PrestaShop

GDPR KEY INFO

White Paper

Version 2022

Contents

Why this regulation? 3

TOPIC 1
Does the GDPR affect you? 5
To which activities does the GDPR apply? 5
Where is the GDPR applicable? 6

TOPIC 2
What is the legal basis for data processing? 6

TOPIC 3
How do you define the purposes of your data processing? 9

TOPIC 4
How do you inform your data subjects? 10

TOPIC 5
How can data subjects exercise their rights? 11

TOPIC 6
How do you incorporate privacy by design and privacy by default? 13

TOPIC 7
When should you appoint a data protection officer? 14

TOPIC 8
How do you respect the accountability obligation? 15

TOPIC 9
How do you institute a data storage policy? 16

TOPIC 10
How do you secure your data processing? 17

TOPIC 11
How do you safeguard data transfers? 18

TOPIC 12
How do you provide a framework for relations with data processors? 19

TOPIC 13
When should you perform an impact assessment? 20

TOPIC 14
What is a supervisory authority? 21
What investigative powers does the supervisory authority have? 21

TOPIC 15
What sanctions do you risk if you are not in compliance with the GDPR? 24

TOPIC 16
How do you manage the use of cookies by your website? 23

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 that regulation's provisions.

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

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. That European regulation defined a new legal framework for the protection of European citizens' personal data, in response to new digital technologies.

This white paper was prepared in order to give you some keys to understanding the main principles that were established or confirmed by the GDPR.

Why this regulation?

The purpose of the GDPR is to define a common, consistent vision of personal data protection within the European Union.

Its text instituted the main 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.

The regulation restates or creates obligations imposed on controllers who must ensure compliance with those obligations by implementing various technical and organisational measures that fall under "accountability".

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.

TOPIC 1

Does the GDPR affect you?

To **which activities** does the GDPR apply?

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

WHAT IS PERSONAL DATA?

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

- Examples: Identity (full name), email address, IP address, telephone number, location data, consumer habits, etc.

WHAT IS DATA PROCESSING?

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

- Examples: Data consultation, collection, storage, modification, extraction, use, communication, destruction, etc.

IN PRACTICE:

Given the extent of these concepts and your e-commerce business, it is highly likely that you process personal data and so operate in the capacity of a data controller. If you have any doubts on this subject, we recommend that you reach out to legal counsel.

Where is the GDPR applicable?

The other criterion for application of the regulation relates to the processing of personal data with a **geographic connection to the territory of the European Union.**

In concrete terms, the GDPR is applicable if:

- The controller or its processor has an **establishment located within the borders of the European Union or**,
- The controller or its processor does not have an establishment located in the European Union but **the data subjects are located there.**

IN PRACTICE:

Whether or not your company has any locations within the borders of the European Union, the GDPR applies to most companies, so long as you process any data concerning EU citizens.

TOPIC 2

What is the legal basis for data processing?

Any personal data you may collect as part of doing business must be processed in a way that is **lawful, fair and transparent.**

According to the GDPR, data processing is only considered lawful if based on one of the six legal grounds defined by Article 6 of the GDPR:

1. **Consent**
2. **Contract**
3. **Legitimate interest**
4. **Legal obligation**
5. **Public interest**
6. Vital **interests of the data subject or another natural person**.

2.1 Consent

PRINCIPLE:

The data subject has consented to communicate their personal data.

That consent must be:

- Freely given: The data subject is offered a genuine choice, with no negative consequences in the event of their refusal.
- Informed: The controller must provide certain information to the data subject before they consent to the characteristics of and methods involved in the data processing.
- Specific: The consent must be given for a single processing operation, for a predefined purpose. As a result, in the case of data processing for multiple purposes, the data subjects must be able to give their consent individually for each purpose.
- Unambiguous: Consent must be given by means of a statement or other clear affirmative act.

The controller must be able to provide proof of each data subject's effective consent.

IN PRACTICE:

Set up a system for collecting consent (tick box, signature, email, etc.).

The consent collection system must:

- Be accompanied by an information notice (the data subject must be informed of the processing that their data will undergo, before they give their consent).
- Offer data subjects equivalent options for rejecting or accepting data processing.

Set up the technical means for data subjects to withdraw their consent at any time (unsubscribe link, etc.).
Document the information notices accompanying the consent.
Keep proof of data subjects' consent.

2.2. **Contract**

PRINCIPLE:

For processing on a contractual (or pre-contractual) basis, the data subject must be a party to the contract.

IN PRACTICE:

A contract between the controller and the data subject (contract, terms and conditions, etc.).

2.3. **Legitimate interest**

PRINCIPLE:

This refers to the interest of collecting the data for the controller.

Processing may be based on the legitimate interests of the controller or of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of their 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 PRACTICE:

- Identify the legitimate interest.
- Examine the legitimate interest and document how it takes precedence over the fundamental rights and freedoms of the data subjects.
- Explain that interest in the organisation's privacy policy.

2.4. **Legal** obligation

PRINCIPLE:

The data is collected in response to an obligation dictated by domestic or European law (e.g. reporting of unlawful content, etc.).

IN PRACTICE:

- Identify the data processing activities.
- Determine the legal source (a clause in a code, regulation, etc.).
- Specify the legal source of the purpose of processing in the organisation's privacy policy.

2.5. **Public** interest

PRINCIPLE:

The processing is necessary in order to carry out a task in the public interest.

IN PRACTICE:

- The controller must be a legal entity tasked with duties to be performed in the public interest.
- The data collection and processing must be linked to those duties.

2.6 **Vital** interests

PRINCIPLE:

The processing is essential in order to protect the vital interests of the data subject or of another natural person (in the case of an epidemic, natural catastrophe, etc.).

IN PRACTICE:

- Use of this legal basis remains rare.

TOPIC 3

How do you define the purposes of your data processing?

Data must only be collected for a purpose that is:

- **Determined**
- **Explicit**
- **Legitimate and**
- Not subsequently reused for a purpose other than the purpose initially stated at the time of data 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.

IN PRACTICE:

- Clearly define the **aim pursued by the processing** (personnel management, advertising, etc.).
- Determine the **relevant data** to collect in order to achieve that aim.
- Determine the **time** required to fulfil that aim or, failing that, objective criteria that can be used to determine its fulfilment.
- Present the **purpose in a way that is easy to understand.**

TOPIC 4

How do you inform your data subjects?

The GDPR requires information that is concise, transparent, intelligible and easily accessible by data subjects.

In order to meet this **obligation of transparency**, you must only collect and process personal data after informing the data subjects through an easily accessible message (e.g. confidentiality policy available online) that is easy to understand, meaning it is written in clear and plain language.

The GDPR lists all the information that must be issued in writing or by any other suitable method (including electronic) to the data subjects, namely including:

- Identity of and contact information for the data controller
- Purposes of data processing
- Legal bases for data processing
- Required or optional nature of data collection and consequences if the person refuses to provide their data
- Recipients or categories of recipients of the data (who need to access or receive the data in view of the defined purposes of its collection, including any processors)
- Data storage period (or criteria used to determine that period)
- Data subjects' rights
- Contact information for the organisation's data protection officer, if one has been appointed, or for a point of contact for questions relating to personal data protection
- Right to lodge a complaint with the CNIL (French Data Protection Authority)..

This information must be communicated to data subjects:

- At the time of data collection, in the case of direct data collection or
- As soon as possible (preferably at the time of first contact with each data subject) and within a maximum of one month (excluding a handful of exceptions) in the case of indirect data collection.

IN PRACTICE:

- Write up data subject information documents (confidentiality policy, cookies policy, etc.).
- Adapt that information to the different data collection situations and methods.
- Write the information to ensure that it is accessible and intelligible.
- Plan a multi-tiered approach to underscore the most important information (without neglecting the rest), in other words prioritising the following information:
  - Identity of the data controller
  - Purposes of data collection
  - Data subjects' rights.

You may want to consider adding a hyperlink pointing to your complete legal notice or else a drop-down menu.

TOPIC 5

How can data subjects exercise their rights?

5.1 What **rights do data** subjects have?

Data subjects have rights that allow them to maintain control over their own data. The GDPR reinforced existing rights and introduced new ones. Here is the list of data subjects' rights you must respect in order to be in compliance:

- Right of access (to all their personal data),
- Right to rectification,
- Right to erasure,
- Right to restriction of processing,
- Right to data portability,
- Right to object.

The exercise of those rights is dependent on the legal basis for the processing:

	RIGHT OF ACCESS	RIGHT TO RECTIFICATION	RIGHT TO ERASURE	RIGHT TO RESTRICTION	RIGHT TO PORTABILITY	RIGHT TO OBJECT
CONSENT	✓	✓	✓	✓	✓	WITHDRAWAL
CONTRACT	✓	✓	✓		✓	✗
LEGITIMATE INTEREST	✓	✓	✓	✓	✗	✓
LEGAL OBLIGATION	✓	✓	✓	✓	✗	✗
PUBLIC INTEREST	✓	✓	✗	✓	✗	✓
VITAL INTERESTS	✓	✓	✓	✓	✗	✗

This table was created by the CNIL and is available here.

5.2 How do you respond to a request to **exercise a data subject's rights?**

- As necessary, the controller must verify the identity of the data subject making the request.
- As needed, the controller must ask which data are covered by the request.
- The controller must confirm that the request does not concern a third party.
- The controller must respond to the request within the timeframe defined by the GDPR:

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.

In any case, you absolutely must inform the data subject within a maximum of one month.

IN PRACTICE:

- **Appoint people in charge of responding** to the requests and complaints you receive.
- **Create a log** for rights requests and track them.
- **Respond within the timeframe** required by the GDPR.
- **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.
- Implement tools for providing a **full response to requests for the erasure of personal data.**

TOPIC 6

How do you incorporate privacy by design and privacy by default?

What is **« privacy by design »** ?

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 rationale 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.

What is **« privacy by default »** ?

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. The idea is that, once the protective system is in place, it will be activated by default, without requiring any further action.

IN PRACTICE:

- Provide **awareness training for your teams.**
- Establish **procedures for adhering to principles**, including in particular:
  - Security measures
  - Documentation of developments
  - Consideration of the right of access from the time of project creation
  - Reduction of the quantity of data collected by restricting it to data that is strictly necessary
  - Pseudonymisation of the collected data as soon as possible,
- Determine the applicable **data storage periods** and set up mechanisms for manual or automatic data purges beyond those storage periods.
- **Give data subjects the opportunity to exercise their rights.**

TOPIC 7

When should you appoint a data protection officer?

A data protection officer (DPO) plays a crucial role in the accountability approach insomuch as the DPO informs and advises decision-makers on which security measures to implement, and checks that those measures meet the GDPR's requirements.

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

1. The processing is carried out by a **public authority or agency**, except for courts acting in their judicial capacity,

2. 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,

3. 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 or personal data relating to the criminal convictions and of fences 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. You should know though that the CNIL and other European authorities encourage all companies to designate an in-house DPO.

TOPIC 8

How do you respect the accountability obligation?

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:

- Implementation of the **organisational and technical measures** that can ensure the processing occurs in a manner that complies with the GDPR
- **Identification and documentation of the implemented measures.**

In practice, this means the controller must be accountable to the authorities and enable the latter to verify the measures taken.
The GDPR aims to hold all actors along the data processing chain accountable for their actions. Those actors must take the necessary steps to demonstrate that their practices are compliant with the provisions of the GDPR.

It is absolutely essential to compile the following information:

Data processing documentation

Record of processing activities (listing all data processing operations, both new and existing – required for all entities with more than 250 employees OR if the processing is not occasional OR if the processing poses a risk to the data subjects' rights and freedoms) – To help companies with this task, the CNIL has provided a sample record of processing activities (in French).

Data protection impact assessments (DPIAs) for any processing that could pose a high level of risk to data subjects' rights and freedoms.

Guidelines for data transfers outside the European Union (standard contractual clauses, etc.).

Information for data subjects

Information notices

Templates for collecting data subjects' consent

Procedures put in place for the exercise of data subjects' rights.

Data processing contracts

Contracts with processors

Internal procedures in the event of data breaches

Proof of data subjects' consent where the processing of their data is based on the legal grounds of consent.

TOPIC 9

How do you institute a data storage policy?

Personal data must be stored in a form that enables the data subjects to be identified and for **a period not exceeding the time required for the purpose** for which the data is being processed.

Personal data cannot be stored indefinitely. **The controller must determine the applicable storage period based on the purpose of the processing**.

1. The data is to be stored in an **active database** for the time required to achieve the aim (purpose) that provided the grounds for collecting / recording the data.

2. Personal data may be stored that is no longer being used to achieve the aim pursued but that may still be of administrative interest to the organisation (to manage future disputes, etc.) or that must be retained in order to satisfy a legal obligation (for example, under the French Commercial Code, invoicing data must be kept for 10 years, even if the data subject is no longer a customer). The data may then be consulted on a one-off basis, on legitimate grounds and by individuals specifically authorised to view the data.

3. Because of its value and interest, certain information is permanently archived.

It is also imperative the technical mechanisms (automatic data purges, manual purges, etc.) are put in place in order to remain in compliance with the regulatory data storage periods.

In concrete terms, what are the **obligations relating to the storage limitation**?

1. **French law stipulates specific storage periods for certain data (10 years for invoicing data, 5 years from the end of a business relationship for data relating to that relationship, etc.).**
2. **If there is no law that defines a storage period for the data you collect, you will have to define that period yourself. Do that on the basis of the purpose for which the data is being collected, by estimating the amount of time required to fulfil that purpose. You can also take advantage of the CNIL's recommendations (3 years for data relating to business leads, etc.).**
3. **Audit your current storage periods for the data you are already collecting, for which no storage period was defined. As soon as it is no longer useful, the data should immediately be deleted.**
4. **Set up technical mechanisms for deleting data once they have passed their storage period (automatic data purges, anonymisation, archiving of data that must be retained by law, etc.). It is not enough to de fine data storage periods in order to be compliant with the GDPR: you must also adhere to those periods and ensure the data is deleted once its storage time has lapsed.**

You can see the CNIL's data storage guide (in French) for more information.

TOPIC 10

How do you secure your data processing?

Data must be processed in such a way as to ensure the data subjects enjoy appropriate security for their personal data, through **technical and/or organisational measures.**

IN PRACTICE:

- **Encode the data** (especially for transfers).
- **Restrict and monitor** physical and digital access to the data.
- **Regularly back up the data** on different, secure media.
- **Install firewalls** and antivirus software.

We recommend reading the Security of Personal Data Guide published by the CNIL.

What do you do in the event of a data breach?

In addition to prevention, the GDPR states that controllers must institute appropriate procedures for identifying any data **breaches (loss of the availability, integrity or confidentiality of personal data, whether accidental or unlawful, or the unauthorised accessing of such data)** and, if applicable, reporting it to the supervisory authority:

RISK LEVEL POSED TO DATA SUBJECTS BY THE DATA BREACH:	NO RISK	SOME RISK	HIGH RISK
Internal documentation in a data breach log	✔	✔	✔
Notification of the relevant supervisory authority within 72 hours		✔	✔
Notification of data subjects as soon as possible, aside from special cases			✔

IN PRACTICE:

- 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.
- **Keep a log** of security breaches.

TOPIC 11

How do you safeguard data transfers?

This refers to all data transfers to countries outside the European Union that will or are intended to undergo processing after the transfer.

1. This kind of transfer can occur 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).
2. Failing this, it is also possible to transfer data if the transfer occurs within the framework of mechanisms that offer the appropriate safeguards, such as standard contractual clauses.
3. 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.
4. 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.

IN PRACTICE:

- Check the country of establishment of any third parties with access to the data.
- Include the standard contractual clauses in your contracts.
- Set up additional security safeguards.
- Document all contracts and standard contractual clauses.

TOPIC 12

How do you provide a framework for relations with data processors?

The GDPR requires the **signature of a written data processing agreement 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.

If there is no "GDPR certification", the CNIL offers a variety of privacy seals. Visit the CNIL website to find out more about how to earn a CNIL privacy seal: https://www.cnil.fr/en/privacy-seals

IN PRACTICE:

- **Make a list** of all your data processors.
- **Provide a framework for your processors' processing in the form of data processing agreements.**
- Produce **templates for data processing agreements.**
- **Document** all signed agreements.
- Institute **audits** of your processors.

TOPIC 13

When should you perform an impact assessment?

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 a privacy impact assessment (PIA) is required when:

- A considerable volume of data is being processed, that is likely to result in greater risk, for instance because of its sensitive nature
- The 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; or systematic large-scale monitoring of a zone open to the public)
- The processing poses a risk to the data subjects' rights and freedoms.

It should lead to the identification of suitable measures to be implemented in order to demonstrate that the processing complies with the requirements laid down by the GDPR.

The regulation does not impose a specific method for carrying out assessments but does state what they must contain.

To find out more about impact assessments, please visit the corresponding page on the CNIL website and download, if applicable, the open source software developed by CNIL to carry out the assessment, available here, as well as the various guides.

IN PRACTICE:

- If necessary, you can use the templates provided by the CNIL.

TOPIC 14

What is a supervisory authority?

In order to carry out its mandate, the supervisory authority has the power to investigate and the ability to issue financial sanctions to those who fail to comply with the provisions of the GDPR (cf. next topic).

What investigative powers does the **supervisory authority** have?

The supervisory authority may, on its **own initiative or following a complaint** lodged 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 the GDPR
Reprimand	Power to issue reprimands where processing operations have violated the GDPR
Compliance order	Power to order the compliance of processing operations with the provisions of the GDPR (where appropriate, in a specified manner and within a specified period)
Respect for data subjects' rights	1) Power to order compliance with the data subject's request to exercise their rights 2) Power to order the controller to notify the data subject of a personal data violation 3) 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 supervisory authority can issue administrative fines.

TOPIC 15

What sanctions do you risk if you are not in compliance with the GDPR?

Sanctions	Type of violation
Up to €10 million or, for a company, up to 2% of its total global 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 (if required) • 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 • DPO not appointed when required, etc.
Up to €20 million or, for a company, up to 4% of its total global turnover for the previous financial year	• Failure to comply with principles applicable to data processing (transparency, fairness, etc.) • Failure to comply with lawful processing conditions • Failure to respect the rights of data subjects (information, access, rectification, etc.) • Failure to comply with an injunction issued by the supervisory authority, etc.

Furthermore, the supervisory authority may also **initiate legal proceedings.**

Similarly, data subjects have the right to **initiate legal proceedings** if they consider that their rights under the GDPR have been violated by data processing. If legal proceedings are initiated by data subjects, this does not exclude any complaint to the supervisory authority, or vice versa.

The GDPR 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.

TOPIC 16

How do you manage the use of cookies by your website?

Pursuant to the ePrivacy Directive, **data subjects must be informed and give their consent before certain cookies are installed and read, while other cookies are exempt from the need for consent.**

The following cookies are exempt from obtaining consent:

- Cookies that are strictly necessary in order to provide an online communication service that was expressly requested by the user
- Cookies whose sole purpose is to enable or facilitate electronic communications.

To be exempt, those cookies must also meet both of these criteria:

- Their purpose is strictly limited to tracking the website's or the application's audience metrics (performance metrics, detection of navigation problems, technical performance or ergonomic optimisation, estimation of the necessary server power and analysis of viewed content), solely on behalf of the publisher
- They are only used to produce anonymous statistics.

Examples of cookies that are exempt from consent:
- Cookies that store user choices regarding the installation of cookies
- Cookies that provide for user authentication with a service
- Cookies that store the contents of a shopping cart, etc.

The following however are not exempt from consent:
- Cookies associated with personalised advertising
- Social media cookies, particularly those generated by sharing buttons.

Regardless of the type(s) of cookies installed in the user's browser, the user must always be informed of their installation.

What are the **storage periods for cookies**?

- As concerns a cookie's installation in a user's browser, the CNIL recommends a maximum period of 13 months before either removing the cookie or asking the user to renew their consent.
- As concerns the browsing data gathered by cookies, the CNIL recommends a maximum storage period of 2 years. .

As a reminder, personal data should only be kept as long as necessary for the purpose for which it was collected (cf. Topic 9).

IN PRACTICE:

- Be sure to consider whether or not you need your users' consent.
- Inform your data subjects (about ALL cookies).
- For cookies requiring consent:
  - Gather consent before installing any cookies
  - Make sure the cookies are not technically installed before consent has been obtained
  - Make sure that, if consent is withheld, the cookies will not be installed in the user's browser
  - Give the user the possibility of withdrawing their consent at any time.
- For cookies exempt from consent:
  - Make sure the cookies really are exempt
  - If in doubt, conduct a study on the cookie and compile arguments corroborating your assertion that user consent is not necessary.
- Ensure that the data storage periods are compliant with the GDPR and the supervisory authority's recommendations.
- Document the cookies you use.


PrestaShop