

PANORAMIC

# DATA PROTECTION & PRIVACY

European Union



LEXOLOGY

# Data Protection & Privacy

Contributing Editors

**Aaron P Simpson and Lisa J Sotto**

Hunton Andrews Kurth LLP

**Generated on: September 5, 2025**

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2025 Law Business Research

# Contents

## Data Protection & Privacy

### LAW AND THE REGULATORY AUTHORITY

- Legislative framework
- Data protection authority
- Cooperation with other data protection authorities
- Breaches of data protection law
- Judicial review of data protection authority orders

### SCOPE

- Exempt sectors and institutions
- Interception of communications and surveillance laws
- Other laws
- PI formats
- Extraterritoriality
- Covered uses of PI

### LEGITIMATE PROCESSING OF PI

- Legitimate processing – grounds
- Legitimate processing – types of PI

### DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

- Transparency
- Exemptions from transparency obligations
- Data accuracy
- Data minimisation
- Data retention
- Purpose limitation
- Automated decision-making

### SECURITY

- Security obligations
- Notification of data breach

### INTERNAL CONTROLS

- Accountability
- Data protection officer
- Record-keeping
- Risk assessment
- Design of PI processing systems

### REGISTRATION AND NOTIFICATION

Registration  
Other transparency duties

## **SHARING AND CROSS-BORDER TRANSFERS OF PI**

Sharing of PI with processors and service providers  
Restrictions on third-party disclosure  
Cross-border transfer  
Further transfer  
Localisation

## **RIGHTS OF INDIVIDUALS**

Access  
Other rights  
Compensation  
Enforcement

## **EXEMPTIONS, DEROGATIONS AND RESTRICTIONS**

Further exemptions and restrictions

## **SPECIFIC DATA PROCESSING**

Cookies and similar technology  
Electronic communications marketing  
Targeted advertising  
Sensitive personal information  
Profiling  
Cloud services

## **UPDATE AND TRENDS**

Key developments of the past year

# Contributors

## European Union



### Simmons & Simmons

---

**Jaap Tempelman**

jaap.tempelman@simmons-simmons.com

**Camille Saettel**

camille.saettel@simmons-simmons.com

**Jérémie Doornaert**

jeremie.doornaert@simmons-simmons.com

**Christopher Götz**

christopher.goetz@simmons-simmons.com

**Alysia Hogaarts**

alysia.hogaarts@simmons-simmons.com

**Tina Gausling**

tina.gausling@simmons-simmons.com

---

## LAW AND THE REGULATORY AUTHORITY

### Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

European Union's data protection framework is built on the following primary legal texts:

- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR);
- Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Law Enforcement Directive) ;
- Directive (EU) 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive); and
- Directive 2002/58/EC 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 (ePrivacy Directive).

Law stated - 2 June 2025

### Data protection authority

Which authority is responsible for overseeing the data protection law?  
What is the extent of its investigative powers?

Each EU member state must provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR, the Law Enforcement Directive, the PNR Directive, and the ePrivacy Directive.

Under the GDPR, the national authorities have the following investigative powers:

- to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- to carry out investigations in the form of data protection audits;
- to carry out a review of certifications issued pursuant to article 42(7) of the GDPR;
- to notify the controller or the processor of an alleged infringement of this Regulation;
- to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; and

- to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with EU or member state procedural law.

Under the Law Enforcement Directive, the national authorities have at least the investigative power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

Under the PNR Directive, the national authorities have the following powers:

- deal with complaints lodged by any data subject, investigate the matter and inform the data subjects of the progress and the outcome of their complaints within a reasonable time period; and
- verify the lawfulness of the data processing, conduct investigations, inspections and audits in accordance with national law, either on its own initiative or on the basis of a complaint referred to in the previous point.

Under the ePrivacy Directive, the national authorities have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

**Law stated - 2 June 2025**

### **Cooperation with other data protection authorities**

**Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?**

A national supervisory authority are required to provide other data protection authorities (DPA) with relevant information and mutual assistance in order to implement and apply the GDPR in a consistent manner (articles 57.1(g) and 61 GDPR). They must put in place measures for effective cooperation with other DPAs. Mutual assistance must cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

Where processing affects data subjects in more than one EU member state (cross-border processing), the lead supervisory authority must cooperate with the other DPAs concerned (article 60 GDPR). The lead supervisory authority and the other supervisory authorities concerned must seek consensus, exchange all relevant information with each other, and follow the consistency mechanism outlined in article 63 of the GDPR if a disagreement arises.

The national supervisory authority must also conduct joint operations, including joint investigations and joint enforcement measures, in which members or staff of the other member states' DPAs are involved (article 62 GDPR). The competent DPA must invite the other member states' DPAs to take part in the joint operations and must respond without delay to a DPA request to participate.

**Law stated - 2 June 2025**

## Breaches of data protection law

### Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Data breaches can lead to administrative sanctions under the GDPR. The national supervisory authority may impose administrative fines as set out in article 83 of the GDPR, including in relation to data breaches – for example, obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR), obligation to notify personal data breaches to the competent DPA (article 33 GDPR), obligation to inform affected data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms (article 34 GDPR). Administrative fines may vary depending on the infringed GDPR provision, between €10 million or 2 per cent of global annual turnover and €20 million or 4 per cent of global annual turnover (article 83 GDPR).

Data breaches can also lead to corrective measures, including warnings, reprimands, temporary or definitive limitations (including a ban) on processing, suspension of data flows to a recipient in a third country, and an order to communicate a personal data breach to the data subject (article 58.2(e) GDPR).

Breaches are first handled through an investigation step. It starts upon the notification of the breach (by the controller) or with a complaint or *ex officio* at the national supervisory authority's own initiative. The national supervisory authority may conduct on-site audits and request information or documents. After the investigation, the national supervisory authority issues a formal written decision, which may include a fine, an order to implement specific measures, and publication of the breach/sanction in serious cases. For cross-border breaches, the national supervisory authority cooperates with other DPAs and, if a disagreement arises, the European Data Protection Board can issue a binding decision (articles 63 to 65 GDPR).

Law stated - 2 June 2025

## Judicial review of data protection authority orders

### Can PI owners appeal to the courts against orders of the data protection authority?

Each natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. They also have the same judicial remedy if the competent supervisory authority fails to handle a complaint or does not inform the data subject within three months of the progress or outcome of the lodged complaint. Proceedings against a supervisory authority are brought before the courts of the member state where the supervisory authority is established.

Law stated - 2 June 2025

## SCOPE

## Exempt sectors and institutions

### Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Data protection rules apply to all sectors and types of organisation, whether in the private or public sector (a controller may be, within the meaning of the General Data Protection Regulation (GDPR), any natural or legal person, public authority, agency or another body), and whether the processing is operated by automated means or by non-automated means.

However, data protection rules do not apply to the processing of personal data by an individual in the course of a purely personal or household activity (article 2.2(c) GDPR).

The processing of personal data by competent authorities for the purposes of law enforcement and criminal justice is not covered by the GDPR but by the Law Enforcement Directive. The processing of personal data by EU institutions, bodies, offices and agencies is neither covered by the GDPR nor a national law but by Regulation (EC) No 45/2001.

**Law stated - 2 June 2025**

## Interception of communications and surveillance laws

### Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Data protection rules cover those areas.

The ePrivacy Directive prohibits listening to, tapping, storing, or otherwise subjecting communications and related traffic data to interception or surveillance without the user's consent. Member states may adopt legislative measures to restrict the scope of these rights when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (ie, state security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or unauthorised use of the electronic communication system.

The ePrivacy Directive also requires the prior consent of the user for the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing. Some exceptions apply.

**Law stated - 2 June 2025**

## Other laws

### Are there any further laws or regulations that provide specific data protection rules for related areas?

In addition to the general data protection legislative framework indicated above, European Union law has several sector-specific laws and regulations that provide data protection rules in related areas. These include but are not limited to:

- Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – NIS2 Directive comprises

cybersecurity obligations for essential/important entities and includes personal data breach reporting and resilience measures;

- Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA) – DORA mandates ICT risk management for financial entities, including protection of personal data in outsourced digital services;
- Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) – Regulation comprises rules applicable to high-risk AI systems processing personal data and includes transparency, data governance and human oversight requirements;
- Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space (EHDS) – Regulation creates a framework for sharing and reusing health personal data (primary and secondary use), with strong data protection safeguards;
- Regulation (EU) 2022/868 of 30 May 2022 on European data governance (Data Governance Act) – Regulation governs data intermediaries, voluntary data altruism and reuse of certain protection public-sector data, including personal data, with safeguards; and
- Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act) – Regulation sets rules on access to and sharing of user-generated data, including personal data from IoT devices, under user control and with privacy compliance.

**Law stated - 2 June 2025**

## PI formats

### What categories and types of PI are covered by the law?

Almost all categories and types of personal data are covered by the law. In accordance with the GDPR, are notably excluded the following personal data types:

- data relating to legal persons (article 4(1) GDPR);
- personal data of deceased persons (Recital (27) GDPR);
- purely personal or household data (article 2.2(c) GDPR);
- anonymous data (Recital (26) GDPR); and
- non-personal information, in statistical and research data (Recital (26) GDPR).

**Law stated - 2 June 2025**

## Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The GDPR may have an extraterritorial effect. It applies to the processing of personal data of data subjects who are in the European Union even if the controller or processor is not established in the European Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the European Union.

The GDPR may also have an extraterritorial effect even where the processing activities are not related to those two situations; for example, a controller or processor may be deemed to have an 'establishment' in Luxembourg (and, therefore, be subject to its law) if it has there a real and effective activity – even a minimal one – exercised through stable arrangements (see Recital (22) GDPR).

**Law stated - 2 June 2025**

### **Covered uses of PI**

**Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?**

Almost all processing or use of personal data is covered, with the exception of processing activities carried out on types of data not covered by the law. In accordance with the GDPR, the law makes a distinction between those who control personal data (controllers) and those who provide processing services to owners (processors).

The 'controller' is any entity that, alone or jointly with others, determines the purposes and means of the processing of personal data (it decides on the 'why' and 'how'). The 'processor' is any entity which processes personal data on behalf of the controller based on a contract under EU or Luxembourg law.

Controllers and processors duties differ. Some examples include the following:

- The controller has a primary responsibility for legal compliance with the data protection rules. The processor must act on documented instructions from the controller.
- The controller must identify and document the processing legal basis. The processor does not need any independent lawful basis for its activity (it relies on the one identified by the controller).
- The controller must respond to the exercise of data subject rights. The processor must assist the controller in fulfilling those rights.
- The controller must notify the National Commission for Data Protection within 72 hours after having become aware of a data breach, and the data subjects if needed. The processor must notify the controller of the data breach without undue delay.

**Law stated - 2 June 2025**

## LEGITIMATE PROCESSING OF PI

### Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Under the GDPR, the processing of personal data shall only be lawful if and to the extent it relies on one of the valid legal grounds.

Article 6(1) GDPR lists these legal grounds. At least one of the following must apply:

- **Consent:** Under the GDPR, consent must be based on a clear affirmative action and be freely given, specific, informed and unambiguous. Consent language hidden in terms and conditions, pre-ticked boxes or consent inferred from silence are not valid. Also, consent is unlikely to be valid where there is a clear imbalance of power between the individual and the data controller seeking the consent, such as in employment matters. Electronic consent is acceptable, but it must be clear, concise and not unnecessarily disruptive. In the context of a service, the provision of the service should not be made conditional on customers consenting to the processing of personal data that is not necessary for the service. Further, the GDPR requires data controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent.
- **Contract:** Processing is necessary for the performance of a contract with the individual. This means it is objectively indispensable for a purpose that is integral to the contractual obligation intended for the individual. The fact that the processing may be merely useful for the performance of the contract is, in itself, irrelevant.
- **Legal obligation:** Processing is necessary for compliance with the controller's legal obligations.
- **Vital interests:** Processing is necessary to protect the vital interests of a natural person.
- **Public task:** Processing is necessary to fulfil a task in the public interest or in the exercise of official authority.
- **Legitimate interests:** Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the interests or fundamental rights and freedoms of the data subject are overridden. Public authorities cannot rely on this last legal basis in the performance of their tasks.

Law stated - 2 June 2025

### Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

Under the GDPR, processing of special categories of personal data is, in principle, forbidden, except if processing can rely on some additional legal grounds listed under article 9.

Those special categories of personal data are as follows:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- health data; and
- data concerning a person's sex life or sexual orientation.

Importantly, these special categories of data may also be inferred from non-special data. In that case, article 9 also applies.

The additional legal grounds are the following:

- the individual has given explicit consent;
- processing is necessary for:
  - employment or social protection law;
  - the vital interests of a natural person;
  - legal claims or when courts act in their judicial capacity;
  - reasons of substantial public interest;
  - for health or social care purposes;
  - for public health reasons; and
  - archiving, research, or statistics purposes;
- processing is carried out by and in the context of a non-profit organisation with a political, philosophical, religious or trade union aim; and
- processing is related to personal data made public by the individual.

Additionally, article 10 of the GDPR provides that the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by law.

**Law stated - 2 June 2025**

## DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

### **Transparency**

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Under articles 13 and 14 of the General Data Protection Regulation (GDPR), data controllers are required to inform data subjects about the processing of their personal data in a concise, transparent, intelligible, and easily accessible manner, using clear and plain language. In practice, this is typically achieved through a privacy notice.

The privacy notice must, at a minimum, include the following information:

- the identity and contact details of the controller, and where applicable, the data protection officer;
- the purposes of the processing and the legal basis for it;
- where applicable, the legitimate interests pursued by the controller or a third party;
- the recipients or categories of recipients of the personal data;
- where relevant, information about data transfers to third countries or international organisations;
- the applicable retention periods for the personal data;
- a description of the rights available to data subjects;
- the right to withdraw consent at any time, where 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 necessary to enter into a contract, and the possible consequences of failing to provide the data; and
- the existence of automated decision-making, including profiling and meaningful information about the logic involved and the potential consequences for the data subject.

Where personal data has not been obtained directly from the data subject, the controller must also inform the data subject of the categories of personal data concerned and the source from which the data originates.

This information must be provided within a reasonable period after obtaining the personal data, and at the latest within one month. If the personal data is used to communicate with the data subject, the information must be provided at the time of the first communication. Where the data is disclosed to another recipient, the information must be provided at the latest at the time of the first disclosure.

**Law stated - 2 June 2025**

## **Exemptions from transparency obligations**

### **When is notice not required?**

Under the GDPR, certain situations allow for exemptions from the obligation to provide notice about the processing of personal data. These exemptions are set out in article 13(4) and article 14(5) of the GDPR. For example, no notice is required where the data subject already possesses the relevant information.

Additionally, where personal data has not been obtained directly from the data subject, the obligation to provide information does not apply if doing so proves impossible or would involve a disproportionate effort. This exception is particularly relevant in cases where the data is processed for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

Lastly, the obligation to inform the data subject does not apply where the personal data must remain confidential in accordance with an obligation of professional secrecy imposed by EU or member state law, including a statutory obligation of secrecy.

**Law stated - 2 June 2025**

### **Data accuracy**

#### **Does the law impose standards in relation to the quality, currency and accuracy of PI?**

Article 5(1)(d) of the GDPR states that personal data must be accurate and kept up-to-date. This means that a data controller is obliged to take steps to ensure that personal data that is inaccurate is erased or rectified without delay.

**Law stated - 2 June 2025**

### **Data minimisation**

#### **Does the law restrict the types or volume of PI that may be collected?**

Under article 5(1)(c) of the GDPR, the personal data being processed must be adequate, relevant, and limited to what is necessary for the specific purposes of the processing. This means that the controller should strictly limit the collection of information to what is directly relevant to the intended purpose. For example, collecting gender information to personalise marketing communications is not necessary for fulfilling a contract and, therefore, does not meet the requirement of being strictly relevant to the intended purpose.

**Law stated - 2 June 2025**

### **Data retention**

#### **Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?**

In line with article 5(1)(e) of the GDPR, a data controller must not retain personal data for longer than is necessary for the purposes for which the data is processed. Moreover, personal data should not be kept in an identifiable form for longer than necessary in relation to those purposes. Lawful retention of data that is no longer required can, therefore, be achieved by anonymising the data.

The GDPR does not specify concrete retention periods for personal data. It is the responsibility of each organisation to determine appropriate retention periods, taking into account the purposes for which the data is processed. However, organisations must also

comply with retention obligations laid down in other applicable (national) laws, such as tax legislation, which may impose specific retention periods.

**Law stated - 2 June 2025**

### **Purpose limitation**

**Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?**

The principle of purpose limitation, as outlined in article 5(f) of the GDPR, requires that personal data be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. These purposes must be determined before the processing begins. By ensuring that processing purposes are clear and specific, transparency is enhanced, and legal certainty is provided to data subjects.

Once personal data has been collected for a defined purpose, any further processing that is incompatible with that original purpose is prohibited. Where data controllers intend to process the data for a new purpose that is not compatible with the initial one, a separate legal basis is required; such further processing cannot rely solely on the fact that the data was lawfully collected for a different purpose.

**Law stated - 2 June 2025**

### **Automated decision-making**

**Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?**

Under the GDPR, individuals have the right not to be subjected to decisions based solely on automated processing, including profiling, if these decisions have legal effects or significantly affect them. A decision is considered solely automated if there is no human involvement in the decision-making process. For human intervention to qualify as meaningful, the controller must ensure that the oversight of the decision is meaningful. The GDPR provides a few exceptions to this rule, such as where the individual has given explicit consent, as set out in article 22(2)(c).

**Law stated - 2 June 2025**

## **SECURITY**

### **Security obligations**

**What security obligations are imposed on PI owners and service providers that process PI on their behalf?**

Under the General Data Protection Regulation (GDPR), both controllers and processors are subject to security obligations to protect personal data. The GDPR requires controllers and processors to implement technical and organisational measures that ensure a level of

security appropriate to the risk (article 32), which may include encryption, pseudonymisation, ensuring the confidentiality, integrity and availability of systems, and regular testing of security controls.

Processors may only process personal data on documented instructions from the controller (Article 28). They must also ensure that any sub-processors implement appropriate technical and organisational measures.

Additionally, the GDPR requires that controllers and processors embed privacy into systems and services from the outset (data protection by design and by default, article 25).

**Law stated - 2 June 2025**

### **Notification of data breach**

**Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?**

The GDPR includes a general data breach notification requirement applicable to all industries. All data controllers must notify data breaches to the data protection authorities (DPAs) without undue delay and, where feasible, within 72 hours after becoming aware of the breach unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Delayed notifications must be accompanied by a reasoned justification, and the information related to the breach can be provided in phases. In addition, data controllers must notify affected individuals if the breach is likely to result in a high risk to the individuals' rights and freedoms. Businesses must maintain data breach response plans and take other breach readiness measures to avoid fines and negative publicity associated with data breaches. Data processors are required to notify data controllers of personal data breaches without undue delay after becoming aware of a breach, but do not have an independent obligation to notify DPAs or affected individuals.

**Law stated - 2 June 2025**

## **INTERNAL CONTROLS**

### **Accountability**

**Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?**

Under the General Data Protection Regulation (GDPR), owners (controllers) and processors of personal data are required to implement internal controls to ensure that they are responsible, accountable, and able to demonstrate compliance with the law. This is established by the accountability principle in article 5(2) of the GDPR and further detailed in articles 24, 28, and 32 of the GDPR.

**Law stated - 2 June 2025**

## Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer (DPO) is mandatory in specific cases. Pursuant to article 37 of the GDPR, a DPO must be appointed if:

- 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 involve regular and systematic monitoring of data subjects on a large scale; and
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data (eg, health, religion) pursuant to article 9 of the GDPR or data relating to criminal convictions and offences referred to in article 10 of the GDPR.

The DPO's legal responsibilities are outlined in article 39 of the GDPR pursuant to which a DPO must:

- inform and advise the controller or the processor and the employees who carry out the processing of their obligations pursuant to the GDPR and to other EU or member state data protection provisions;
- monitor compliance with the GDPR, with other EU or member state data protection provisions and internal data protection policies, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- provide advice on Data Protection Impact Assessments (DPIAs) and monitor their performance;
- cooperate with the supervisory authority (eg, the data protection authority); and
- act as a point of contact for the supervisory authority and for data subjects on issues related to data processing.

Pursuant to article 37(5) of the GDPR, a DPO shall be designated on the basis of professional qualities, and, in particular:

- expert knowledge in the field of data protection law and practices; and
- the ability to fulfil the tasks referred to in article 39 of the GDPR as described above.

**Law stated - 2 June 2025**

## Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Under article 30 of the GDPR, controllers and processors are required to maintain internal records of processing activities, except where an exemption applies (eg, organisations employing fewer than 250 persons unless the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data pursuant to article 9(1) of the GDPR or personal data relating to criminal convictions and offences referred to in article 10 of the GDPR.

**Law stated - 2 June 2025**

### **Risk assessment**

#### **Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?**

Under article 35 of the GDPR, controllers are required to carry out a Data Protection Impact Assessment (DPIA) when a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA is particularly required in the following cases:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in article 9(1) of the GDPR, or of personal data relating to criminal convictions and offences referred to in article 10 of the GDPR; or
- a systematic monitoring of a publicly accessible area on a large scale.

Processors must assist the controller in fulfilling these obligations pursuant to article 28(3)(f) GDPR. The DPIA is used to assess risks and define appropriate measures to mitigate them.

**Law stated - 2 June 2025**

### **Design of PI processing systems**

#### **Are there any obligations in relation to how PI processing systems must be designed?**

Under article 25 of the GDPR, controllers are required to implement data protection by design and by default. This means that data protection principles such as data minimisation and purpose limitation must be embedded when designing systems and processes that involve personal data.

Controllers are expected to take into account the state of the art, cost of implementation, and the nature, scope, context and purposes of the processing, as well as the risks to individuals' rights and freedoms. Based on that, they must implement appropriate technical and organisational measures, such as pseudonymisation, access controls, or purpose-specific configurations, to ensure that data protection is effectively built into the lifecycle of the system.

Law stated - 2 June 2025

## REGISTRATION AND NOTIFICATION

### Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Under the General Data Protection Regulation (GDPR), there is no general obligation to register with the supervisory authority. However, article 23(1) of the GDPR allows member states to impose restrictions on certain GDPR rights and obligations, including through national laws for specific purposes (eg, public security and national interests). This opens the door for sector-specific registration or notification obligations under national law.

Law stated - 2 June 2025

### Other transparency duties

Are there any other public transparency duties?

Under the GDPR, controllers have several public transparency obligations. They must provide individuals with clear and accessible information about how their personal data is processed, as set out in articles 12 to 14 of the GDPR. This includes details about the purposes of the processing, the legal basis, data recipients, retention periods, and data subject rights (articles 15 to 22 GDPR). In the event of a personal data breach likely to result in a high risk to individuals' rights and freedoms, the controller must inform the affected individuals without undue delay (article 34 GDPR). If a data protection officer is appointed, their contact details must be made available to the supervisory authority (see article 37(7) GDPR).

Law stated - 2 June 2025

## SHARING AND CROSS-BORDER TRANSFERS OF PI

### Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

When a controller engages a processor, this relationship must be governed by a written contract (or other binding act) (article 28(3)). This contract must specify that the processor will only act on the documented instructions of the controller, and it must define the nature, purpose, and duration of the processing, as well as the types of personal data involved and the categories of data subjects. It must also include obligations concerning confidentiality, the implementation of appropriate security measures, and clear rules around sub-processing. The processor can only act on the documented instructions of the controller. The processor must also be required to assist the controller in meeting their General Data Protection Regulation (GDPR) obligations. At the end of the processing relationship,

the processor must be required to return or delete all personal data as instructed by the controller. Additionally, the contract must provide for the controller's right to carry out audits or inspections to verify the processor's compliance.

Even though the processor carries out the processing, the controller remains fully responsible for ensuring that personal data is handled in accordance with GDPR and must only rely on processors that offer sufficient guarantees of compliance.

Law stated - 2 June 2025

### Restrictions on third-party disclosure

#### Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The GDPR does not contain specific restrictions on the sharing of personal data with third parties.

Law stated - 2 June 2025

### Cross-border transfer

#### Is the transfer of PI outside the jurisdiction restricted?

The GDPR maintains the general prohibition of data transfers to countries outside of the EU that do not provide an 'adequate' level of data protection but introduces alternative tools for transferring personal data outside the EU, such as codes of conduct and certification mechanisms. The previous contractual options for data transfers have been expanded and made easier; regulators may also adopt standard contractual clauses for data transfers to be approved by the European Commission, and it is no longer required to obtain the prior authorisation of the data protection authorities for transferring personal data outside the EU and submit copies of executed standard contractual clauses (which was previously required in some member states). In addition, the GDPR formally recognises binding corporate rules (BCRs) – internal codes of conduct used by businesses to transfer personal data to group members outside of the EU – as a valid data transfer mechanism for both data controllers and data processors. As a result of the *Schrems II* decision, organisations that relied on standard contractual clauses (and other transfer mechanisms, such as BCRs) must assess each data transfer on a case-by-case basis to determine whether there is an adequate level of protection for personal data transferred outside the EU and, where necessary, implement additional technical, contractual and organisational safeguards for the transfer. In addition, the European Commission has issued new standard contractual clauses (SCCs) for international data transfers, which were adopted on 4 June 2021.

On 10 July 2023, the European Commission adopted an adequacy decision for the EU-US Data Privacy Framework. The EU-US Data Privacy Framework is the successor of the EU-US Privacy Shield Framework that was invalidated as a result of the *Schrems II* decision. Organisations in the United States participating in the EU-US Data Privacy Framework may freely receive personal data from the EEA on the basis of the adequacy decision. In October 2023, an action was brought before the EU General Court aimed at invalidating this Framework. The case is still pending.

In March 2025, the European Commission proposed a six-month extension of the United Kingdom extension, which is set to expire on 27 June 2025. This would ensure the free flow of personal data between the EU and the UK until 27 December 2025.

Law stated - 2 June 2025

### Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The GDPR restrictions on transfers of personal data apply equally to transfers made to processors and onward transfers.

Law stated - 2 June 2025

### Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

Under the GDPR, there is no requirement that personal data or a copy of it must be retained within the EU.

Law stated - 2 June 2025

## RIGHTS OF INDIVIDUALS

### Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under article 15 of the General Data Protection Regulation (GDPR), individuals have the right to request confirmation from the data controller as to whether their personal data is being processed. If this is the case, the individual is entitled to access these data, as well as to receive information about:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed;
- the envisaged retention period, or, if not possible, the criteria used to determine that period;
-

the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

- the right to lodge a complaint with a supervisory authority;
- where the personal data is not collected from the data subject, any available information as to their source; and
- the existence of automated decision-making, including profiling.

The right of access aims to give individuals more control over their personal data. It enables data subjects to exercise their rights as outlined in articles 16-19, 21, 79 and 82 of the GDPR. In this respect, the right of access entails the ability for data subjects to obtain information from the data controller about the specific recipients who have received or will receive their data.

**Law stated - 2 June 2025**

## Other rights

### Do individuals have other substantive rights?

In addition to the right to access, data subjects have the following rights:

- the right to rectification (article 16 GDPR): data subjects have the right to obtain the rectification of inaccurate personal data concerning them.
- the right to erasure (article 17 GPDR): data subjects have the right to request the erasure of their personal data when certain conditions are met.
- the right to restriction of processing (article 18 GDPR): data subjects have the right to request that the processing of their personal data be restricted.
- the right to data portability (article 20 GDPR): data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller.
- the right to object (article 21 GDPR): data subjects have the right to object to the processing of their personal data on grounds relating to their particular situation.
- the right to human intervention in decision-making processes (article 22 GDPR): data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, without meaningful human intervention; and
- the right to complain to a national supervisory authority: data subjects have the right to lodge a complaint with a national data protection authority.

**Law stated - 2 June 2025**

## Compensation

## Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

In accordance with article 82 of the GDPR, any individual who suffers material or non-material damages due to an infringement of the regulation's provisions has the right to receive compensation from the data controller or processor.

This right to compensation also applies when a data subject experiences fear regarding the potential misuse of their personal data by third parties as a result of the infringement. In this context, there is no *de minimis* threshold. Furthermore, when determining the amount of compensation for non-material damages, it must be recognised that such damages caused by a personal data breach are not less significant than physical injury.

Law stated - 2 June 2025

## Enforcement

### Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

In addition to the right to complain to the supervisory authority, individuals must have the right to an effective judicial remedy against a data controller or processor and to bring their case before a court. This right is established in article 79 of the GDPR.

When initiating proceedings against a controller or processor, data subjects must be given the choice of forum. They may commence the action either in the member state where the controller or processor is established or in the member state of their own habitual residence. In conclusion, data subjects can exercise their rights through both the judicial system and enforcement by the supervisory authority.

Law stated - 2 June 2025

## EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

### Further exemptions and restrictions

#### Does the law include any derogations, exclusions or limitations other than those already described?

In addition to the derogations, exclusions, and limitations outlined in the General Data Protection Regulation (GDPR), the GDPR provides member states the competence to establish further exceptions and restrictions through national legislation.

Law stated - 2 June 2025

## SPECIFIC DATA PROCESSING

### Cookies and similar technology

#### Are there any rules on the use of 'cookies' or equivalent technology?

Under the General Data Protection Regulation (GDPR), cookies that involve the processing of personal data – such as tracking cookies – require a legal basis, typically the user’s consent pursuant to article 6(1)(a) of the GDPR. This consent must be freely given, specific, informed, and capable of being withdrawn at any time.

In addition, the ePrivacy Directive (2002/58/EC) – which applies alongside the GDPR – requires that prior consent be obtained before storing or accessing information on a user’s device unless the cookie is strictly necessary for providing the service explicitly requested by the user. As an EU directive, the ePrivacy Directive must be implemented into national law by each member state, meaning that cookie consent requirements may be further detailed in national legislation.

Therefore, most non-essential cookies, such as those used for analytics, advertising, or personalization, may only be used after valid user consent has been obtained, in line with both the GDPR and applicable national ePrivacy rules.

**Law stated - 2 June 2025**

### **Electronic communications marketing**

#### **Are there any rules on marketing by email, fax, telephone or other electronic channels?**

Under the GDPR, electronic marketing often involves processing personal data and thus requires a legal basis, usually the data subject’s consent pursuant to article 6(1)(a) GDPR. In addition, the ePrivacy Directive sets specific rules: unsolicited marketing by email, fax, or automated calls generally requires prior consent, while telephone marketing may be allowed under national laws if the recipient has not objected. Clear opt-out options must always be provided, and all communications must respect the principles of transparency and data minimisation.

**Law stated - 2 June 2025**

### **Targeted advertising**

#### **Are there any rules on targeted online advertising?**

Under the GDPR, targeted online advertising, including behavioural or interest-based advertising, requires a valid legal basis, usually explicit user consent pursuant to article 6(1)(a) of the GDPR, especially when it involves tracking technologies such as cookies or profiling. Users must be clearly informed about how their data is collected and used and must have the ability to withdraw consent at any time. Additionally, profiling that significantly affects individuals (eg, automated decision-making) triggers stricter requirements under article 22 of the GDPR.

**Law stated - 2 June 2025**

### **Sensitive personal information**

## Are there any rules on the processing of 'sensitive' categories of personal information?

The GDPR places strict rules on processing sensitive personal data, such as racial or ethnic origin, political or religious beliefs, trade union membership, genetic or biometric data, health data, or data on sex life or sexual orientation, pursuant to article 9(1) of the GDPR. This data is generally prohibited from being processed unless a specific exception applies (eg, if the data subject has given explicit consent if the processing is necessary for carrying out legal obligations in employment) to protect the data subject's vital interests, or for reasons of substantial public interest. Additional safeguards, like data protection impact assessments or stricter access controls, may also be required to ensure protection and compliance.

**Law stated - 2 June 2025**

## Profiling

### Are there any rules regarding individual profiling?

The GDPR sets specific rules for profiling, particularly when it involves automated processing to evaluate personal aspects such as behaviour, interests, or performance (see article 4(4) GDPR). If profiling involves solely automated decision-making – meaning decisions made without any human involvement – that produce legal effects or similarly significant impacts on the individual (eg, credit approval, hiring decisions), then article 22 of the GDPR applies. In such cases, individuals have the right not to be subject to this type of decision-making unless certain exceptions apply, such as:

- it is necessary for entering into or performing a contract,
- it is authorised by EU or member state law, or
- the individual has given explicit consent.

Where such processing is permitted, the controller must implement safeguards, including the right to human intervention to express a point of view and to contest the decision.

Even outside of article 22 of the GDPR, profiling must comply with general GDPR principles, such as transparency, fairness, and data minimisation. Individuals must be informed about profiling in privacy notices and may also have the right to object under article 21 of the GDPR, especially in the context of direct marketing.

**Law stated - 2 June 2025**

## Cloud services

### Are there any rules or regulator guidance on the use of cloud computing services?

The GDPR permits the use of cloud services but under strict conditions. Controllers must have a data processing agreement, pursuant to article 28 of the GDPR, in place and ensure the provider implements appropriate technical and organisational measures in accordance with article 32 of the GDPR. This includes verifying the provider's security standards, access controls, and compliance with data protection obligations. Where personal data

is transferred outside the EU/EEA, appropriate safeguards such as Standard Contractual Clauses must be in place (see article 44 et seqq GDPR). Several supervisory authorities have issued guidance stressing the need for due diligence, including reviewing the provider's security certifications, sub-processor arrangements, and data transfer mechanisms, before engaging a cloud provider.

Law stated - 2 June 2025

## UPDATE AND TRENDS

### Key developments of the past year

#### Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Some emerging trends in EU personal data protection include the following:

- Enforcement of the AI Act: the EU's AI ACT, effective February 2025, prohibits practices posing unacceptable risks, such as social scoring and untargeted facial recognition. From August 2025, developers of general-purpose AI models must assess and mitigate systemic risks, document training data, and ensure adequate security measures.
- Implementation of the Data Act: The Data Act, in force since January 2024, will become applicable in September 2025. It mandates that users have access to data generated by their connected devices, promoting fair data sharing and use across sectors.
- Launch of the European Health Data Space (EHDS): The EHDS Regulation entered into force in March 2025, aiming to provide EU citizens with better control over their personal health data and facilitate its use for research and policy-making. Member states are required to establish digital health authorities within two years.
- Scrutiny of 'Consent or Pay' model: In April 2024, the European Data Protection Board issued a non-binding opinion stating that 'consent or pay' models, where users must pay to avoid data tracking, generally do not constitute valid consent under the General Data Protection Regulation. This has led to increased regulatory attention on such practices.

Law stated - 2 June 2025