as well as details on the frequency of its usage. In addition, the bodies must also make available a description of measures that will be implemented in case of incidents, as well as an overview of human oversight of the processes.

The AI Act imposes transparency obligations on many providers and users of certain AI and general-purpose AI models.

Enforcement and Fines

To ensure effective oversight over the field, the European Commission has established an AI Board and an expert group, both operating at the EU level. Additionally, each EU Member State is required to designate a national competent authority. This authority acts as a national supervisory body, empowered to ensure compliance with the AI Act.

Under the AI Act, EU Member States are required to establish specific rules regarding penalties and other enforcement measures for violations of the AI Act by operators. These measures can include both warnings and non-monetary actions. Additionally, EU Member States must ensure that any breaches of the AI Act are effectively implemented.

According to the AI Act, non-compliance with the prohibitions on certain AI practices specified in the regulation can lead to administrative fines of up to EUR 35 million or up to 7% of the total worldwide annual

turnover for the preceding financial year, whichever is higher. In addition to these fines, the AI Act also stipulates a range of other administrative fines.

Next steps

Now that the final text of the AI Act has been adopted, key upcoming milestones include the enforcement of prohibitions against unacceptable risks associated with AI systems starting in late 2024. By mid-2025, enforceable obligations concerning general-purpose AI will begin and by Spring 2026, the entire AI Act will come into full effect.

Organisations should promptly review the AI systems they currently use to determine the category these systems come under according to the AI Act. Moreover, if an AI governance framework is already in place, organisations should ensure it aligns with the AI Act's standards and adheres to the best industry practices. If such a framework is not yet established, organisations need to develop one. In addition to governance frameworks, it is essential for organisations to have robust data governance to manage and secure the data used by AI systems effectively. Companies must also evaluate their third-party risk management processes, enhancing them as necessary to meet the AI Act's stringent requirements.

Authors

Nicholai Pfeiffer

Managing Partner
White Label Consultancy
np@whitelabelconsultancy.com

André Arnes

Partner, Head of Cyber Security
White Label Consultancy
aa@whitelabelconsultancy.com

Arina Kostina

Consultant, Data Protection
White Label Consultancy
ako@whitelabelconsultancy.com

Meredith Primrose Jones

Senior Consultant, Cyber Security
White Label Consultancy
mjo@whitelabelconsultancy.com

Norman Aasma

Associate, Data Protection
White Label Consultancy
noa@whitelabelconsultancy.com

Alisa Mujanic

Senior Consultant, Cyber Security
White Label Consultancy
amu@whitelabelconsultancy.com

Marie Kristine Reyes

Associate, Data Protection
White Label Consultancy
mkr@whitelabelconsultancy.com

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

WHITELABELCONSULTANCY.COM