

General Data Protection Regulation (GDPR)

Vendasta Technologies Inc.

Last modified: April 2, 2026

GDPR GUIDELINES Last modified: April 2, 2026

What is the GDPR?

General Data Privacy Regulation ("GDPR") is the European Union ("EU") privacy legislation, which took effect on May 25, 2018, replacing the 1995 EU Data Protection Directive. A binding regulation that is written directly into Member States' laws designed to regulate how organizations collect, handle, and protect personal data of EU residents. The GDPR is to strengthen privacy rights by giving data subjects control of how their personal data is obtained, used, and shared. It is the strongest global privacy law in effect today.

The GDPR set out with three main goals in mind:

1. Establish and protect the fundamental privacy rights of individuals.
2. Unify privacy laws across the EU by replacing the 28 individual EU member state laws and the previous 1995 Data Protection Directive.
3. Adapt privacy laws that reflect the change the technology landscape has made on personal data over the last 25 years.

GDPR Terminology – Key Terms

1. Data Subject is a natural person who can be directly or indirectly identified, in particular by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. Personal Data means any information (objective and/or subjective) relating to an identified or identifiable natural person ("data subject"); such as information relating to their private, professional, or public life, including a name, email address, photos, bank statements, online identifiers etc.
3. Processing means anything done to personal data, whether or not by automated means. It involves any automated or manual operation or set of operations performed on personal data or sets of personal data, including the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval or accessing or viewing, consultation, use, analyzing, combining, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, deletion or destruction and so on.
4. Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes, lawful basis and means of the processing of personal data;
5. Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
6. Consent refers to any "freely given, specific, informed and unambiguous indication" that the data subject agrees to the processing of personal data related to them. Data subjects can provide consent with either a statement or explicit affirmative action.
7. Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

disclosure of, or access to, personal data transmitted, stored or otherwise processed;

8. Pseudonymous Data is personal data that cannot be tied to a specific data subject without additional information that is stored separately, provided that such additional information is kept separately.

GDPR Scope

The GDPR applies to organizations that are based in the EU, even if the PI is being stored or used outside of the EU, and to organizations that are not in the EU if: (1) the organization offers goods or services to individuals in the EU; or (2) the organization monitors their online behavior. To decide whether we are covered under the GDPR, we need to consider both the 'territorial scope' and the 'material scope'.

What are the GDPR's key principles?

Significant changes in GDPR:

1. The purpose for Data Processing: GDPR requires that there must be at least one of the following legal purposes before personal data of data subjects can be processed: Consent, Contract, Legal obligation, Vital interests, Public interest, Legitimate interests.

2. Compliance Obligations: Both, data controllers and also data processors are responsible for demonstrating compliance not just to the regulator; also to data subjects if necessary.

3. Breach Notifications: Data Controllers must report any data breach to the appropriate data protection authority as soon as possible and not later than 72 hours after becoming aware of the breach. Data subjects should be informed immediately of any breach that will cause high harm to them.

4. Privacy by Design: Companies must follow Privacy by Design principles and implement appropriate technical and organizational measures in an effective way to meet the requirements of the GDPR and protect the rights of data subjects.

5. Data Privacy Impact Assessment (DPIA): There is an obligation to perform a Data Privacy Impact Assessment (DPIA) when data processing may use "new technologies" or is risky, so that potential privacy issues can be identified before they arise.

6. Data Subject Rights: The "right of portability" and the "right to be forgotten" are two new privacy rights granted to individuals under the GDPR. Upon request, individuals will be able to transfer all data from one provider of goods or services to another. Under the "right to be forgotten," individuals can have their personal data erased upon request in certain circumstances.

7. One-Stop Shop: The GDPR's new "one-stop-shop" provision, under which organizations with offices in multiple EU countries will have a "lead supervisory authority" to act as a central point of enforcement.

8. Appointment of a Data Protection/Privacy Officer: A DPO is required for any enterprise with over 250 employees or for any enterprise processing the personal data of over 5,000 data subjects in any 12-month period.

9. Enforcement: Under the GDPR, organizations can be fined up to €20 million or 4% of a company's annual global revenue, based on the seriousness of the breach and damages incurred.

Data Subject Rights under GDPR

The GDPR outlines eight fundamental data subject rights, plus the right to withdraw consent:

- Right to be informed: Data subjects have the right to be informed about the collection and use of their personal data.
- Right of access: Data subjects have the right to access their personal data and supplementary information.
- Right to be forgotten / Right to erasure: Data subjects have the right to request their personal data be deleted. Note that this is not an absolute right and may be subject to exemptions based on certain laws.
- Right for data portability: Data subjects have the right to ask for their data to be transferred to another controller or provided to them in a machine-readable electronic format.
- Right to restrict Processing: Data subjects have the right to request the restriction or suppression of their personal data.
- Right to withdraw consent: Data subjects have the right to withdraw previously given consent to process their personal data.
- Right to object: Data subjects have the right to object to the processing of their personal data.
- Right to object to automated processing: Data subjects have the right to object to decisions being made with their data solely based on automated decision making or profiling.

What is Vendasta doing to comply with GDPR?

Safeguarding the privacy and security of personal information is a priority for Vendasta. We have invested time and resources in preparation for the European General Data Protection Regulation (GDPR). At Vendasta we understand that GDPR is an ongoing governance commitment and as such, we will ensure that Vendasta is and remains fully compliant. For additional information please contact us at: privacy@vendasta.com.

As part of this GDPR program, we are reviewing and enhancing our platform, products, solutions and services so as to address our obligations as processors.

Data processing: Vendasta processes personal data to the extent necessary and in accordance with applicable regional privacy laws including GDPR. Vendasta ensures that there is an applicable legal basis for all processing activities.

Legal documentation: Vendasta has ensured that all legal documents—including, without limitation, our Terms of Service, Privacy Policy, and Cookie Policy available on our Trust Center at trust.vendasta.com—are compliant with the GDPR.

Data protection and privacy awareness, education and training: Vendasta has ongoing educational, training and awareness programs for its personnel and employees with regards to the data security, risks, and privacy regulations including GDPR.

Technical, organizational and security standards: Vendasta is committed to continuously improving the security of our platform and protecting the privacy of our users. We take all reasonable precautions, technical and organizational security measures to safeguard and protect personal data. As a part of this effort, we also run a vulnerability disclosure program (VDP) through HackerOne. For additional information please contact us at: security@vendasta.com.

Consent – marketing email campaigns: We are committed to making continual improvements to the email experience for both our partners and their customers. We provide end users the ability to unsubscribe from marketing campaign emails and allow users to adjust notification preferences within the platform.

Data breach response procedure: To mitigate the risks to data subjects from any data breach and to implement GDPR

breach notification to the extent required under the applicable laws, Vendasta has implemented a Data Breach Incident response procedure, which is available for review on our Trust Center at trust.vendasta.com.

Data subject rights (DSR) request handling procedure: To ensure that all DSR requests are handled in a correct and timely manner, Vendasta has implemented a set of DSR request handling procedures, which is available for review on our Trust Center at trust.vendasta.com.

Data Subject Rights: In accordance with GDPR, data subjects may exercise the following rights: (i) request to access Personal Data; (ii) request the rectification of Personal Data; (iii) object to processing of Personal Data; (iv) right to withdraw consent (to the extent applicable); (v) request to exercise right of data portability; (vi) request the erasure of Personal Data; and (vii) request to restrict processing of Personal Data.

Vendasta understands how important and complicated these requests can be and manual processes are prone to human error. We have committed ourselves to provide self-serve access to our partners and users so that they can manage their requests conveniently and efficiently. Alternatively, in order to exercise any of the above rights please contact us at privacy@vendasta.com.

You also have the right to lodge a complaint with the supervisory authority in your country of residence, place of work or the country in which an alleged infringement of data protection law has occurred within the EU.

GDPR awareness: Need help? Email us at privacy@vendasta.com. Disclaimer: This website is neither legal advice for your company in complying with GDPR/other data privacy laws nor a magnum opus on EU/EEA data privacy. What we are providing is background information to help you better understand how we, at Vendasta, have addressed some important legal points. This legal content is not the same as legal advice, where an attorney applies the law to your specific circumstances, so we insist that you consult an attorney if you'd like advice on your interpretation of this information or its accuracy.

KEY CHANGES IN THE GDPR Last modified: February 8, 2023

The GDPR does not fundamentally change any of the core rules in the 1995 Data Protection Directive. Instead, it extends the Directive's requirements significantly by introducing a range of new obligations for organizations to support those core rules.

GDPR Scope

1. The Regulation is directly effective in all EU member states from 25 May 2018 without the need for further national legislation. However, some national divergences will remain because member states have limited rights to amend some of the obligations under the Regulation.

2. One-stop-shop: Organizations that are established in multiple EU states will be able to nominate a single national data protection authority to act as the lead regulator for all of that organization's data protection compliance issues in the EU.

3. The GDPR applies to all organizations – whether commercial business or public authority – that collect, store or process the personal data of EU individuals, "whatever their nationality or residence". Organizations based outside the EU that

monitor or offer goods and services to individuals in the EU will have to observe the Regulation.

4. The GDPR directly regulates data processors – Direct obligations are imposed on data processors as opposed to data controllers under the previous EU law. Both data controllers and also data processors are responsible for demonstrating compliance not just to the regulator; also to data subjects if necessary. These legal obligations include: processing personal data only in accordance with the controller's instructions, restrictions on data sharing without the controller's consent, return/destruction of personal data upon cessation of relationship, implementing appropriate security measures, maintaining records of personal data, and how it is processed, and providing a much higher level of legal liability should the organization be breached.

Data Subject Rights

Sensitive personal data: Stricter controls have been placed on the processing of sensitive personal data, whose definition has been expanded to include genetic and biometric data, such as fingerprints and retina scans. Personal data also includes unique online identifiers, including IP addresses and mobile device identifiers, and geolocation data about an individual.

The purpose for Data Processing: GDPR requires that there must be at least one of the following legal purposes before personal data of data subjects can be processed: Consent, Contract, Legal obligation, Vital interests, Public interest, Legitimate interests.

Consent: Data subjects' consent to process their personal data must be given freely and for the purposes specified. Consent forms should be laid out in clear and simple terms, outlining the purpose of data collection and processing, and onward data transfers to third parties. Silence or inactivity does not constitute consent. Consent from a child under 16 for online services is only valid if authorized by a parent.

Data subjects' rights under GDPR:

1. Right to be Informed: Organizations must inform data subjects what personal data of theirs is being collected, how it's being used, how long it will be kept, and whether it will be shared with any third parties.

2. Right of access: The GDPR requires companies to provide, at the data subject's request, confirmation as to whether personal data pertaining to them is being processed, along with the information in a concise, transparent, intelligible, and easily accessible form.

3. Right to object: Data subjects can at any time object to the processing of their personal data especially if the processing is for marketing purposes including profiling.

4. Right to rectification: Data subjects have the right to without undue delay to the rectification of inaccurate or incomplete personal data concerning them.

5. Right to erasure ("right to be forgotten"): This right enables the data subject to demand complete deletion and removal of personal data without undue delay in circumstances including: data no longer needed for the purpose collected; withdrawal of consent; data subject exercises right to object; unlawful processing; personal data has to be erased to comply with a legal obligation; or if the personal data relates to a child.

6. Right to restriction of processing: Data subjects have the right to request the Controller to stop processing of personal data in circumstances including: accuracy of personal data is contested; continuous processing will be unlawful and the data subject opts for restriction; the controller no longer needs personal data but is still required by the data subject for legal

claims; or the data subject has exercised right to object pending verification.

7. Right to Data Portability: In certain cases, the GDPR requires companies to provide mechanisms for a data subject to receive any previously provided personal data in a structured, commonly used, and machine-readable format.

8. Rights Related to Automated Individual Decision-Making and Profiling: This is a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects data subjects.

Accountability

1. Records of data processing: Data controllers and data processors that process personal data need to comply with a number of obligations to demonstrate compliance including maintaining adequate documentation, by keeping records of data processing activities, appropriate security standards, data protection impact assessments, rules on international data transfers and making these available to the supervisory authority on request.

2. Data protection impact assessments (DPIAs) are now a prerequisite before processing personal data using "new technologies" or that is likely to result in a high risk to the rights and freedoms of individuals.

3. Data protection and privacy by design require organizations to follow Privacy by Design principles and to embed data protection measures throughout the design phase of a new product, system, or business process, rather than treating it as an afterthought.

4. Appointment of a Data Protection/Privacy Officer: A DPO is required for any enterprise with over 250 employees or for any enterprise processing the personal data of over 5,000 data subjects in any 12-month period.

5. Data breach notification: The GDPR introduces a specific obligation on organizations to report any data breach to their supervisory authority as soon as possible and not later than 72 hours of becoming aware of it.

6. Enforcement: Under the GDPR, the maximum penalties are permitted to attract attention and encourage compliance – regulators are able to impose penalties on organizations for non-compliance of up to 4% of annual global turnover or €20 million, whichever is higher.

GDPR COMPLIANCE Last modified: February 8, 2023

Territorial Scope

Just one of these criteria must be met for the GDPR to be applicable:

1. GDPR applies to the processing of personal data in the context of the activities of a controller or a processor established in the EU, regardless of whether the processing takes place in the EU or not. The presence of a single representative may be sufficient to satisfy the presence of an establishment.

2. Processing the personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to (a) offering goods or services to data subjects in the EU, irrespective of whether a payment of the data subject is required and (b) monitoring their behaviour in the EU.

3. Processing of personal data by a controller not established in the EU but in a place where member state law applies by

virtue of public international law.

Material Scope

Activities must also fall within the material scope of the GDPR, as set out in Article 2:

1. Processing personal data wholly or partly by automated means (without or partly without human intervention).
2. Processing, other than by automated means of personal data, that forms part of a filing system. This covers most activities done with data, including collecting, recording, storing, accessing or viewing, using, analyzing, combining, disclosing or deleting personal data.

Exclusions to the material scope – The exclusions for data processing not regulated by the GDPR for purposes that include:

1. Activities outside the scope of EU law: for example, national security activities
2. Law enforcement and public security
3. Purely personal or household activities.

GDPR PRINCIPLES Last modified: February 8, 2023

The General Data Protection Regulation (GDPR) sets out seven principles for the lawful processing of personal data. These guiding principles are at the center of the GDPR and compliant processing. We are obliged to comply with these principles for all personal data processing activities protected under the GDPR. The seven principles are: 1. Lawfulness, fairness, and transparency; 2. Purpose limitation; 3. Data minimization; 4. Accuracy; 5. Storage limitation; 6. Integrity and confidentiality; 7. Accountability.

1. Lawfulness, Fairness, and Transparency Principle

This principle concerns, in particular, information to the data subjects on the identity of the controller and the purpose of the processing, including further information to ensure fair and transparent processing and the right to obtain confirmation and communication of personal data concerning them, and on the risks, rules, safeguards, and rights in relation to the processing of personal data.

Lawfulness: Lawfulness is related to two things in regards to the GDPR: choosing a proper lawful basis for processing personal data and ensuring that the processing itself is not in breach of any other law. Before processing personal data, we should always identify an appropriate lawful base or grounds for the processing and document it. The six lawful bases for processing personal data are: (1) Consent; (2) Contract; (3) Legal obligation; (4) Vital interests; (5) Public interest; (6) Legitimate interests.

Fairness: Fairness means that we must process personal data only in a way that is reasonably expected from us. Collecting, storing, and processing personal data that were collected in a deceiving way or by misleading the data subject will lead to a breach of the fairness principle.

Transparency: At the time of data collection, the transparency principle requires us to have clear, open and honest

communication towards data subjects about how their personal data is being collected, used, consulted, or otherwise processed. Any information and communication should be easily accessible and written in clear and plain language.

2. Purpose Limitation Principle

Purpose limitation means personal data must be collected for specified, explicit, and legitimate purposes only and it should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. The purpose for processing data must be clearly established and documented from the outset. We can only use personal data for the purpose we have collected it for in the first place. Any additional processing has to be compatible with the original purpose, or we must obtain consent from a data subject.

3. Data Minimization Principle

The data minimization principle limits the data controller to collect, store, process, and use only personal information that is necessary to provide the required service or fulfill a specific purpose. This means we will have to identify the minimal amount of data needed to fulfill the purpose of collecting personal data in the first place in order to ensure that the processing is: adequate – sufficient to properly fulfill the stated purpose; relevant – has a rational link to that purpose; and limited to what is necessary – not more than what is needed to achieve the purpose.

Data minimization has two major benefits:

- In the event of a data breach, limited and minimal data is exposed, thus reducing the scope and impact of the breach;
- Data minimisation makes it easy to keep data accurate and up to date.

4. Accuracy Principle

The accuracy of personal data is integral to data protection. It should not be incorrect or misleading as to any matter of fact. This means that we are responsible for taking all reasonable measures to ensure that the personal data we hold is correct and accurate. Inaccurate personal data should be either rectified or erased without delay. Also, data subjects have the right to rectification that grants them the ability to demand inaccurate personal data to be erased or rectified.

5. Storage Limitation Principle

The storage limitation principle ensures that personal data stored is limited to a strict minimum period, preventing us from keeping it for longer than we need to. Therefore, we must be able to justify why we are keeping it as well as the length of time we are storing it for. A periodic review of personal data will help identify data that is no longer needed so it can be erased or anonymised. Data retention policy and data deletion schedules can help us comply with the storage limitation principle.

6. Integrity and Confidentiality Principle

The integrity and confidentiality principle, also known as the security principle, is tightly connected with the security and confidentiality of the personal data as well as the equipment used for data processing. This principle goes beyond the way we store or transmit data to cover every aspect of personal data processing. It ensures appropriate security of the personal data against any intentional or unintentional risks, unauthorized third-party access, malicious attacks, unauthorized or unlawful processing, accidental loss, destruction or damage and exploitation of data, using appropriate technical and organizational measures.

7. Accountability Principle

The accountability principle means that we, as a data controller and also as data processor, are responsible for what we do with personal data and how we comply with all of the above-mentioned GDPR principles. Most importantly, we are responsible for demonstrating compliance not just to the regulator but also to data subjects if necessary. This means we should complete the following:

- Keep evidence of the steps we take to comply with GDPR;
- Document of processing activities;
- Implement technical and organizational measures;
- Implement data protection policies and procedures;
- Prepare data protection impact assessments (if we had to conduct one); and
- Appoint a data protection and privacy officer.

Why are these principles of GDPR important? GDPR principles represent the main building blocks of data protection and set the tone for the rest of the regulation. Any violation of GDPR principles will accrue hefty administrative fines—up to €20 million or 4% of the total worldwide annual turnover, whichever is higher.