

EU GDPR: Data Protection Rights and Obligations

Principles, Lawful Bases, Controller Obligations, Data Subject Rights, and Enforcement

What rights, obligations, and legal bases should you understand to process personal data lawfully under the GDPR?

Overview: The EU General Data Protection Regulation

As an employee at a company that processes personal data — customer records, employee data, website analytics, AI training inputs — the General Data Protection Regulation (Regulation (EU) 2016/679) ^[1] is the legal framework that governs your work. Applicable since 25 May 2018, the GDPR is built on seven foundational **principles** ^[tn100] (Art. 5) requiring that personal data be processed lawfully, fairly, and transparently. Any processing must rest on one of six **lawful bases** ^[tn200] (Art. 6). Controllers bear specific **obligations** ^[tn300] to implement privacy by design, maintain records, and notify breaches. Individuals enjoy extensive **data subject rights** ^[tn400] (Art. 15–22) including access, rectification, erasure, and portability.

Article 3 sets out two scope tests: GDPR applies to processing in the context of the activities of an establishment in the Union (regardless of whether the processing takes place in the Union), and to processing by non-EU controllers or processors that offer goods or services to data subjects in the Union or monitor their behaviour within the Union. Mere accessibility of a website from the Union is not sufficient on its own; targeting evidence (e.g., language, currency, top-level domain, EU-specific marketing) is required. **Enforcement** ^[tn500] is via national supervisory authorities with fines of up to €20 million or 4% of global annual turnover.

Principles [tn100]: Art. 5 — Foundations of Data Processing

Article 5 of the GDPR establishes seven principles that form the foundation of all lawful data processing. Controllers must demonstrate compliance with each principle under the **accountability** [tn107] obligation (Art. 5(2)). These principles **require a legal basis** [te101] from one of the six **lawful bases** [tn200] under Art. 6 [1].

- **Lawfulness, Fairness, Transparency** [tn101]: Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject (Art. 5(1)(a))
- **Purpose Limitation** [tn102]: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes (Art. 5(1)(b))
- **Data Minimisation** [tn103]: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (Art. 5(1)(c))
- **Accuracy** [tn104]: Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate data are erased or rectified without delay (Art. 5(1)(d))
- **Storage Limitation** [tn105]: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed (Art. 5(1)(e))
- **Integrity & Confidentiality** [tn106]: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (Art. 5(1)(f))
- **Accountability** [tn107]: The controller is responsible for, and must be able to demonstrate compliance with, all of the above principles (Art. 5(2)). Article 24 operationalises this: the controller must implement appropriate technical and organisational measures, taking into account the nature, scope, context, and purposes of processing as well as the

risks of varying likelihood and severity for the rights of natural persons; these measures must be reviewed and updated

Lawful Bases [tn200]: Art. 6 — Legal Grounds for Processing

Article 6 sets out six lawful bases upon which personal data may be processed. At least one basis must apply before any processing activity begins. The choice of basis affects which **data subject rights** [tn400] are available and **requires safeguards** [te102] to protect individuals [1].

- **Consent** [tn201]: The data subject has given consent to the processing of his or her personal data for one or more specific purposes (Art. 6(1)(a)). Consent must be freely given, specific, informed, and unambiguous. Article 7 governs the operational requirements: the controller must be able to **demonstrate** that the data subject has consented (Art. 7(1)); requests for consent must be presented in a manner clearly distinguishable from other matters, in clear and plain language (Art. 7(2)); the data subject has the **right to withdraw consent at any time** and withdrawal must be as easy as giving consent (Art. 7(3)); and when assessing whether consent is freely given, account must be taken of whether performance of a contract is conditional on consent that is not necessary for that performance (Art. 7(4))
- **Contract Performance** [tn202]: Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract (Art. 6(1)(b))
- **Legal Obligation** [tn203]: Processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 6(1)(c))
- **Vital Interests** [tn204]: Processing is necessary in order to protect the vital interests of the data subject or of another natural person (Art. 6(1)(d))

(d))

- **Public Interest** [tn205]: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6(1)(e))
- **Legitimate Interests** [tn206]: Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (Art. 6(1)(f))

Special Categories of Personal Data [tn250]: Art. 9 — Additional Layer

Article 9 establishes a heightened protection layer for sensitive categories of personal data. A valid **lawful basis** [tn200] under Article 6 is necessary but not sufficient — Article 9 requires an **additional layer for sensitive data** [te108] before processing may lawfully begin. For organisations using personal data in AI training, customer profiling, biometric authentication, or health analytics, Article 9 is the most consequential provision after Article 6. Special-category processing also **imposes heightened obligations** [te109] on the controller (DPIA likelihood, security measures, sometimes a DPO).

- **Special Categories Defined** [tn251] (**Art. 9(1)**): Article 9(1) prohibits processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; the processing of genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health; or data concerning a natural person's sex life or sexual orientation. The prohibition applies regardless of whether a valid Article 6 basis exists.
- **Conditions for Lifting the Prohibition** [tn252] (**Art. 9(2)**): Processing of special-category data is permitted only when one of the ten conditions in Article 9(2) applies. The most operationally relevant are: (a) explicit consent of the data subject; (b) employment, social-security, and social-

protection law; (c) vital interests of a data subject who is unable to give consent; (e) data manifestly made public by the data subject; (g) substantial public interest with appropriate safeguards; (h) preventive or occupational medicine, medical diagnosis, or treatment under professional secrecy; (i) public health; and (j) archiving, scientific or historical research, or statistical purposes in the public interest. Member States may add further conditions for genetic, biometric, or health data (Art. 9(4)).

- **AI Training and Special Categories** ^[tn253]: For organisations using personal data for AI training: any inference or feature derivation that reveals a special category (e.g., inferring health status, sexual orientation, or political opinions from non-special-category inputs) brings the processing into Article 9's scope. Pseudonymisation does not by itself remove data from the special-category regime; only true anonymisation (Recital 26) does — and the bar for anonymisation is high (no reasonable means of re-identification). Special-category processing in AI also tends to trigger the DPIA requirement under Article 35(3)(b).

Controller Obligations ^[tn300]: Key Duties of the Data Controller

The GDPR imposes specific obligations on data controllers to ensure that personal data is processed in compliance with its **principles** ^[tn100]. These **obligations** **protect** ^[te103] the **data subject rights** ^[tn400] and help prevent breaches that could **trigger enforcement** ^[te104] ^[1].

- **Controller vs. Processor** ^[tn220] (**Art. 4(7), 4(8), 26, 28**): The GDPR distinguishes **controllers** (who determine the purposes and means of processing, Art. 4(7)) from **processors** (who process personal data on behalf of a controller, Art. 4(8)). A company can be a controller for some activities (e.g., processing its own employees' data) and a processor for others (e.g., providing SaaS to business customers). The distinction

determines who is responsible for which obligations: controllers carry primary responsibility for principles and rights; processors are bound by Art. 28 (contracts), Art. 32 (security), Art. 33 (breach notification to the controller), and Arts. 37–39 (DPO where applicable). Both can be fined directly. **Joint controllers** (Art. 26) jointly determine purposes and means and must agree their respective responsibilities by transparent arrangement, made available to data subjects.

- **Privacy by Design & Default** [tn301] (**Art. 25**): The controller must implement appropriate technical and organisational measures — such as pseudonymisation and data minimisation — both at the time of determining the means for processing and at the time of processing itself, to ensure that by default only personal data necessary for each specific purpose is processed
- **Processor Requirements** [tn302] (**Art. 28**): Where processing is carried out on behalf of a controller, the controller must use only processors providing sufficient guarantees. Processing by a processor must be governed by a contract or other legal act setting out the subject-matter, duration, nature, and purpose of the processing
- **Records of Processing** [tn303] (**Art. 30**): Each controller and processor must maintain a record of processing activities under its responsibility, including the purposes of processing, categories of data subjects and personal data, recipients, and envisaged time limits for erasure
- **Breach Notification to Authority** [tn304] (**Art. 33**): In the case of a personal data breach, the controller must notify the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it (Art. 33(1)). Where notification is not made within 72 hours, it must be accompanied by reasons for the delay. Notification is not required if the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification must contain the categories and approximate number of data subjects and records concerned, the name of the DPO, the likely consequences, and the measures taken (Art. 33(3)).
- **Data Protection Impact Assessment** [tn305] (**Art. 35**): Where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the controller

must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data prior to the processing

- **Breach Notification to Data Subjects** ^[tn311] (**Art. 34**): **If high risk, notify subjects** ^[te305]: When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the breach to the affected data subjects without undue delay (Art. 34(1)). The communication must describe the breach in clear and plain language and contain the name and contact of the DPO, the likely consequences, and the measures taken or proposed (Art. 34(2)). Notification to subjects is not required where the controller has implemented appropriate protection measures (e.g., encryption rendering the data unintelligible), where subsequent measures eliminate the high risk, or where individual notification would involve disproportionate effort — in which case a public communication is required (Art. 34(3)).
- **Information at Collection** ^[tn306] (**Art. 13**): When personal data is collected directly from the data subject, Article 13 requires the controller to provide, at the time of collection: identity and contact of the controller; contact of the DPO where applicable; purposes and lawful basis for processing; the legitimate interests pursued where the basis is Art. 6(1) (f); recipients or categories of recipients; details of any international transfers and the safeguards used; retention period or criteria; existence of data-subject rights (Arts. 15–22); right to withdraw consent; right to lodge a complaint with a supervisory authority; whether provision is statutory or contractual; and existence of automated decision-making (Art. 22) including meaningful information about the logic involved.
- **Information When Data Not From Subject** ^[tn307] (**Art. 14**): When personal data is collected indirectly (for example from data brokers, public sources, or other controllers), Article 14 requires the controller to provide the same content as Article 13 plus the categories of personal data concerned and the source from which the data originated. Information must be provided within a reasonable period and at the latest within one month, or at first communication with the data subject if used for that communication, or at first disclosure to a third party — whichever is earliest. Limited exceptions apply where provision proves impossible or would involve disproportionate effort (Art. 14(5)).

- **DPO Designation** [tn308] **(Art. 37)**: A Data Protection Officer (DPO) must be designated when (a) processing is carried out by a public authority or body; (b) the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities consist of large-scale processing of special-category data (Art. 9) or criminal-conviction data (Art. 10). Designation may be voluntary in other cases. A group of undertakings or a public-sector group may designate a single DPO. The DPO's contact details must be published and communicated to the supervisory authority (Art. 37(7)).
- **DPO Position** [tn309] **(Art. 38)**: The DPO must be involved properly and in a timely manner in all issues relating to data protection (Art. 38(1)); be supported with the resources and access necessary to perform tasks (Art. 38(2)); and not receive instructions regarding the exercise of those tasks (Art. 38(3)). The DPO cannot be dismissed or penalised for performing their tasks. The DPO reports directly to the highest level of management. Data subjects may contact the DPO with regard to all issues related to processing and to the exercise of their rights (Art. 38(4)).
- **DPO Tasks** [tn310] **(Art. 39)**: Article 39 lists the DPO's core tasks: informing and advising the controller, processor, and employees of their obligations under data-protection law; monitoring compliance with the GDPR and internal policies (including assignment of responsibilities, awareness-raising, training, and audits); providing advice on Data Protection Impact Assessments (Art. 35) upon request; cooperating with the supervisory authority; and acting as the contact point for the supervisory authority on issues relating to processing (Art. 39(1)(e)).

Data Subject Rights [tn400]: Art. 15–22 — Individual Rights

The GDPR grants individuals a comprehensive set of rights over their personal data. When these rights are **denied** [te105], data subjects may lodge complaints triggering

enforcement [tn500]. Processing without a valid **lawful basis** [te106] from the **lawful bases** [tn200] also constitutes a violation [1]. The controller must respond to a data-subject request **without undue delay and in any event within one month** of receipt (Art. 12(3)). The period may be extended by two further months where necessary, taking into account the complexity and number of requests; the data subject must be informed of the extension and the reasons within one month.

- **Right of Access** [tn401] (**Art. 15**): If a customer or user submits an access request, the controller must confirm whether personal data concerning the requester is being processed and, where that is the case, provide a copy of the data and information about the processing purposes, categories of data, and recipients (Art. 15)
- **Right to Rectification** [tn402] (**Art. 16**): If a customer reports that data about them is inaccurate, the controller must rectify it without undue delay (Art. 16). The data subject also has the right to have incomplete data completed. This right connects to the **accuracy** [tn104] principle: when data is **inaccurate, it must be rectified** [te301]
- **Right to Erasure** [tn403] (**Art. 17**): If a customer requests deletion of their data, the controller must erase it without undue delay (Art. 17) where the data are **no longer needed** [te302], consent is withdrawn, the data subject objects, or the data have been unlawfully processed
- **Right to Restriction** [tn404] (**Art. 18**): If a customer asks to restrict processing of their data, the controller must comply where: the accuracy of the data is contested (during verification); the processing is unlawful but the subject opposes erasure; the controller no longer needs the data but the subject needs them for legal claims; or the data subject has objected to processing pending verification of overriding grounds (Art. 18)
- **Right to Data Portability** [tn405] (**Art. 20**): If a customer asks for their data in a portable format, the controller must provide the data the subject has provided in a structured, commonly used, and machine-readable format, and (where technically feasible) transmit it directly to another controller of the subject's choice (Art. 20)
- **Right to Object** [tn406] (**Art. 21**): If a customer objects to processing based on public interest or legitimate interests (Art. 6(1)(e) or (f)), the controller must stop processing unless it can demonstrate compelling

legitimate grounds that override the data subject's interests, rights, and freedoms — or the processing is for legal claims (Art. 21(1)). Data subjects **can also object** [te303] to processing for direct marketing purposes, in which case the data must no longer be processed for that purpose

- **Automated Decision-Making** [tn407] (**Art. 22**): If a customer is subject to a decision based solely on automated processing (including profiling) that produces legal effects or similarly significantly affects them, they have the right not to be subject to that decision (Art. 22(1)), except where necessary for a contract, authorised by law, or based on explicit consent. Where automated decision-making is permitted under Art. 22(2), the controller must implement suitable safeguards including, at a minimum, the **right to obtain human intervention**, the right to express the data subject's point of view, and the right to contest the decision (Art. 22(3)). Decisions based on special-category data require either explicit consent or a substantial-public-interest basis with safeguards (Art. 22(4)). The data subject also has the right to obtain **meaningful information about the logic involved** and the significance and envisaged consequences of such processing (Arts. 13(2)(f), 14(2)(g), 15(1)(h))

International Transfers [tn600]: Art. 44–49 (Chapter V)

Chapter V regulates transfers of personal data to third countries or international organisations. Any cross-border **transfer requires lawful basis and safeguards** [te110] to preserve the GDPR's level of protection. The mechanism is layered — adequacy decisions where they exist, appropriate safeguards otherwise, and narrow derogations for one-off cases. Following the CJEU Schrems II judgment, transfers under standard contractual clauses also require a transfer impact assessment evaluating local-law access risks. Non-compliance with Chapter V **triggers Tier 2 fines** [te111] under Art. 83(5).

- **General Principle** [tn601] **(Art. 44)**: Article 44 establishes the general principle: any transfer of personal data to a third country or international organisation may take place only if the conditions laid down in Chapter V are complied with. The level of protection guaranteed by the GDPR must not be undermined.
- **Adequacy Decisions** [tn602] **(Art. 45)**: Transfers may take place where the European Commission has decided that a third country, territory, or specified sector ensures an adequate level of protection. Existing adequacy decisions cover (among others) the United Kingdom, Switzerland, Japan, South Korea, and the EU-US Data Privacy Framework. Adequacy decisions are subject to ongoing Commission review and may be challenged before the Court of Justice of the EU.
- **Appropriate Safeguards** [tn603] **(Art. 46)**: In the absence of an adequacy decision, transfers may take place where the controller or processor has provided appropriate safeguards: standard contractual clauses (SCCs) adopted by the Commission; binding corporate rules (Art. 47); approved codes of conduct (Art. 40) with binding enforceable commitments; approved certification mechanisms (Art. 42); or legally binding and enforceable instruments between public authorities. Following the CJEU Schrems II judgment, transfers under SCCs require a transfer impact assessment evaluating local-law access risks.
- **Binding Corporate Rules** [tn604] **(Art. 47)**: Binding Corporate Rules (BCRs) are internal data-protection rules adopted by a multinational group of undertakings or enterprises engaged in a joint economic activity, approved by a competent supervisory authority. BCRs allow intra-group transfers without further safeguard. The approval process typically takes 12–24 months and the BCRs must include the elements set out in Article 47(2).
- **Derogations for Specific Situations** [tn605] **(Art. 49)**: In the absence of an adequacy decision or appropriate safeguards, a transfer may be made on a one-off, non-systematic basis under one of seven specific derogations: explicit consent after being informed of risks; necessary for performance of a contract with the data subject; necessary for important reasons of public interest; necessary for the establishment, exercise, or defence of legal claims; necessary to protect vital interests where the data subject is unable to consent; transfers from a public register; or,

narrowly, where compelling legitimate interests apply (Art. 49(1) second subparagraph).

Enforcement [tn500]: Remedies, Liability, and Fines

The GDPR provides multiple enforcement pathways for data subjects and supervisory authorities. **Obligation breaches** [te107] by controllers failing to meet their **obligations** [tn300] can trigger complaints, judicial actions, and significant administrative fines. A **risk found during processing requires notification** [te304] under the breach notification duty [1].

- **Complaint to Authority** [tn501] (**Art. 77**): Every data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work, or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes the GDPR
- **Judicial Remedy** [tn502] (**Art. 79**): Each data subject has the right to an effective judicial remedy where he or she considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the Regulation
- **Right to Compensation** [tn503] (**Art. 82**): Any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered
- **Fines: up to €10M / 2%** [tn504] (**Art. 83(4)**): Infringements of controller and processor obligations (including Art. 25, 28, 30, 33, 35), certification body obligations, and monitoring body obligations are subject to administrative fines of up to €10,000,000 or up to 2% of total worldwide annual turnover of the preceding financial year, whichever is higher

- **Fines: up to €20M / 4% [tn505] (Art. 83(5)):** Infringements of the basic principles for processing (Art. 5–7), data subject rights (Art. 12–22), transfer provisions (Art. 44–49), and non-compliance with supervisory authority orders are subject to administrative fines of up to €20,000,000 or up to 4% of total worldwide annual turnover, whichever is higher

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation). *Official Journal of the European Union*, L 119. [\[Source\]](#)
2. European Data Protection Board. Guidelines, Recommendations & Best Practices. [\[Source\]](#)

Frequently Asked Questions

Q: What is the GDPR?

A: The GDPR (Regulation (EU) 2016/679) is the European Union's comprehensive data protection regulation, applicable since 25 May 2018. It establishes rules for the processing of personal data by controllers and processors, built on seven core [principles \[tn100\]](#) (Art. 5) and six [lawful bases \[tn200\]](#) for processing (Art. 6), and grants individuals extensive [data subject rights \[tn400\]](#).

Q: Does GDPR apply to my company?

A: Article 3 sets out two scope tests. First, GDPR applies whenever processing happens in the context of the activities of an establishment of a controller or processor in the Union — even if the processing itself takes place outside the Union (Art. 3(1)). Second, GDPR applies to controllers or processors not established in the Union when processing relates to (a) the offering of goods or services to data subjects in the Union, or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union (Art. 3(2)). Mere accessibility of a website

from the Union is not sufficient on its own; targeting evidence (e.g., language, currency, top-level domain, EU-specific marketing) is required. Worked examples: a US SaaS targeting EU customers — yes; a non-EU company with no EU offerings or monitoring — no; an EU-established processor for a non-EU controller — yes for the EU establishment's activities.

Q: What are the lawful bases for processing personal data?

A: Article 6 sets out six lawful bases: **consent** [tn201] of the data subject, **contract performance** [tn202], **legal obligation** [tn203], protection of **vital interests** [tn204], **public interest** [tn205] or official authority, and **legitimate interests** [tn206] of the controller or a third party. At least one basis must apply before any processing can begin.

Q: What rights do individuals have under the GDPR?

A: Individuals have seven key rights: **access** [tn401] to their data (Art. 15), **rectification** [tn402] of inaccurate data (Art. 16), **erasure** [tn403] (Art. 17), **restriction** [tn404] of processing (Art. 18), **data portability** [tn405] (Art. 20), the right to **object** [tn406] (Art. 21), and protection against **automated decision-making** [tn407] (Art. 22).

Q: What are the fines for GDPR violations?

A: Fines are tiered by severity. Violations of **controller obligations** [tn300] such as **privacy by design** [tn301], **records of processing** [tn303], and **breach notification** [tn304] can result in **fines up to €10M or 2%** [tn504] of global turnover. More serious violations of processing principles and data subject rights can result in **fines up to €20M or 4%** [tn505] of global turnover.

Q: What must a controller do in case of a data breach?

A: Under Art. 33, the controller must notify the competent supervisory authority of a **personal data breach** [tn304] without undue delay and, where feasible, within 72 hours. If the breach is likely to result in a high risk to the rights of individuals, the controller must also notify the affected data subjects directly (Art. 34). The controller should also carry out a **data protection impact assessment** [tn305] for high-risk processing activities and maintain **processor requirements** [tn302] in contracts.