Global Data and Cyber Handbook - EU

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

2024 has seen major changes to the EU legislative framework for data and cyber, and 2025 promises to showcase a couple of further interesting legal developments.

The **Data Act** entered into force in January 2024 and mostly applies from 12 September 2025, except for specific provisions that apply at a later stage. The Data Act contains provisions regarding the access, use, making available and sharing of data (both personal and non-personal data) generated by the use of connected products and related services.

The **EU AI Act** was adopted in July 2024, with the first obligations taking effect in February 2025. The EU AI Act provides for graduated regulation of AI products based on risk categories: it prohibits certain technologies and imposes obligations on technology producers and deployers based on the risk category into which the AI product falls, and provides an important additional layer of regulation where personal data is processed by AI technologies.

The implementation deadlines for both the **NIS 2 Directive** (which broadens the scope of application and also extends the relevant obligations in comparison to NIS) and the **Critical Entities Resilience Directive** (which strengthens the resilience of critical entities) passed in October 2024. National implementing legislation is already in force in some jurisdictions, although many jurisdictions have not yet passed their implementing legislation.

The **Cyber Resilience Act (“CRA”)** has been published on 20 November 2024. The CRA will enter into force on 10 December 2024 and will be mostly applicable from 11 December 2027 with some provisions applying at an earlier stage. The CRA will introduce new obligations on manufacturers of products with digital elements designed to ensure the cybersecurity of such products.

The **Data Governance Act** is applicable since 24 September 2023., The prohibition on exclusive agreements for use of public sector data (except in limited circumstances) will take effect on 24 December 2024.

The **Political Advertising Regulation** has also been adopted on 13 March 2024 and will be mostly applicable from 10 October 2025, with some provisions applying since 9 April 2024. It lays down certain rules and requirements, including transparency and due diligence obligations, for the provision of political advertising and related services as well as on targeting techniques and ad-delivery techniques involving personal data processing in the context of online political advertising provision.

The **Digital Operational Resilience Act (“DORA”)** will also mostly apply from 17 January 2025. It sets forth uniform requirements concerning the security of network and information systems supporting the business processes of financial entities.

It is expected that that the **European Health Data Space Regulation**, on which a political agreement has been reached,will be published and enter into force later in 2025.

In 2025, it is anticipated that the **GDPR Enforcement Procedures Regulation** will either be adopted, or at the very least, reach the final stages of the legislative process.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: January 2025*

☒ omnibus — all data

☒ sector-specific — e.g., financial institutions, governmental bodies

## What are the key data privacy laws and regulations?

*Last review date: January 2025*

*This chapter provides information on the position under European Union law and guidance. For information on implementation in specific jurisdictions, see the relevant individual chapter.*

[EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679)

[Directive 2002/58/EC](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (“**e-Privacy Directive**”)

[Regulation (EU) 2024/900](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202400900#fnp_1) of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (“**Political Advertising Regulation**”)

## What are the key cybersecurity laws and regulations?

*Last review date: January 2025*

*This chapter provides information on the position under European Union law and guidance. For information on implementation in specific jurisdictions, see the relevant individual chapter.*

[Regulation (EU) 2019/881](https://eur-lex.europa.eu/eli/reg/2019/881/oj) 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 and repealing Regulation (EU) No 526/2013 ("**Cybersecurity Act**")

[Regulation (EU) No 910/2014](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (“**eIDAS Regulation**”)

[Directive (EU) 2022/2555](https://eur-lex.europa.eu/eli/dir/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 (EU) 2016/1148 (“**NIS 2 Directive**”)

[Commission Implementing Regulation](https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks) of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (“**Commission NIS 2 Implementing Regulation**”)

[Regulation (EU) 2024/2847](https://eur-lex.europa.eu/eli/reg/2024/2847/oj) of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)(“**Cyber Resilience Act**”)

[Regulation (EU) 2022/2554](https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554) 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) 2016/1011 (Digital Operational Resilience Act – “**DORA**”)

[Directive (EU) 2022/2557](https://eur-lex.europa.eu/eli/dir/2022/2557/oj) of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (“**Critical Entities Resilience Directive**”)

[Directive (EU) 2015/2366](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366) of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (“**PSD2 Directive**”)

## What are the key laws and regulations relating to non-personal data?

*Last review date: January 2025*

*This chapter provides information on the position under European Union law and guidance. For information on implementation in specific jurisdictions, see the relevant individual chapter.*

[Regulation (EU) 2018/1807](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807) of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

[Regulation (EU) 2022/868](https://eur-lex.europa.eu/eli/reg/2022/868) of the European Parliament and of the Council of 30 May 2022 on European data governance (“**Data Governance Act**”)

[Regulation (EU) 2023/2854](https://eur-lex.europa.eu/eli/reg/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 (“**Data Act**”)

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: January 2025*

*This chapter provides information on the position under European Union law and guidance. For information on implementation in specific jurisdictions, see the relevant individual chapter.*

New data- and cyber-related legislation was enacted in the European Union in recent years that will come into force, or be implemented in Member States, in 2025 and beyond.

The Digital Operational Resilience Act ("**DORA"**), which lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities, entered into force in January 2023, and includes a two-year implementation window with the new rules mostly taking effect on 17 January 2025.

Obligations imposed by the **EU AI Act**, **Data Governance Act** and the **NIS2 Directive** and **Critical Entities Resilience Directive** (as implemented into national laws) will continue to take effect throughout 2025. The obligations under the **Cyber Resilience Act** largely take effect from 2026 onwards, but the Commission should further specify in-scope products before the end of 2025. The **Data Act** will take effect from September 2025.

The **Political Advertising Regulation**, which will be mostly applicable from 10 October 2025, lays down specific rules and requirements on personal data processing in the context of the provision of online political advertising.

There is further data- and cyber-related legislation pending in the EU.

A proposal for an [**ePrivacy Regulation**](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&amp;reference=2017/0003(COD)) has been pending at a European level since 2017 to adapt rules for electronic communications to the GDPR and to strengthen privacy protection online. If enacted, it would introduce reforms to the EU law on areas such as direct marketing, cookies and similar technologies and electronic communications data. However, progress has been slow in comparison to other major EU digital files of the EU’s data strategy.

In relation to EU-US data transfers, in July 2023 the European Commission adopted its adequacy decision for the [**EU-U.S. Data Privacy Framework**](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en). On the basis of this adequacy decision, personal data can flow from EU companies to US companies participating in the EU-U.S. Data Privacy Framework, without the need for an additional transfer mechanism to be implemented. The first review of the EU-U.S. Data Privacy Framework was completed in [October 2024](https://commission.europa.eu/document/download/25695177-8073-4ce3-bf81-eb816dc6b468_en?filename=Report%20on%20the%20first%20periodic%20review%20of%20the%20functioning%20of%20the%20adequacy%20decision%20on%20the%20EU-US%20Data%20Privacy%20Framework.pdf) and concluded that the U.S. authorities have put in place the necessary structures and procedures to ensure that the Data Privacy Framework functions effectively. The adequacy decision is being challenged in the courts.

The [**European Health Data Space Regulation**](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197), on which the Council of the EU and the European Parliament reached political agreement in spring 2024, is currently pending formal adoption at EU level and it is anticipated to enter into force in 2025. It seeks to create a common space for health data within the EU and establishes harmonised rules on the primary and secondary use of electronic health data.

In June 2023, the European Commission put forward a proposed **framework for Financial Data Access (“FIDA”)** that aims to open the access of financial institutions to each other’s customer data. The Council of the EU reached agreement on its position in [December 2024](https://www.consilium.europa.eu/en/press/press-releases/2024/12/04/capital-markets-union-council-agrees-to-make-consumers-financial-data-more-accessible/#:~:text=The%20FIDA%20framework%20complements%20the,on%20FIDA%20in%20April%202024.) and the final shape of the legislation will now be negotiated with the European Parliament.

The draft [**GDPR Enforcement Procedures Regulation**](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0348) is expected to either be adopted, or at the very least, reach the final stages of the legislative process end of 2024 or beginning 2025. The aim of this Regulation is to lay down harmonized rules for cross-border data protection cases, especially cross-border complaints and investigations initiated *ex officio* by data protection authorities.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: January 2025*

The **data privacy regulators** in the EU are primarily **national data protection authorities**. These are independent public authorities that supervise the application of data protection laws, provide expert advice and guidelines on data protection issues, and handle complaints lodged against violations of the General Data Protection Regulation (GDPR) and relevant national laws. Additionally, the **European Data Protection Board (EDPB)**, which gathers representatives of all EEA data protection authorities, oversees the consistent application of data protection rules across the EU (notably by elaborating guidelines) and facilitates cooperation between national data protection authorities. The EDPB should not be confused with the **European Data Protection Supervisor (EDPS)** which is the EU’s independent data protection authority. Its main role is to supervise the data processing activities of the EU institutions and bodies and to advise these on all matters relating to personal data processing, including on relevant legislative proposals.

With respect to **non-personal data**, Regulation 2018/1807 on the free flow of non-personal data does not establish specific regulators for non-personal data. The oversight of these rules is therefore handled by **national competent authorities** which work in coordination with the European Commission to ensure compliance and address any issues related to the free flow of non-personal data.

Additionally, under the Data Governance Act and the Data Act, which apply to both personal and non-personal data, each EU Member State is required to designate one or more **competent authorities** responsible for enforcing the respective regulations. A **European Data Innovation Board (EDIB)** has also been established by the Data Governance Act to support the consistent application of both the Data Governance and the Data Acts, notably by issuing relevant guidance, advising and assisting the European Commission on the implementation of these regulations and facilitating cooperation between competent authorities.

Cybersecurity is regulated by several key authorities in the EU:

**European Union Agency for Cybersecurity (ENISA)**: ENISA is an EU agency that provides support to EU Member States, EU institutions, and businesses in key cybersecurity areas, including the implementation of the NIS 2 Directive;

N**ational Cybersecurity Certification Authorities**: under the EU Cybersecurity Act, each Member State must appoint one or more national cybersecurity certification authorities which supervise, and enforce the rules of the European cybersecurity certification schemes;

**National competent authorities** that have been designated by Member States to supervise compliance with and enforce the eIDAS Regulation, the NIS 2 Directive and the Critical Entities Resilience Directive with different **Cooperation Groups** (consisting notably of representatives of national authorities) being established to notably facilitate cooperation between national authorities and elaborate guidance with a view to ensure consistent application of the different cybersecurity frameworks.

Under the EU AI Act, enforcement is spread across three different levels:

**National enforcement** through **national competent authorities** whose tasks include supervising the application and implementation of the AI Act as well as carrying out market surveillance activities;

**EU-wide enforcement** through the European Commission’s **AI Office** - whose tasks include contributing to fostering standards and testing practices and enforcing specific cross-border cases - and the **AI Board** which will act as a coordination platform among the national competent authorities and as an advisory body to the European Commission;

**Stakeholder involvement** with a **scientific panel of independent experts** to advise the AI Office about general-purpose AI models and an **advisory forum for stakeholders** to provide technical expertise to the AI Board and the European Commission.

## How active is each of the regulator(s)?

*Last review date: January 2025*

Very active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: January 2025*

*This chapter provides information on the position under European Union law and guidance. For information on implementation in specific jurisdictions, see the relevant individual chapter.*

A huge number of regulators are involved in the enforcement of EU data and cyber legislation. National regulatory priorities are described in individual country chapters and we have summarized the priorities of two key regulators – the EDPB and ENISA – here.

The key priorities of the European Data Protection Board, as set out in its [2024/2025 work program](https://www.edpb.europa.eu/about-edpb/what-we-do/strategy-work-programme_en), are:

Enhancing harmonisation and promoting compliance

Reinforcing a common enforcement culture and effective cooperation

Safeguarding data protection in the developing digital and cross-regulatory landscape

Contributing to the global dialogue on data protection

Key concrete actions relevant to private sector organisations include:

the development of further guidance on topics including anonymisation and pseudonymisation, legitimate interests, children’s data, “consent or pay” models, processing of data for scientific research purposes, data subject rights under the LED, and age verification criteria;

issuing opinions on accreditation requirements for monitoring bodies of codes of conduct and for certification bodies, and on codes of conduct and on certification criteria , including the European Data Protection Seal;

establishing common positions and guidance in the cross-regulatory landscape on topics including the interplay between EU data protection law and other EU laws, guidelines on the processing of personal data to target or deliver political advertisements, and transfers of personal data in the context of crypto assets;

monitoring and assessing new technologies, including guidelines on generative AI and data scraping, telemetry and diagnostic data, and blockchain; and

providing further guidance on practical implementation of data transfer mechanisms.

Priorities of the European Union Agency for Cybersecurity (ENISA), as set out in its [2024-2026 program](https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA-Single%20Programming%20Document%202024-2026_Condensed_online_1.pdf), include:

combatting attempts to destroy critical infrastructures and render them unavailable, thus impacting the target’s resilience, or to dissuade and manipulate public opinion through misinformation and information manipulation;

enhancing its proactive capabilities, to better support MSs in their efforts to respond to cyber threats and incidents while providing them with knowledge and expertise and increasing preparedness in key sectors;

strengthening its capabilities and capacities in supporting MSs with the implementation of NIS2; and

launching a review of ENISA strategy and adopting the first ever state of cybersecurity in the EU report under Article 18 of NIS2.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: January 2025*

Are **regulatory investigations or direct enforcement activity by data or cyber regulators**:

☒   Common

If applicable, are they:

☒   Increasing

Are **class actions/group actions under data or cyber regulation**:

☒   Rare

If applicable, are they:

☒   Increasing

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: January 2025*

There are:

☒   administrative remedies /civil penalties applied by regulators and law enforcement

☒   criminal penalties from regulators and law enforcement

☒   private remedies

## If data subjects have private remedies, what form can these remedies take?

*Last review date: January 2025*

☒   individual personal actions

☒   representative actions (e.g., brought by a consumer/data privacy body or the supervisory authority)

# Key Definitions

## Personal data

*Last review date: January 2025*

"Personal data" means any information relating to an identified or identifiable natural person. An "identifiable person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: January 2025*

Sensitive data includes:

☒   personal data revealing racial or ethnic origin
☒   personal data revealing political opinions
☒   personal data revealing religious or philosophical belief
☒   personal data revealing trade / professional union or association membership
☒   genetic data
☒   biometric data for the purpose of uniquely identifying a natural person or biometric templates
☒   data concerning health/medical information
☒   data concerning a natural person's sex life or sexual orientation
☒   government identity card or number information
☒   personal data regarding an individual's criminal convictions or record
☒   other

For some Member States a broader scope of sensitive/special personal data may apply.

## Controller vs Processor

*Last review date: January 2025*

**Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:**

the controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Yes**

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: January 2025*

☒   applies to organizations located in the jurisdiction
☒   applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction
☒   applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
☒   other

The CRA and Political Advertising Regulation apply irrespective of the location of the organization.

The CRA applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

The Political Advertising Regulation applies to political advertising where the political advertisement is disseminated in the Union, is brought into the public domain in one or several Member States or is directed to Union citizens.

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: January 2025*

Yes

The following are potential legal bases for processing personal data:

☒   the data subject has provided consent to the processing for the identified purposes
☒   the personal data is necessary to perform a contract with the data subject
☒   the personal data is necessary to comply with a legal obligation
☒   the personal data is necessary to protect the vital interests of a natural person
☒   the personal data is necessary for a public interest
☒   the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)
☒   other

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: January 2025*

Yes

The following are potential legal bases for processing special categories of personal data:

☒   the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")
☒   processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
☒   processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
☒   processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions
☒   processing relates to personal data which are manifestly made public by the data subject
☒   processing is necessary for the establishment, exercise or defense of legal claims
☒   processing is necessary for reasons of substantial public interest
☒   processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
☒   processing is necessary for reasons of public interest in the area of public health
☒   processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
☒   other

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: January 2025*

Yes

## In what circumstances do these special requirements apply?

*Last review date: January 2025*

Generally

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: January 2025*

☒   consent must be given or authorized by the holder of parental responsibility over the child
☒   additional data subject rights are granted to minors (e.g., deletion, access, transparency)
☒   additional data security requirements apply
☒   other

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: January 2025*

☒   the identity and the contact details of the controller and, where applicable, of the controller's representative
☒   the contact details of the data protection officer, where applicable
☒   the purposes of the processing for which the personal data is intended
☒   the legal basis for the processing
☒   the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground
☒   the recipients or categories of recipients of the personal data, if any
☒   information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available
☒   the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
☒   the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.
☒   the existence of the right to withdraw consent if processing is based on consent
☒   the right to lodge a complaint with a supervisory authority
☒   whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
☒   if applicable, information regarding automated decision making, including profiling
☒   other

The requirement to include information in the privacy notice on the categories of personal data concerned and the source from which the personal data originates only apply if the data is collected indirectly.

The obligation to provide information on the existence of data subjects’ rights requires the provision of information on the existence of all data subjects’ rights, (i.e., the right to access, rectification, erasure, data portability, restriction on processing, objection to processing) with a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right.

The privacy notice must explain that data subjects have the right to withdraw consent at any time if the processing is based on consent.

Providing information on the security provided to the data is good practice, but not mandatory.

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: January 2025*

Yes

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒   right to access the data subject's own personal data

☒   right to rectify/correct the data subject's own personal data where inaccurate or incomplete

☒   right to erasure of personal data

☒   right to restrict data processing

☒   right to data portability

☒   right to object to the processing of personal data

☒   right to withdraw consent

☒   other

The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject;  right to transparent information (which, in practice, is an obligation of the data controller to provide such transparent information about its data processing activities).

We also note, pursuant to recital (27) of Regulation (EU) 2016/679 (GDPR), that although the GDPR does not apply to deceased persons, Member States of the European Union may establish local rules regarding the processing of personal data of deceased persons (e.g., specific rights that close relatives may exercise relative to such deceased persons’ personal data). Furthermore, the data subject also has the right to lodge a complaint with the competent data protection supervisory authority and make civil claims against the data controller and/or the data processor regarding alleged breaches of the GDPR; however, such rights cannot be operationalized, because the data subject does not exercise them by way of contacting the data controller or the data processor.

## Are there accountability and governance requirements?

*Last review date: January 2025*

Yes

There are accountability and governance requirements to:

☒   take privacy by default and design measures for all processing of personal data

☒   perform and document data protection impact assessments (DPIAs) for high-risk processing:

☒   maintain a record of processing activities

☒   implement appropriate measures to comply with data privacy and cybersecurity

☒   demonstrate compliance with data privacy and cybersecurity

☒   identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

☒   provide training to employees

☒   audit or supervise data processors

☒   appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: January 2025*

Yes

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

*Last review date: January 2025*

Yes

If yes, under what circumstances?

☒   the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

☒   the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

☒   the core activities of the controller or the processor consist of processing on a large scale of special categories of data

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: January 2025*

Yes

The DPO must have appropriate professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil their tasks pursuant to applicable data protection laws.

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: January 2025*

No

We note though that the following scenarios may trigger similar requirements:

When transferring personal data to a third country or an international organization, the following may be used as safeguards for such data transfers only if they are approved by a data protection supervisory authority in the EU:

binding corporate rules (Article 47 of the GDPR);

codes of conduct (Article 40 of the GDPR); and

certification mechanisms, where a data protection supervisory authority acts as the certification body; and (Article 42 of the GDPR).

Where the data controller carries out a data protection impact assessment concerning a proposed data processing activity and as a result, it concludes that in the absence of risk-mitigating measures, the proposed data processing activity would result in a high risk to the data subjects’ rights and freedoms, it must consult the competent data protection supervisory authority before it begins the proposed data processing(Article 36 of the GDPR).

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: January 2025*

Yes

The obligations are as follows:

☒   controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data

☒   controllers must only use processors subject to a written agreement that complies with specific requirements

☒   other

If the data controller is subject to the NIS2 Directive, it must aim to ensure the security of its supply chain. Such general obligation may include that that the data controller must ensure that data processors, that participate in the establishment, operation, maintenance and/or repair of the data controller’s electronic information system, maintain an appropriate level of cybersecurity relative to their services provided to the data controller. Local laws implementing NIS2 might stipulate specific obligations.

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: January 2025*

**Yes**

The following provisions apply directly to processors:

Art. 28, Art. 29, Art. 30 par. 2, Art. 31, Art. 32, Art. 33 par. 2, Art- 37-39, and Chapter V of the GDPR.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: January 2025*

Yes

Yes. Third country is not defined in the GDPR, but means countries (1) outside of the European Union, and (2) countries outside of the European Economic Area.

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

☒   approved adequate/whitelisted jurisdictions

☒   to holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and cybersecurity authority (e.g., EU-US Data Privacy Framework)

☒   approved standard contractual clauses

☒   binding corporate rules

☒   derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: January 2025*

Yes

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: January 2025*

**Email marketing**

☒   prior opt-in consent
☒prior existing business relationship (and subject to other requirements) with opt-out consent

 **Telephone marketing**

☒   prior opt-in consent

**SMS/text message marketing**

☒   prior opt-in consent

**Postal marketing**

☒   prior opt-in consent

**Online behavioral advertising targeting/social media targeting/ad personalization marketing**

☒   prior opt-in consent

Note that for telephone, SMS/text message and postal marketing, it’s also necessary to check opt-out registers, and other requirements may apply.

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: January 2025*

Yes

## Can consent be validly obtained in the employment context?

*Last review date: January 2025*

Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

There are some concerns that the consent is unlikely to be freely given in the employment context.

Pursuant to recital 43 of the GDPR "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller", which could be the case in the employment relationship.

The European Data Protection Board has indicated in its [Guidelines on Consent](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf) under the GDPR, that it "deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given". Thus, "given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent".

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

No

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: January 2025*

Yes

The restrictions or requirements are as follows:

☒   qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

☒   right to information / transparency requirement

☒   right to request human review of the automated decision making

☒   other

*This chapter provides information on the position under European Union law and guidance. For information on implementation in specific jurisdictions, see the relevant individual chapter.*

Art. 22 GDPR sets forth a qualified right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning a data subject or similarly significantly affects him or her. In this respect, "decisions producing legal effects" are those which, for example, affect someone's legal rights, such as the freedom to associate with others, to vote in an election or to take legal action, or their legal status or rights under a contract. On the other hand, for data processing to “similarly significantly affect” someone the effects of the processing must be sufficiently great or important to be worthy of attention (e.g., it has potential to significantly affect the circumstances, behavior or choices of the individuals concerned, have a prolonged or permanent impact on the data subject, or to lead to the exclusion or discrimination of individuals).

Arts. 13 and 14 GDPR require data controllers to inform data subjects of the existence of automated decisions that meet the above description, including providing meaningful information about the logic involved, as well as the significance and envisaged consequences of the processing for the data subject.

In certain cases where the data subject right laid down in Art. 22 GDPR does not apply in light of legal exceptions, Art. 22 GDPR requires data controllers to implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, which must include at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

There are also other EU data regulations that impose requirements or restrictions in relation to profiling and automated decision making. For example, AI systems used for profiling in the course of the detection, investigation or prosecution of criminal offences for law enforcement purposes are considered high-risk systems under the AI Act.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: January 2025*

**Yes**

**The exceptions are as follows:**

For instance, the right not to be subject to a decision based solely on automated processing, including profiling, laid down in Article 22 GDPR, is not applicable if, in particular, the decision (i) is necessary for entering into or performance of a contract between a data subject and a data controller, (ii) is authorized by EU or Member State law to which the data controller is subject (and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests), or (iii) is based on the data subject’s explicit consent.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: January 2025*

Yes

The EDPB has endorsed the [Guidelines on Automated individual decision-making and Profiling](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053) produced Article 29 Working Party in 2018. Additionally, it has published other more specific guidelines such as the [Guidelines 8/2020 on the targeting of social media users](https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf) and [Statement 2/2019 on the use of personal data in the course of political campaigns](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf).

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: January 2025*

☒   Enforcement activity against AI developer(s)

☒   Enforcement activity against AI user(s)/deployer(s)

☒   Enforcement activity under existing privacy law

☒   Enforcement activity by data or cyber regulator

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: January 2025*

☒   Yes, laws in force

*This chapter provides information on the position under European Union law and guidance. For information on implementation in specific jurisdictions, see the relevant individual chapter.*

The EU AI Act entered into force on 1 August 2024. From 2 February 2025, specified “prohibited systems” will be banned in the EU, and a risk-based framework of obligations for other AI systems will begin to take effect from 2025 onwards. Depending on the nature of the AI system and the way it is being used, those obligations might include a requirement for human oversight and/or transparency requirements. The use of automated decision making or profiling by AI systems may determine their classification from a regulatory perspective and the respective obligations that arise.

The Digital Services Act (Regulation 2022/2065 of 19 October 2022 on a Single Market For Digital Services - “**DSA**”), which entered into force on 17 February 2024, imposes specific restrictions on certain uses of profiling. In particular, under Art. 26 DSA, providers of online platforms may not present advertisements to recipients of the service based on profiling as defined in Art. 4 (4) GDPR using special categories of personal data referred to in Art. 9(1) GDPR. Furthermore, pursuant to Art. 28 DSA, providers of online platforms may not present advertisements on their interface based on profiling (within the meaning of Art. 4(4) GDPR) using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. Lastly, according to Art. 38 DSA, providers of very large online platforms and of very large online search engines that use recommender systems must provide at least one option for each of their recommender systems which is not based on profiling (within the meaning of Art. 4(4) GDPR).

In addition, under Art. 15 of the Digital Markets Act (Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector – “**DMA**”), within 6 months after its designation, a gatekeeper must submit to the Commission an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services listed in the designation decision. The Commission will transmit that audited description to the European Data Board.

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: January 2025*

No

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: January 2025*

It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

For example, it may be possible to argue that liability is not inherited where there is a change in the identity of the data controller and it remains a wholly distinct entity after closing, although this will need to be analyzed on a case-by-case basis. A system of representations and warranties and indemnities may be included in the asset purchase agreement.

## If so, how would any regulatory fines be calculated?

*Last review date: January 2025*

Unclear

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: January 2025*

Yes

It is likely that the acquiring entity will inherit liability for pre-acquisition data privacy or cybersecurity breaches, as there would generally be no change in the identity of the data controller. A system of representations and warranties and indemnities may be included in the share purchase agreement.

## If so, how would any regulatory fines be calculated?

*Last review date: January 2025*

Unclear

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: January 2025*

**Yes**

☒   general obligation to take appropriate / reasonable technical, physical and/or organizational security measures
☒   obligation to take specific security measures e.g., encryption
☒   requirement to undertake third party due diligence (security assessment of third party providers)

Art. 5(1)(f) and 32 GDPR impose a general obligation to take appropriate / reasonable technical, physical and/or organizational security measures.

Encryption is not a strict legal requirement, but encryption is considered by the GDPR as an appropriate technical and organizational measure.

Although undertaking processor due diligence is not a GDPR requirement as such, under Art. 28 GDPR, data controllers must only use processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the GDPR requirements.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: January 2025*

**Yes**

☒   network information security requirements (broader than telecommunications)

☒   financial services requirements

☒   providers of critical infrastructure

☒   digital or connected (IOT) products

The NIS2 Directive, via national implementing law, imposes obligations on providers or critical infrastructure to protect systems from cyberattack. The scope of NIS2 is broad and may encompass public listed companies, and companies in the health, financial services or telecommunications sectors.

DORA, as well as the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, the revised Payment Services Directive (“**PSD2**”), impose specific cyber resilience and reporting obligations on in-scope organisations in the financial services sector.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (“**European Electronic Communications Code**”) imposes detailed security requirements for electronic communication providers.

The **Cyber Resilience Act** of 25 September 2024 will introduce new obligations on manufacturers, importers and distributors of products with digital elements designed to ensure the cybersecurity of such products. The Cyber Resilience Act will take effect in stages, with the obligation to notify actively exploited vulnerabilities for in-scope products taking effect from 11 September 2026 and the remaining obligations from 11 December 2027.

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

N/A

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: January 2025*

Yes

## Controllers/Owners have to notify:

*Last updated date: January 2025*

☒   data protection authorities

☒   affected individuals

"Personal data breach" is defined under the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Under the GDPR, the controller must notify the **competent supervisory authority** of a personaldata breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The controller must notify the **data subject** of a personaldata breach if it is likely to result in a high risk to the rights and freedoms of natural persons, without undue delay, unless:

the controller has implemented appropriate technical and organisational protection measures to the personal data affected, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

## Processors/Agents have to notify:

*Last review date: January 2025*

controller/ owner

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: January 2025*

Yes

☒   cybersecurity authorities

☒   financial services requirementst

☒   providers of critical infrastructure

The NIS2 Directive, via national implementing law, imposes obligations on providers or critical infrastructure to protect systems from cyberattack and notification obligations. The scope of NIS2 is broad and may encompass public listed companies, and companies in the health, financial services or telecommunications sectors.

DORA, as well as the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, the revised Payment Services Directive (“**PSD2**”), impose specific cyber resilience and reporting obligations on in-scope organizations in the financial services sector.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (“**European Electronic Communications Code**”) imposes detailed security requirements and notification obligations for electronic communication providers.

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: January 2025*

 **No**

Regulation (EU) 2018/1807 on the framework for the free flow of non-personal data in the European Union prohibits data localization requirements unless they are justified on grounds of public security in compliance with the principle of proportionality (Art. 4). As a consequence, data localization requirements should have been repealed in the EU by 30 May 2021, unless justified under Regulation (EU) 2018/1807.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: January 2025*

☒   Obligation for public sector organizations to share or make accessible non-personal data

☒   Obligation for private organizations to share or make accessible data generated by connected or "IoT" devices

Regulation (EC) No 1049/2001 grants public access to European Parliament, Council and Commission documents, on request (if not already proactively published) and subject to a broad list of public and private interest exceptions.

In September 2023, the **Data Governance Act** took effect, and key substantive provisions apply from 24 December 2024. The Data Governance Act provides a framework to enhance trust in voluntary data sharing, and limits the ability of public sector bodies to enter into exclusive agreements for the re-use of in-scope data.

In December 2023, the **Data Act** was published in the Official Journal of the EU. It shall apply from 12 September 2025. The Data Act contains provisions regarding the access, use, making available and sharing of data (both personal and non-personal data) generated by the use of connected products and related services. Users can also ask data holders to make this data available to third parties.

In spring 2024, the European Parliament and the Council reached a political agreement on the [Commission proposal](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197) for the European Health Data Space. The proposal includes mandatory data-sharing obligations for data holders, such as private entities in the health care sector.

In June 2023, the European Commission put forward a proposed framework for Financial Data Access (**“FIDA”**) that aims to open the access of financial institutions to each other’s customer data. The Council of the EU reached agreement on its position in [December 2024](https://www.consilium.europa.eu/en/press/press-releases/2024/12/04/capital-markets-union-council-agrees-to-make-consumers-financial-data-more-accessible/#:~:text=The%20FIDA%20framework%20complements%20the,on%20FIDA%20in%20April%202024.) and the final shape of the legislation will now be negotiated with the European Parliament.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: January 2025*

☒   Obligation to share data on request

☒   Obligation to (re)design products or services to facilitate data accessibility

☒       Obligation to standardize products or services to facilitate data portability or interoperability

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.