PrestaShop

GDPR Key Info

Whitepaper

IMPORTANT

This document is not intended to offer any legal advice, simply to provide comprehensive information about the provisions of the European regulation of 27 April 2016 (General Data Protection Regulation).

PrestaShop cannot answer any specific questions from its users about implementing the aforementioned regulation's provisions.

If you have any questions, we recommend you contact a lawyer specialising in personal data legislation questions.

The **2016/679 European Regulation of 27 April 2016** regarding personal data protection will apply from 25 May 2018.

Consequently, if you have not considered it already, it is high time that you think about the practical implications of this regulation.

This article is intended to give you a key to understanding the main principles restated or created by these new provisions, which are better known by their acronym: GDPR.

Why this regulation?

These new provisions create a unified European framework for personal data protection which until now has been governed by the French Data Protection Act of 6 January 1978 and the EU directive 95/46/CE adopted in 1995 and transposed into French law with Law 2004-801 of 6 August 2004.

These texts established the principles relating to how the personal data of natural persons is collected and processed: consent from the person, purpose prior to collection, data security, transfer guidelines, etc.

Adopted in the late 1970s and 1990s, these texts could not foresee the explosion of personal computing, the internet, social networks, smart devices, cloud computing, and more, which have revealed the limitations of these measures and made it necessary to update the legislation.

Furthermore, transposing the directive into the laws of the various EU member states resulted in divergences in national legislations, which need to be standardised.

Consequently, in 2012 the EU started drafting proposed regulations that would not need transposing and would enable greater standardisation, to replace the directive. It was adopted on 27 April 2016.

What is the scope of this regulation?

The GDPR is intended to apply to all processing of personal data, whether automated or manual.

Processing of data is defined as an operation or set of operations carried out using automated or manual processes and applied to personal data or data sets.

E.g. Collection, storage, modification, extraction, viewing, use, communication, destruction, etc.

Personal data comprises all information relating to a natural person and enabling that person to be directly or indirectly identified.

E.g. Identity (full name), email address, IP address, telephone number, location data, consumer habits, etc.

Given the extent of these concepts and your e-commerce business, it is highly likely that you process personal data.

Furthermore, the other regulation

application criteria relates to processing personal data with a geographical link to the European Union region.

In practical terms, the GDPR will apply when:

The controller or its processor has an establishment located in the European Union region.

The controller or its processor does not have an establishment located in the European Union region but the persons whose data is being processed are located there.

In other words, regardless of whether your company is located in the European Union region or not, this regulation applies to the majority of companies!

What does the regulation cover? How can you comply with it?

The regulation restates or creates obligations imposed on controllers (I) who must ensure compliance with those obligations by implementing various technical and organisational measures that fall under “accountability” (II).

Lastly, what is new in this regulation is the greater role played by the regulatory authority and the severity of sanctions in the event of the controller’s failure to comply with the provisions (III)..

I. OBLIGATIONS INCUMBENT ON CONTROLLERS

The regulation requires the controller to comply with the obligations relating to:
- Processing **(A)**
- Respecting the rights of data subjects **(B)**

A. Processing obligations under the regulation

1. Applicable basic principles for processing of personal data

Article 5 of the GDPR lists the various principles relating to processing of personal data.

Under this principle, data must be:

a - Processed in a **lawful (see I.2 below), fair and transparent manner.**

b – Collected for a **set, explicit, legitimate** purpose and not reused later for a purpose that is incompatible with the intended purpose at the time of collection.

> To know if planned later processing is compatible or not with the purpose stated when initially collecting the data, you must consider various criteria such as: the existence of a link between the initial and later purposes (for example, later archiving of data to meet legal obligations or for statistical purposes), the nature of the processed data, the relationship between the data subject and controller (e.g. the existence of a contact), etc.

c – **Appropriate, relevant and limited** with regard to the purpose for which they are processed (principle of minimisation).

This means only collecting the data required for the implemented processing purpose.

d – **Accurate** and, where appropriate, updated **(see I.B below regarding this)**.

e – **Stored** in a form that enables the data subject to be identified and f**or a period not exceeding the time required for the purpose for which the data is processed.**

Personal data must be stored in a form that enables the data subject to be identified, only for the time required to accomplish the purpose of their collection. The data storage period and start date are freely determined by the controller as long as that period does not exceed the time required for the purpose for which the data is processed. These data constitute what are called the controller's **"current" archives**.

As soon as they are no longer useful, the data must immediately be deleted.

There is an exception: some situations require that the **data be archived**. These are "**intermediate" archives** which comprise "data that preserve their administrative interest for the departments involved."

The storage period for these data, in archive form and for archiving purposes, is set by legal and regulatory provisions: **CNIL (French National Commission for Information Technology and Civil Liberties) repository of storage periods**.

Data that is stored to meet legal and regulatory obligations must be archived for the period required to accomplish that obligation and be deleted as soon as the reason justifying their archival no longer exists.

Lastly, the controller also has the option (not obligation, unlike for intermediate archive data) of storing certain data, including those of historical, scientific or statistical interest. These data comprise the controller's permanent archives.

The choice of archive method is decided by the file manager, however certain technical and organisational measures must still be taken to protect the data and ensure a suitable level of security given the nature of the data.

For intermediate archives, the **CNIL deliberation on 11 October 2005 on electronic archiving terms** recommends limiting access to a specific server (for example, to the legal department) and "at the least, isolating archived data using a logical separation (managing access rights and authorisations)."

Regarding permanent archives, CNIL recommends storing them "on an independent medium that cannot be accessed by production systems, with only single, occasional distinct access authorised for a specific reason by a specific department that holds sole authorisation to consult this type of archive."

CNIL also recommends "implementing archived data consultation tracking systems" as well as using "anonymisation procedures, in particular for sensitive data (...)."

See II below regarding this.

f – Processed in such a way as to ensure the data subjects enjoy appropriate security for their aforementioned data, through technical and/or organisational measures **(See II below regarding this)**

2. Processing-related obligations: the principle of "lawful" processing

As stated in 1 a) of Article 5 of the regulation, processing of personal data must be lawful.

Yet Article 6 of the GDPR states that processing is only lawful when it is implemented based on one of the following alternative conditions:

- The person has given their consent for the processing.

The controller must be able to prove the data subject gave consent to the processing operation of their own free will (the person must have a choice of consenting to or refusing the processing but must also be able to withdraw consent or refuse to give consent without being penalised) and it must be informed consent (after being informed in a clear, comprehensive manner about the processing terms and characteristics).

- Processing is required to perform a contract or precontractual measures.

For processing on this basis, the data subject must be party to the contract.

- Processing is required for a legal obligation to which the controller is subject or for a task carried out in the public interest or in the exercise of official authority vested in the controller

Your processing must have a basis in European Union or EU member state law.

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

Processing can only fall under this area if it is motivated by a medical emergency and is required for administering the appropriate treatment.

- 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 which require protection of personal data.

The regulation gives examples of purposes that show the controller's legitimate interest (e.g. canvassing or fraud prevention) but you should carry out a case by case assessment of each processing operation intended to be implemented on this basis.

If you want to implement processing on this basis, you must think about whether or not your legitimate interest prevails over the interests of the data subject for their data to not be processed.

To answer this question, a set of criteria must be assessed: relevance and reality of interests in the presence,

type and volume of processed data, repercussions of processing on data subjects, processing terms (sharing, security, etc.), safeguards provided to data subjects (encoding method), etc.

In addition to the processing-specific obligations, the regulation also covers obligations relating to the rights of data subjects.

B. Obligations relating to the rights of data subjects

In order to meet the obligations relating to the rights of data subjects, you must only collect and process their data after informing them through an easily accessible message (e.g. confidentiality policy available online) that is easy to understand, meaning it is written in clear and simple terms.

The GDPR lists all the **information that must be issued in writing or other suitable method** (including electronic) to the data subject affected by initial and further (when applicable) data processing **at the time the data are obtained**, including:

- The identity and contact details of the controller and its representative, and the contact details of the data protection officer (when required).

- The basis for the processing (see Article 6 of the GDPR) and the consequences for the data subject of not providing that data.

- The existence of the right to withdraw consent, the right to access, correct, delete and limit data, the right to object, and the right to data portability.

IMPORTANT: Information relating to the right to object must be given to the data subject in the first communication with that person and must be presented separate from all other information.

- The data recipient, the existence of transfers outside the EU and the associated safeguards.
- The data storage period.
- The right to lodge a complaint with a supervisory authority (in France, the CNIL).
- The existence (where appropriate) of any automated decision, logic, importance or consequence of the processing.

TO CONSIDER: You are exempt from this obligation to inform if the data subject already has the information.

In addition to the right to information about the items listed above, people whose data is collected have the right to request certain actions be performed, including:

- The right to access their data, Article 15 of the GDPR
In practice, in the situation where the data subject sends you such a request, you must tell that person if the data in question have been processed or not, and where appropriate provide a copy of the data as well as information on the characteristics of the processing.

IMPORTANT: People who exercise this right to access their data must be able to obtain all data concerning themselves.

- The right to obtain rectification of inaccurate personal data and have incomplete data completed, (Article 16 of the GDPR) - See II.1 below regarding this.

- **The right to erasure**, which can occur on the grounds listed in Article 17 of the GDPR

- **The right to restriction**, which can also occur on the grounds listed in Article 18 of the GDPR

- **The right to data portability,** Article 20 of the GDPR: for the data subject, this consists of the right to receive the personal data they provided to a controller, in a structured, commonly used and machine-readable format, and the right to transmit those data to another controller without hindrance from the controller to whom the data were initially provided. If certain conditions are met (technical possibilities, consent- or contract-based processing carried out using automated processes), the data subject may ask that their data be directly sent from one controller to another.

To find out more about the right to portability: G29 Guidelines adopted on 13 December 2016 & FAQ

- The right to object, Article 21 of the GDPR.
The data subject has the right to object to the use of their data for canvassing purposes and, under certain conditions, has the right to request that the controller cease processing their data.

- The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects them.

If there are any exceptions to this right, you must still allow the data subject the right to obtain human intervention, to express his or her point of view and to contest the decision - **Article 22** of the GDPR

IMPORTANT

If you receive a request relating to exercising one or more of these rights, you must reply to the data subject as soon as possible, and this must occur within one month of receiving the request. This timeframe may be extended in certain situations but you must inform the data subject of this.

If you do not reply to the data subject, you must inform them within one month of the reason for your refusal and their right to lodge a complaint with the CNIL or seek a judicial remedy.

As a controller, you must show that you have met all these obligations.

To do this, you must be able to document all internal procedures and mechanisms. This is the principle of "accountability" **(II).**

II.

II. IMPLEMENTING SUITABLE TECHNICAL AND ORGANISATIONAL MEASURES TO COMPLY WITH THE REGULATION'S PROVISIONS

The **general security of processing obligation** in article 32 of the GDPR **requires** both the controller and processor to **implement all necessary, appropriate measures to ensure a suitable level of security,** taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects.

This general obligation is met through accountability, which means:

Implementing the organisational and technical measures that can ensure the processing occurs in a manner that complies with the Regulation (1).
Identification and documentation of the measures implemented (2).

In practice, this means the controller must be accountable to the authorities and enable the latter to verify the measures taken.

To date, the prerequisite to implementing personal data processing in France consisted of submitting the prerequisite formalities (declarations or requests for authorisation) to the CNIL.

The regulation changes this logic by making the parties involved in the processing operation responsible as they must now take all necessary measures to prove their practices comply with the regulation's provisions.

In order to meet this obligation of security, the controller must provide guarantees of a high level of personal data protection for data subjects.

To do this, you must organise internal procedures and adapt tools.

1. Organising internal procedures and adapting tools

Article 25 of the GDPR introduces concepts such as "privacy by design" and "privacy by default".

Privacy by design consists of taking the necessary and appropriate measures to incorporate data protection obligations when designing projects and ensuring that the developed tools comply throughout their period of use.

In practice, this is a logic of anticipating legal obligations

relating to personal data protection when making the processing choice in order to incorporate them when implementing that processing.

In order to incorporate these legal obligations regarding personal data protection, it is helpful to create specifications that translate them into technical requirements.

Privacy by default consists of implementing operational and technical measures so you can guarantee to data subjects that only the data required for the intended processing purpose is collected and processed, and that these operations sit within the highest level of protection possible.

What specific measures can be implemented?

- Reducing the quantity of data collected and the scope of processing.
- Pseudonymising the collected data as soon as possible.
- Enabling data subjects to exercise their rights (see II above).
- Implementing systems to ensure the security of the collected data and continue developing them.

- Managing requests from data subjects

Controllers must ensure that procedures are in place to enable data subjects to exercise their rights and process their requests within the timeframes stated in the regulation (see II above).

- Appointing a data protection officer (DPO)

The DPO plays a crucial role in the accountability approach insomuch as the officer informs and advises the decision makers on security measures to implement and checks that they meet the regulation's requirements.

What specific measures can be implemented?

- Appoint people in charge of responding to the requests and complaints you receive.
- Draft model response templates so you can reply quickly to people.
- Implement the necessary tools to efficiently respond to certain requests (including the right to access and to portability), with tools for exporting all of a person's data, for instance.

IS IT MANDATORY TO APPOINT A DPO?

Article 37 of the GDPR lists the obligation to appoint a DPO in certain situations, specifically when:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale, or
- the core activities of the controller or the processor consist of processing on a large scale the special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Outside of these situations, appointing a DPO is optional unless the European Union or EU member state law requires it.

IMPORTANT

The terms of Article 37 of the GDPR are sufficiently broad for this obligation to be interpreted to a great extent by the supervisory authorities. Furthermore, looking at the guidelines and FAQs in the G29 of 13 December 2016, appointing a DPO is strongly encouraged even when it is not mandatory.

- Ensuring processing security and anticipating violations

The controller must ensure the data's security, identify processing-related risks and take all necessary preventative measures.

In addition to prevention, the regulation requires the controller to implement suitable procedures to be able to identify all personal data violations and, where appropriate, notify the supervisory authority:

Article 33 of the GDPR - Notifying the supervisory authority

- Obligation to notify of security breaches as quickly as possible, preferably within 72 hours of noticing the breach + reasons for the delay if longer than 72 hours.
- Notification content stated in Article 33 of the GDPR.

Article 34 of the GDPR - Notifying the data subject

if the violation is likely to result in greater risk to a natural person's rights and freedoms.

What specific measures can be implemented?

- Encode the data (including for transfers).
- Restrict and monitor physical and digital access to the data.
- Regularly carry out back-ups on different, secure media.
- Install firewalls and anti-virus programs.

Furthermore, in order to quickly meet the requirements set by articles 33 and 34 of the GDPR, we recommend you:

- Implement a security breach management procedure that states the various steps: identifying and rectifying the breach, gathering technical and legal proof, making a declaration to the police, declaring loss to the insurance company, notifying the supervisory authority and, when required, notifying the data subject, and lastly, potentially notifying the public about the security breach.
- Draft model templates for notifying the supervisory authority, the data subject(s) and the public.
- Document a security breach register.

Educating and training all your employees

Given the value represented by personal data and the fact they are handled by everyone within the company, the controller must educate all employees on the topic of protecting that data. You could, for example, implement a communication strategy, charter or even procedures regarding their use.

Important:

In order to help professionals achieve compliance, CNIL publishes a **guide recapping the fundamental measures** that must be systematically implemented.
Another aspect of accountability consists of drafting the necessary documentation for ensuring the traceability of the measures taken by the controller.

2. Accounting for measures taken

- Keeping a record of processing activities – Article 30 of the GDPR

The GDPR requires that processing be listed in the "Record of Processing Activities".

This record must be in written form and must list all processing activity, whether new or existing. It must regularly be updated and provided to the supervisory authority on request.

The information in this record will vary depending on whether it is the controller's or processor's record of processing activities.

Important: The regulation does not require entities with fewer than 250 employees to hold a record, however this exception does not apply when the processing is likely to pose a risk to the data subjects' rights and freedoms or if it is not occasional.

Therefore, any processing carried out which has a certain ongoing nature must be transposed to the record, regardless of how many employees the entity has.

In other words, the scope of this exception is considerably reduced.

Completing this record requires various actions to first be implemented which identify the processing carried out.

In order to support companies, CNIL has provided a model **Record of Processing Activities** example on its website.

- Completing one or more data protection impact assessments (PIA) – Article 35 of the GDPR

When personal data processing is likely to result in greater risk to the data subject's rights and freedoms, an assessment must be carried out to assess the origin, characteristics and seriousness of the risk in order to determine which measures to implement.

Carrying out an impact assessment is mandatory when:

- Operations are to process a considerable volume of data likely to result in greater risk, for instance because of their sensitive nature.

- Processing presents specific risks given the characteristics of the data being processed (criminal offences and convictions; automated, systematic or in-depth assessments of personal aspects in order to take a decision producing legal effects; systematic large-scale monitoring of a zone open to the public).

- Processing presents a risk to the data subjects' rights and freedoms.

It must lead to the establishment of suitable measures to implement in order to prove that the processing complies with the requirements imposed by the regulation.

The regulation does not impose a specific method for carrying out assessments but does state what they must contain. To find out more on the Impact Assessment, please visit the corresponding page on the CNIL website and download here, if required, the open source software developed by CNIL to carry out the assessment, as well as the various guides.

- Framework for data transfers outside the EU – Articles 44 à 50 of the GDPR

The regulation provides the framework for transfers to a non-EU country of data that will be or are intended to be processed after the transfer.

Despite the concept of transfer not being defined in the regulation, CNIL has published a guide to personal data transfers to non-EU member countries in which you can find examples of data transfers.

This kind of transfer can occur without it being necessary to obtain prior approval if the non-EU country

or international organisation has been recognised by the European Commission as providing an adequate level of data protection (adequacy decision).

Failing this, it is also possible to transfer data without prior approval if the transfer occurs within the framework of mechanisms that offer the appropriate safeguards, such as **standard contractual clauses** and binding corporate rules (BCR).

It is also possible, in the absence of an adequacy decision or suitable safeguards, to carry out a transfer if it is based on one of the exceptions listed in **Article 49** of the GDPR.

As a last resort, if none of these exemptions apply (no adequacy decision, no mechanisms providing suitable safeguards, and no exemptions under Article 49 of the GDPR apply), the regulation states that data transfer may occur if all of the following conditions are met:

- Not repetitive in nature.

- Limited number of data subjects.

- Necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject.

- The controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards.

- The supervisory authority has been informed.

- The data subject has been informed, including about the transfer and the compelling legitimate interests pursued.

IMPORTANT

Insomuch as these exemptions can be interpreted in a restricted way by supervisory authorities, the controller should be cautious in using an exemption as the basis for a transfer.
Furthermore, when there is no adequacy decision, EU and member state law can set limits on transfers to non-EU member countries and international organisations.

Quelles mesures concrètes mettre en œuvre ?

In order to meet the documentation obligation for this, and in addition to ensuring the processing is based on one of the exceptions in the aforementioned article, the controller is recommended to store the consent collection models (by any means: written, digital, audio recording, etc.).

When processing is based on "legitimate interest", you must verify and document the balance between the legitimate interest invoked by the controller and the rights of the data subject.

- Implementing a clear data storage period policy – see I.A.1.e above

- Documenting the legal basis for the processing

To be lawful, the processing must be based on one of the exceptions in Article 6 of the GDPR (see I.A.2 above).

- Informing people

When data is collected, certain information must be given to the data subject (see I.B above).

In practice, the proof that you have met your obligations regarding personal rights can be shown in the following ways: drafting and providing to the authorities the confidentiality policy intended for data subjects, along with all documents intended for employees which require them to process the collected data in accordance with the GDPR (IT charter appended to company rules, information memo on collecting provided data, emails, information on signs displayed within the company, etc.).

- Framework for the processor - Article 28 of GDPR

The regulation requires that a written contract be signed between the controller and processor.

In addition to the details of the processing itself (purpose, subject, duration, etc.), the contract must state that the processor agrees to: only act on the controller's documented written instructions, ensure the confidentiality and security of the data, obtain authorisation in the event of subcontracting to another provider, etc.

- Carrying out regular audits

We recommend implementing verification procedures (auditing the tools and processors) to ensure that the measures taken are operating and effective, as well as to identify any failures in order to take suitable corrective actions.

- Applying codes of conduct and certifications – Articles 40 to 43 of the GDPR

The GDPR states that following and applying a code of conduct as well as achieving certifications are proof of compliance and constitute mitigating circumstances that supervisory authorities will take into account when deciding on sanctions.

There is no GDPR certification, however **CNIL offers several certifications** (Freedom & Digital Governance, Training, and Digital Safe) and has recently published **updated training and governance certifications that take into account the GDPR's requirements.**

- Visit the CNIL website to find out more about **how to achieve a CNIL certification**

Lastly, the GDPR gives the authority charged with checking that the regulation is correctly applied the power to issue administrative penalties for failures (III).

III. SUPERVISORY AUTHORITY'S POWERS TO INVESTIGATE AND ISSUE SANCTIONS FOR FAILURE TO COMPLY WITH THE REGULATION'S PROVISIONS

In order to carry out its mandate, the supervisory authority has the power to investigate (1) and the ability to issue financial sanctions to those who fail to comply with the regulation's provisions (2).

1. Supervisory authority's powers to investigate

The supervisory authority may, on its own initiative or following a complaint addressed by a data subject, carry out an investigation, including:

- Auditing the data protection measures.
- Assessing any certifications issued.
- Requesting all information required to carry out its mandate.
- Accessing the collected and processed personal data.
- Accessing the premises, and data processing equipment and means
- Notifying of the alleged regulation violations.

Following its investigation, the authority may adopt one of the following measures:

Warning	Power to issue a warning that intended processing operations are likely to violate the provisions of this Regulation.
Reprimand	Power to issue reprimands where processing operations have violated this Regulation.

Compliance order	Power to order the compliance of processing operations with the provisions of this Regulation (where appropriate, in a specified manner and within a specified period).
Respecting personal rights	- Power to order compliance with the data subject's request to exercise their rights. - Power to order the controller to notify the data subject of a personal data violation. - Power to order the rectification or erasure of personal data or restriction of processing, and the notification of such actions to recipients to whom the personal data have been disclosed.
Limitation	Power to impose a temporary or permanent limitation including a ban on processing.
Withdrawal/denial of certification	Power to withdraw a certification, or to order the certification body to withdraw or deny certification if the requirements for the certification are not or are no longer met.
Flow suspension	Power to order the suspension of data flows to a recipient in a non-EU member country or to an international organisation.

In addition to these powers, the authority can issue administrative fines.

2. Supervisory authority's powers of sanction

Article 83 of the GDPR distinguishes two different sanction levels according to the seriousness of the failure:

Sanction	Violation type
Up to €10 million or, for a company, up to 2% of its total global annual turnover for the previous financial year	- Failure to comply with by design and by default privacy principles. - Failure to have a Record of Processing Activities (when mandatory). - Failure to notify the supervisory authority or data subject of a personal data breach. - Insufficient, inadequate or lack of data security measures. - No impact assessment carried out when required. - No contractual framework for the relationship between joint controllers or with processors. - No DPO appointed when mandatory. Etc.

Up to €20 million or, for a company, up to 4% of its total global annual turnover for the previous financial year	- Failure to comply with data processing-applicable principles (transparency, fairness, etc. See I above). - Failure to comply with lawful processing conditions (see II above). - Failure to respect the rights of data subjects (information, access, rectification, etc. See I.1 above). - Failure to comply with an injunction issued by the supervisory authority. Etc.

Furthermore, the supervisory authority may institute legal proceedings.

Similarly, data subjects have the right to institute legal proceedings if they consider that their rights under the regulation have been violated by data processing.

If legal proceedings are instituted by data subjects, this does not exclude any complaint to the supervisory authority, or vice versa.

IMPORTANT

The regulation states that Member States may set the regulatory regime for other sanctions in the event of the regulation being violated, including the option of setting the criminal sanction regulatory regime.