BCLP. Client Intelligent

Insights

DATA AND CYBERSECURITY - EUROPEAN UNION LEGISLATION AND PROPOSALS

Nov 30, 2023

SUMMARY

The pace of new EU law continues unabated, with IoT, cyber security and digital services being key areas of activity. The BCLP Data Privacy & Security team is tracking EU law developments relevant to data and cyber security. In our tracker we (1) provide a snapshot, (2) explain who is impacted and (3) confirm the status and timeline for each of: the Digital Services Act, the Digital Markets Act, the Data Governance Act, the Data Act, the NIS2 Directive, the Cybersecurity Act and the Cybersecurity Resilience Act.

DIGITAL SERVICES ACT

The Digital Services Act (*Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services*) ("**DSA**") imposes obligations on providers of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content.

The DSA aims to ensure a safer and more open digital space for users and a level playing field for companies.

The obligations increase cumulatively depending on the provider's size and the nature of their activities, with "very large online platforms" ("**VLOPs**") and "very large online search engines" ("**VLOSEs**") having the most stringent obligations, as explained below.

MORE INFORMATION

WHO DOES IT APPLY TO?

The DSA applies to a wide range of online intermediaries (**providers of information society intermediary services)**, including internet service providers, cloud service providers, messaging

service providers, marketplaces, and social networks.

Specific due diligence obligations apply to **hosting services**, and in particular to online platforms, such as **social networks, content-sharing platforms, app stores, online marketplaces,** and **online travel and accommodation platforms**.

Online platforms and online search engines with at least 45 million monthly active users in the EU (representing 10% of the EU's population) are categorised as VLOPs and VLOSEs respectively. The first VLOPs and VLOSEs were designated on 25 April 2023, with the Commission identifying 17 VLOPS and 2 VLOSEs who currently reach the relevant monthly user threshold.

The most far-reaching rules in the DSA apply to VLOSEs and VLOPs. These include:

- requirements to identify and remove **illegal content**,
- restrictions on the **use of misleading user interfaces** that hamper users from making free and informed decisions (for example, through the use of "**dark patterns**" and “nudging” practices that manipulate users' choices),
- requirements to **enhance the transparency of online advertising** (including provision of more information to users and the ability to opt-out from recommendation systems based on profiling),
- increased **protection for children** using these online services (including a ban on targeted advertising based on profiling), and
- requirements to carry out **annual risk assessments** and report these to the Commission.

ENFORCEMENT

EU member states are required to designate competent (national) authorities to be responsible for the supervision of intermediary service providers and to enforce the DSA. However, the European Commission (**Commission**) is the primary regulator for VLOPs and VLOSEs.

Designated regulators under the DSA have extensive investigatory and enforcement powers, with the Commission having the right to impose fines of up to **6%** of the provider’s annual worldwide turnover in the preceding financial year for non-compliance with the DSA.

TIMING

The DSA entered into force on 16 November 2022. The majority of its provisions apply to service providers from **17 February 2024**. However, all online platforms, except micro and small ones (determined by staff headcount and turnover), were required to publish information about their average active service recipients by **17 February 2023**. This was to enable the Commission to

establish which service providers should be designated VLOPs and VLOSEs. VLOPs and VLOSEs must comply with their obligations under the DSA within four months of their designation, i.e. by **25 August 2023** for the first set of designated VLOPs and VLOSEs.

FURTHER INFORMATION

- Legislation
- Q&A

DIGITAL MARKETS ACT

The Digital Markets Act (*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*) ("**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.

Examples include prohibiting gatekeepers from:

- **self-preferencing**: ranking their own products or services in a more favourable manner compared to those of third parties; and
- **combining and cross-using an end user's personal data** collected through their platform with personal data acquired from other services offered by them or third parties unless the user has given specific consent.

Gatekeepers will also be required to facilitate effective portability for data generated through their platform and to provide advertisers with transparent information regarding performance data and marketing-related pricing. For further information on the DMA, refer to our "10 Things you need to know about the Digital Markets Act" publication from BCLP's Antitrust & Competition team.

MORE INFORMATION

WHO DOES IT APPLY TO?

The DMA applies to companies that are designated as "gatekeepers" for one or more of the "core platform services" ("**CPSs**") listed in the DMA (for example, app stores, online search engines, social networking services, video-sharing platform services and cloud computing services).

There are three main, cumulative criteria that qualify a company as a "gatekeeper":

1. **A size that impacts the EU's internal market.** This is presumed where the company's annual turnover in the EEA was at least EUR 7.5 billion in each of the last three financial years or its average capitalisation or fair value was at least EUR 75 billion in the last financial year, and it provides services in at least three EU member states.

2. **The control of an important gateway for business users towards final consumers.** This is presumed if the company operates a CPS that has more than 45 million monthly active EU end users and more than 10,000 yearly active EU business users in the last financial year; and

3. **An entrenched and durable position.** This is presumed if the company met the above criteria in each of the last three financial years.

Companies that satisfy these criteria are presumed to be gatekeepers but can challenge the presumption and submit substantiated arguments to demonstrate that they should not be designated as a gatekeeper, despite meeting all the thresholds.

Conversely, the European Commission ("**Commission**") may launch a market investigation to assess a given company's specific situation and designate it as a gatekeeper on the basis of a qualitative assessment, even if it does not meet the quantitative thresholds.

ENFORCEMENT

The Commission will be the sole enforcer of the DMA (though there will be cooperation with national authorities) and the Commission has various enforcement powers under the act, including investigatory powers, and the ability to require remedies or to impose penalties to ensure compliance (including fines of up to **20%** of a company's worldwide annual turnover for repeated infringements).

Third parties can also pursue gatekeepers for failure to comply with the DMA and seek damages for such infringements.

TIMING

The DMA entered into force on **1 November 2022** and started to apply on **2 May 2023**. By **3 July 2023**, potential gatekeepers must notify their CPS(s) (core platform services) to the Commission if they meet the thresholds established by the DMA.

The Commission has 45 working days from receipt of such notification to make an assessment whether the company in question meets the thresholds and, if so, to designate them as a gatekeeper (**6 September 2023** is the latest date for such a designation). Following their designation, gatekeepers will then have six months to comply with the requirements in the DMA, at the latest by **6 March 2024**.

FURTHER INFORMATION

- Legislation
- Q&A
- 10 Things you need to know about the Digital Markets Act

DATA GOVERNANCE ACT

The Data Governance Act (*Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance*) ("**DGA**") aims to bolster the data economy by encouraging **public sector bodies** to share certain categories of protected data (e.g. personal data and commercially confidential data) and promote data altruism.

It seeks to do this by: (i) establishing conditions for the re-use of protected data held by public bodies; (ii) creating a new business model for data intermediary services who will provide the infrastructures for such data to be hosted, accessed, shared and exchanged; (iii) introducing a mandatory registration requirement and supervisory framework for providers of such data intermediary services; and (iv) providing for frameworks at a national level for the voluntary registration of entities that collect and process data provided for altruistic purposes and for the establishment of a European Data Innovation Board.

The DGA does not, however, create any obligation on public sector bodies to allow the re-use of data, nor does it release them from their confidentiality and data protection obligations under EU or national law.

MORE INFORMATION

WHO DOES IT APPLY TO?

The DGA applies to public sector bodies that grant rights to re-use data, the recipients of such rights, providers of data intermediation services and recognised data altruism organisations. Non-EU entities offering services into the EU which qualify as data altruism organisations or as data intermediaries under the DGA must appoint a legal representative in one of the Member States where those services are offered.

ENFORCEMENT

EU member states are required to appoint competent authorities to support the activities of public sector bodies allowing the re-use of data and also to monitor the compliance of data intermediation services providers and recognised data altruism organisations. Competent authorities are empowered to take certain actions in the event of infringement including, with respect to data

intermediation services providers, requiring the suspension or cessation of data intermediation service or imposing financial penalties.

The level of financial penalties is not set out in the DGA and is left for individual member states to determine; however, the DGA requires them to be "proportionate, effective and dissuasive".

TIMING

The DGA entered into force on **23 June 2022** and applies from **24 September 2023**.

FURTHER INFORMATION

- Legislation

DATA ACT

The European Commission ("**Commission**") adopted its proposal for a Regulation (*Regulation on harmonised rules on fair access to and use of data COM/2022/68*) ("**Data Act**") on 23 February 2022. Together with the Data Governance Act ("**DGA**"), it aims to promote the flow of data within the EU. While the DGA creates the processes and structures to facilitate data sharing, the Data Act is intended to clarify who can create value from data and under what conditions.

It is aimed at unlocking the value of data generated by connected objects in Europe (the internet of things or "**IoT**"), one of the key areas for innovation in the coming decades. The Data Act clarifies who can create value from such data and under which conditions.

The Data Act includes:

- Measures to allow users of connected devices to access data generated by the device and share it with third parties to enable other services to be provided. It maintains incentives formanufacturers to continue investing in high-quality data generation, by covering their transfer-related costs and preventing use of shared data where this would be in direct competition with the manufacturer's product.
- Measures to protect SMEs from unfair contractual terms relating to data sharing, imposed by parties with a significantly stronger bargaining position. Model contractual terms will also be produced by the Commission in order to help such companies to draft and negotiate fair data-sharing contracts.
- Means for public sector bodies to access and use private sector-held data where there is an exceptional need, particularly in cases of public emergency or to implement a legal mandate.
- New rules allowing customers to switch effectively between different cloud data-processing services providers and safeguarding against unlawful data transfers by such providers.

MORE INFORMATION

WHO DOES IT APPLY TO?

The Data Act applies to:

- manufacturers of connected products and suppliers offering related services (such as digital services or software which are incorporated into a connected product) in the EU;
- "data holders", who have the right or obligation to make data from such products and services available; and
- business and public sector bodies to whom such data is made available, i.e. "data recipients".

ENFORCEMENT

The Data Act will be enforced at a national level. Competent authorities will have investigatory powers and also the power to issue financial penalties. The level of such penalties will also be set at a national level.

TIMING

The final text of the EU Data Act was adopted on 27 November 2023. The Data Act will enter into force on the 20th day following its publication in the Official Journal and will become applicable 20 months after its entry into force.

FURTHER INFORMATION

- Legislation
- Q&A
- Procedure tracker

NIS 2 DIRECTIVE

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* ("**NIS 2**") reforms and repeals Directive (EU) 2016/1148 ("**NIS**") and aims to create a higher, common level of cybersecurity in the EU. It will require companies to comply with more stringent security requirements, put governance structures in place to manage cybersecurity, comply with breach reporting obligations, and monitor supply chains for cybersecurity risk.

MORE INFORMATION

WHO DOES IT APPLY TO?

NIS 2 broadens the scope of NIS and applies to all “essential” and “important” entities, i.e. those operating, respectively, in a high criticality sector or other critical sector (as set out in the table below), which meet the size-cap rule and provide their services, or carry out their activities, within the EU.

High criticality sectors (essential entities)

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (B2B)
- Public administration
- Space

Other critical Sectors (important entities)

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemical products
- Production, processing and distribution of food
- Manufacturing
- Digital providers

- Research

Avoiding overlap with sector-specific acts

The relevant provisions of NIS 2 will not apply to entities who are already subject to sector-specific EU legal acts (for example, the Regulation on digital operational resilience for the financial sector ("**DORA**")) where these require in-scope entities to adopt cybersecurity risk management measures or to notify regulators of significant incidents, and such requirements are at least equivalent in effect to the obligations laid down in NIS 2.

Impact on out of scope entities

The enhanced requirements under NIS 2 for in-scope entities to address risks in their ICT supply chains, mean that some businesses outside the direct scope of NIS 2 will also be impacted by it. This is likely to be seen in relation to the due diligence and contractual requirements that such suppliers are subjected to when engaging with in-scope entities.

ENFORCEMENT

NIS 2 provides competent national authorities with greater powers to supervise and sanction in-scope entities. These apply differently depending on whether an entity is an "essential" or "important" entity.

Essential entities are subject to a proactive supervisory regime, with national authorities empowered to carry out random inspections, regular and ad hoc audits, and security scans to check for vulnerabilities, as well as having the ability to request certain information and evidence of compliance.

Important entities, on the other hand, are only subject to supervisory action in the event of evidence or indications of non-compliance.

NIS 2 imposes an obligation on member states to ensure that competent national authorities are given specific, minimum enforcement powers, including on-site inspection, off-site supervision and audit rights, and uniform fine thresholds for breaches, up to a maximum of **EUR 10 million or 2%** of global annual turnover for essential entities and **EUR 7m or 1.4%** of global annual turnover for important entities.

TIMING

NIS 2 came into force on **16 January 2023** and EU member states have until **17 October 2024** to transpose NIS 2 into national law. NIS 2 is a directive, and requires implementation into each member state's national law in order to have effect. This can be contrasted with the various European Commission acts referred to on this page (which have direct effect).

FURTHER INFORMATION

- Legislation
- FAQs

CYBERSECURITY ACT

The EU Cybersecurity Act (*Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification*) (the "**CSA**") is an EU regulation that came into force on 27 June 2019, repealing the previous EU Cybersecurity Act (*Regulation (EU) 526/2013*).

THE REGULATOR

The CSA strengthens the EU Agency for cybersecurity ("**ENISA**"). It grants a permanent mandate and provides ENISA with more resources and responsibilities.

ENISA has adopted a key role in establishing and maintaining the European cybersecurity certification framework. Its functions include preparing the technical ground for specific certification schemes and informing the public on those certification schemes and the certificates issued. ENISA is also mandated to increase operational cooperation at EU level, assisting EU member states who wish for it to handle their cybersecurity incidents. ENISA also assists in supporting cross-EU collaboration in the case of large scale, multi-jurisdictional cyber-attacks and crises.

CERTIFICATION SCHEMES

The CSA introduces an EU wide cybersecurity certification framework for information and communications technology ("**ICT**") products, services and processes. Three levels of security (referred to as "assurance levels") are specified, these being (i) basic, (ii) substantial, or (iii) high. These levels define the resiliency of a product, service or process against cyber-attacks involving a certain level of skill and resources.

Companies doing business in the EU are only required to certify their ICT products, services and processes on one occasion, following which they may receive a mutually recognised certificate that can be used throughout the EU. The CSA requires all EU member states to identify at least one national cybersecurity certification authority.

MORE INFORMATION

WHO DOES IT APPLY TO?

The CSA offers businesses the opportunity to certify that their products meet EU cybersecurity standards. While CSA certification is voluntary unless otherwise specified in national or EU law, several EU legislative proposals including the NIS 2 Directive, AI Act and Cyber Resilience Act require the EU Commission to specify the obligations for CSA certification under those laws.

TIMING

The CSA was originally enacted on 27 June 2019, following which it became directly applicable in all EU member states.

Articles 58 (*National cybersecurity certification authorities*), 60 (*Conformity assessment bodies*), 61 (*Notification*), 63 (*Right to lodge a complaint*), 64 (*Right to an effective judicial remedy*) and 65 (*Penalties*) of the CSA came into force on 28 June 2021.

On 18 April 2023, the European Commission proposed an amendment to enable the future adoption of European certification schemes for "managed security services" covering areas such as security audits, incident response, penetration testing and consultancy. The European Parliament and the Council will now consider this targeted amendment to the CSA.

FURTHER INFORMATION

- Legislation
- FAQs

CYBER RESILIENCE ACT (PROPOSED)

The European Commission adopted its proposal for an EU Cyber Resilience Act (*Regulation (EU) 2022/0272 of the European Parliament and of the Council of 15 September 2022 on horizontal cybersecurity requirements for products with digital elements*) on 15 September 2022 (the "**CRA**"). The CRA introduces cybersecurity requirements for "products with digital elements", with the intention of better securing hardware and software products in the EU. The proposed regulation aims to address four specific objectives:

- ensure that *manufacturers improve the security of products with digital elements* since the design and development phase and throughout the whole life cycle;
- ensure a *coherent cybersecurity framework*, facilitating compliance for hardware and software producers;
- enhance the *transparency of security properties* of products with digital elements, and
- enable businesses and consumers to *use products with digital elements securely*.

MORE INFORMATION

WHO DOES IT APPLY TO?

The CRA proposes minimum cybersecurity requirements for (i) manufacturers, (ii) importers, and (iii) distributors of "products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network". Manufacturers will face the largest compliance burden.

A "**product with digital elements**" is "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed in the market separately". Certain products (e.g. those developed for national security or military purposes), will be excluded. Also excluded are medical devices subject to the EU Medical Devices Regulation (2017/745).

In-scope products will need to satisfy essential security requirements (e.g. technical standards and additional governance obligations) when being placed on the market and thereafter. The essential security requirements will oblige manufacturers to account for cybersecurity throughout the product lifecycle (i.e. design, development and production), exercise due diligence on security aspects in the creation of their products, ensure transparency regarding cybersecurity factors that need to be known by customers, provide proportionate support on security (e.g. via software updates) and comply with the CRA's vulnerability handling requirements.

A *cybersecurity risk assessment* must be completed to ensure cybersecurity "by design" from the outset, with identified risks being accounted for throughout the product lifecycle. In addition, manufacturers will be required to complete a conformity assessment to demonstrate whether specified requirements have been fulfilled, with products considered "critical" being subject to stricter assessment rules requiring the input of third party bodies.

Manufacturers must also draw up *technical documentation* as specified in the CRA and have a *vulnerability handling process* established before products with digital elements are made available on the EU market (for the lifespan of the product or a period of 5 years from the product being placed on the market, whichever is shorter), among other requirements.

Manufacturers will be subject to **strict reporting obligations** and must notify ENISA within 24 hours upon becoming aware of (i) any actively exploited vulnerability contained in the product with digital elements, and (ii) any incident having impact on the security of the product with digital elements. Manufacturers are also required to notify users of the product about the incident and, where necessary, any corrective measures that the user can deploy.

Importers and distributors that identify vulnerabilities are required to inform the manufacturer without undue delay.

Importers may only import products that comply with the CRA's minimum obligations, and are required to take steps to verify this.

Distributors are subject to the less prescriptive requirement to act "with due care in relation to the requirements" of the CRA.

ENFORCEMENT

Entities that do not comply with the CRA may be subject to maximum fines of up to 15,000,000 EUR or, if the offender is an undertaking, up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

TIMING

The proposal is **currently being reviewed** by the EU Parliament and the Council, as part of the EU's legislative process. Once adopted, economic operators and member states will have a transitional two year period to comply with the CRA's requirements and undertake the necessary conformity assessments.

FURTHER INFORMATION

- Proposal

AI ACT (PROPOSED)

Read our commentary on the draft EU Artificial Intelligence Act.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483
