Doc. name : **Oxygis - General Data Protection Regulation (GDPR)**

Version updated on : 18/06/2025

Summary: Oxygis' guide to European data protection rules. Overview of new privacy laws and best practices with Oxygis

Since 25 May 2018, the **General Data Protection Regulation (GDPR)** has come into force, ushering in a new era of data protection and privacy for all. While you've certainly heard and read a lot about the GDPR, it can be difficult to understand exactly **what it means for your business**, in practical terms, and **what you need to do** to comply with the new rules.

At Oxygis, we are committed to following best practices in terms of security and confidentiality. We strive to offer the same level of protection to all users and Clients, regardless of location or nationality. And we apply these best practices to all data, not just personal data.

Oxygis provides tools to facilitate RGPD compliance, but each client remains solely responsible for assessing their own compliance, particularly with regard to their activities outside of the platform.

Oxygis Partners SRL and its subsidiaries are therefore GDPR compliant.

I. What you need to know about the GDPR

Advice
If you can, the best way to understand the GDPR is to **read the official text**. It is a little long (99 articles on 88 pages), but quite readable for non-experts.

This European **regulation** aims to **harmonise** and **modernise** existing privacy protection legislation, such as the European Data Protection Directive, which it replaces. It establishes rules for the protection of individuals with regard to the processing of their personal data, and the free movement of personal data within Europe.

It is **a regulation**, not a directive, and is therefore immediately applicable in all EU Member States, without the need to transpose it into the national law of each country. EU countries have a limited margin of interpretation for the finer points , but **the fundamental rules will be the same for everyone**, everywhere in the EU.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

The GDPR also **brings legislation into the next millennium**, taking into account social media, cloud computing, cybercrime and the major challenges they pose in terms of the privacy and security of personal data.

In a nutshell: Don't panic!
The GDPR is not a revolutionary new piece of legislation, and it is fundamentally a good thing for citizens and businesses.

It's a good thing!
We'd like to stress that the GDPR can be great for you and your Customers. Complying with GDPR can initially be a lot of work, but there are benefits to these new rules:

- Increased confidence from your customers and users
- Simplification: the same rules apply in all EU countries.
- Streamlining and centralising your organisational processes

The aim of the GDPR is to give individuals more control over their personal data. If your business has the right strategies and systems in place, it will be easier to manage, safer and more secure for years to come.

What are the risks if you don't comply?

The maximum penalty for non-compliance is an administrative fine of €20 million or 4% of your worldwide annual turnover, whichever is greater. A lower fine of €10 million or 2% of your worldwide annual turnover is applicable for minor infringements.

These ceilings are intended to act as a **deterrent** for businesses of all sizes, but the GDPR also requires fines to remain **proportionate**.

The supervisory authorities (also known as data protection authorities: DPAs) must take into account the circumstances of each case, in particular the nature, seriousness and duration of the infringement. These authorities also have the power to **investigate** and **impose corrective measures**, including the restriction of unlawful activities, without necessarily imposing a fine.

Another risk if you don't comply is that your customers and prospects will lose confidence in you because they are concerned about how you handle their data!

Key principles of the GDPR

- ***Range***

The Regulation applies to all **processing of personal** data **by any organisation**:

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

- If the controlling or processing organisation **is located in the EU**
- If the organisation **is not located in the EU**, but the processing involves personal data of data subjects located in the EU, and is related to commercial offers or behavioural monitoring.

The scope therefore includes non-European companies, which was not the case under the previous legislation.

- ***Roles***

The regulations distinguish between two main types of entity:

- **Data controller:** any entity that **determines the purposes and means of** processing personal data, either alone or jointly. As a general rule, each organisation is a controller of its own data.
- **Data processor**: any entity that processes data on behalf of a data controller.

For example, if your company has a database hosted on **the Oxygis Cloud Infrastructure**, you are the **controller of** this database, and **Oxygis Partners SRL** is only a **data processor**. If, on the other hand, you use **Oxygis for self-hosting**, you are both the **controller and the** data **processor**.

- ***Personal data***

The GDPR gives a broad definition of personal data: **any information relating to an identified or identifiable natural person.** An identifiable person is one who can be identified, **directly or indirectly**, by means of his or her name, email address, telephone number, biometric information, location data, financial data, etc. Online identifiers (IP addresses, device identifiers, etc.) are also concerned.

This **also applies in professional contexts**: *info@oxygis.eu* is not considered personal, but *john.smith@oxygis.eu* is, because it can be used to identify a physical person within a company.

The GDPR also requires a higher level of protection for **sensitive data**, which includes specific categories of personal data such as information about health, genetics, race or religion.

- ***Data processing principles***

To be compliant, processing activities must comply with the following rules:
(as listed in Article 5 of the GDPR)

1. **Legality, fairness and transparency**: to collect data, you must have a *legal basis*, a clear *purpose* and you must *inform* the subject.

- Have a simple, clear confidentiality policy, and refer to it wherever you collect data.
- Check the legal basis for each of your data processing activities

2. **Limiting the purpose**: once data has been collected for a specific purpose, ask permission if you wish to use it for a different purpose.

   For example, you cannot decide to sell your Customer data if it has not been collected for this purpose.

3. **Minimisation**: you should only collect the data you need to achieve your objective.

4. **Accuracy**: reasonable steps must be taken to ensure that data is kept up to date, having regard to its purpose.

   For example, make sure you deal with bounced emails, and correct or delete addresses.

5. **Limits on storage**: personal data may only be stored for as long as is necessary to fulfil its primary purpose.

   Set deadlines for deleting or revising the personal data you process, depending on its purpose.

6. **Integrity and confidentiality:** data controllers must implement appropriate access control, security and data loss prevention measures, depending on the type and scale of the data processed.

   For example - Make sure your backup system is working, implement appropriate security controls, use encryption to protect sensitive data such as passwords, etc.

7. **Responsibility**: data controllers are responsible for compliance with all the above processing principles and must be able to demonstrate this.

   - Establish and maintain a data mapping reference for your organisation, describing the compliance of your processing activities.
   - Inform your customers with a clear privacy policy

- ***Legal basis***

To be lawful under the GDPR (*first principle*), the processing of personal data must be based on **one of the 6 possible legal bases** listed in Article 6 (1):

1. **Consent.** Valid when the data subject has *explicitly* and *freely* given his/her consent after having been properly *informed*, in particular by a *clearly stated* and *specific purpose*. The burden of proof for all this lies with the data controller.
2. **Necessary for the performance of a contract**, or to respond to requests from the data subject in preparation for a contract.
3. **Compliance with a legal obligation** imposed on the data controller.
4. **Protection of vital interests**. When treatment is necessary to save a life.
5. **Public interest or official authority**.
6. **Legitimate interest.** Applicable where the controller has a legitimate interest which is not overridden by the interests and fundamental rights of the data subject.

One of the major changes brought about by the GDPR compared with the previous data privacy regulations is the strengthening of the requirements for obtaining valid **consent.**

- ***Rights of the persons concerned***

Existing data privacy rights of individuals are further expanded by the GDPR. Organisations must be prepared to deal with data subjects' requests in a timely manner (within one month), free of charge :

1. **Right of access** - Individuals have the right to know *what* and *how* their personal data is processed, in full transparency;
2. **Right of rectification** - Individuals have the right to have their personal data *rectified* or *completed*;
3. **Right to erasure** - Individuals have the right to have their personal data *erased* for legitimate reasons (withdrawal of consent, data no longer necessary for the purpose, etc.).
4. **Right of restriction** - Individuals may ask the controller to *stop processing their* personal data if they are unwilling or unable to request its complete deletion;
5. **Right to object** - Individuals have the right to *object at any time to* certain processing of their personal data, for example for direct marketing purposes;
6. **Data portability** - Individuals have the right to request that personal data held by one data controller *be provided to them*, or to another data controller.

II. How to prepare for the GDPR

Disclaimer of liability

We cannot provide legal advice, this section is for information purposes only. Please speak to your legal advisor to determine exactly how the GDPR affects your business.

Here are the key steps we suggest for a GDPR compliance roadmap:

1. **Map out** your organisation's data processing **activities** to *get a clear picture of the situation*. Data protection authorities often provide model spreadsheets to help you with this task. For each process, document the type of personal data and how it was collected; the *purpose*, *legal basis* and *erasure policy* of the processing; the technical and organisational *security measures* implemented, and the *subcontractors* (processors) involved.

   You will need to maintain this data map regularly, as your processes evolve.

2. On the basis of step 1, choose a **remediation strategy** for any processing for which you do not have a legal basis (e.g. missing consent) or for which you have not put in place appropriate security measures. Adapt your processes, your internal procedures, your access control rules, your safeguards, your monitoring, etc.
3. Update and publish a clear **privacy policy** on your website. Explain what personal data you process, how you do it, and what rights individuals have regarding their data.
4. Review your **contracts** with a legal advisor and adapt them to the GDPR.
5. Decide how you are going to respond to the different types of **requests from the people concerned**.
6. Prepare your **incident response procedure in** the event of a data breach.

Depending on your situation, other items could be added to the list, such as the appointment of a Data Protection Officer. Consult your in-house processing experts and legal advisors to determine any other relevant measures.

Don't forget!

By clearly mapping your processes, everything will be easier on the road to compliance!

III. How does Oxygis comply with the GDPR?

At Oxygis, implementing privacy and security best practices is not a new idea. As a cloud-based software company, we are constantly reviewing and improving our systems, tools and processes to maintain a high-performance, secure platform.

Our GDPR roles

Our responsibilities with regard to the protection of personal data depend on our various data processing activities:

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Our roles	Data processing	Type of data
Controller and data processor	**On Oxygis.eu**	The personal data provided to us by our Clients and direct prospects, our partners and all **direct users of Oxygis.eu** (names, emails, addresses, passwords, etc.).
Data **processor**	**On Oxygis Cloud** (Oxygis Online, Oxygis Mobile and other Oxygis enterprise services)	Any personal data stored in our Clients' databases, hosted in the Oxygis Cloud or transferred to us for the purpose of using one of our services. The owner of the database is the **data controller**.
No role	**On site**	Any data located in Oxygis databases hosted on site or in any hosting not operated by us.

Our GDPR documents

As **a data controller**, our activities are covered by our ***Privacy Policy*** which has been updated for the GDPR. This policy explains as clearly as possible *what* data we process, *why* we process it and *how* we process it. Closely linked to this, our ***Security Policy*** explains the best security practices we have implemented at Oxygis, at all levels (technical and organisational) to ensure your data is processed safely and securely.

In addition to these policies, our activities as **Data Controller** are subject to acceptance of our ***Oxygis Subscription Agreement*****.** See also section 6.5 of the Subscription Agreement for contractual clauses relating to the processing of personal data. This contract has been updated to add the necessary data protection clauses (often referred to as a "data processing contract"), as required by the GDPR. As an Oxygis Client you don't have to do anything to agree to these changes, **you already benefit from the new safeguards**, and we'll assume you agree if we don't hear anything from you!

In addition to these documents, we have also updated our website to include privacy notices in all relevant places, in order to keep our users informed at all times.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

IV. How can Oxygis help you implement GDPR best practices?

Using Oxygis to manage your business **may not be sufficient for GDPR compliance**, *as the regulation applies to your entire organisation.* However, because Oxygis centralises your data, reduces data redundancy and implements granular access rights and security controls, it can be a great help in complying with the GDPR.

Here are some of the ways we think Oxygis can help you in the context of GDPR, for both on-premise and cloud-hosted Oxygis databases.

Disclaimer: As always, consult your legal advisor to determine how you need to comply with the GDPR and data subject requests. At all times, keep in mind that you may also be processing personal data outside of Oxygis.

Right of access (art. 15) and right to data portability (art. 20)

- Oxygis provides tools that allow data subjects to access and update their personal information in self-service mode.
- If you need to export all the data, or to communicate private data that is not accessible via the portal, certain manual steps are necessary. You can export all the information using your browser's "Print as PDF" function or the "*Export*" menu. Both options provide GDPR-compliant electronic formats.

Reminder: In addition to the ability to export to PDF via your browser, Oxygis has a tool that allows you to export certain records, or a list of records, to a CSV or Excel file, along with the documents linked to that record. To use it, go to the list view of any screen, select the record(s) and click on Export, then choose "Export all data".

Our Helpdesk will be happy to assist you with larger exports.

Right to be forgotten (art. 17)

The GDPR grants data subjects the right to request the erasure of their personal data, under specific conditions, such as:

- **The data is no longer required for the** *purpose for which it* was collected;
- **They are withdrawing their consent for treatment that was based** *solely* **on** *consent;*
- **The treatment is also** *illegal*.

If you determine that the request is legitimate, and you have confirmed the identity of the subject, you may attempt to delete the corresponding *contact* in Oxygis. In this case, you must

decide whether you have any other obligations to retain these documents, and must refuse the deletion request.

If you have no legal reason to keep personal information, but cannot or do not want to delete a document or contact, consider making it anonymous. You can rename the contact and change their recognisable data (email, address, etc.), or you can reassign the documents to a generic *anonymous* contact. Once correctly anonymised, this data will no longer be *personal data*.

Restriction of processing (art. 18) and withdrawal of consent (art. 7)

Users often ask to be unsubscribed from commercial emails. Users can unsubscribe themselves using the unsubscribe link in the footer.

Right to rectification (art. 16) and accuracy of data (art. 5(1)(d))

In terms of rectification, Users and Clients can correct their own personal data (name, email) via the Oxygis Resources / Personal Screen tab. They may also contact our helpdesk at any time.

Consent (art. 7)

When you collect personal data using Oxygis custom fields (for example, by creating your own contact form, subscribing to a mailing list, or registering for an event), you must establish a *purpose* and a *legal basis* for the processing. This largely depends on how you will use the data.

If the purpose is specific and obvious (for example, to store the participants registered for an event in order to keep them informed of the progress of the event; to register a person on the mailing list they have chosen), you do not need to ask for their explicit consent (personal data is *necessary for the performance of a contract* - art. 6 (1) b). However, you must always specify the purpose to the user and refer them to the page of your privacy policy where you provide further information.

However, if you intend to use the data collected for other purposes, you must obtain the user's explicit consent for each purpose.

Privacy from conception (art. 25)

Security by design is at the heart of our R&D work at Oxygis, and we apply security best practices to make our software **safe, robust and resilient** for everyone.

- **Access Control -** Oxygis' default group access control mechanism allows you to restrict access to personal data based on each user's role and needs. If you review

user group assignments and maintain them correctly as roles change in your organisation, you have a solid foundation for confidentiality. You can easily add or modify user groups to suit your organisation.

- **Passwords -** Oxygis stores user passwords in a secure, industry-standard hash.
- **Employee Data -** One area where Oxygis databases are likely to include personal data is in the *Resource / Personal Page tab*, which collects employee usernames.

Security of processing (Articles 25 and 32)

If you use Oxygis Cloud services, we implement best practices in terms of security and confidentiality at all levels. You can read more about this in our ***security policy.***

If you use Oxygis on site, you are responsible for complying with best security practices.

Partners SRL
Belgium : Eikelenbergstraat, 20, 1700 Dilbeek - Belgium- Tel: +32 (0)2 736 10 17 - VAT : BE 0872.350.989
France : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - VAT: FR 13 811593730
www.oxygis.eu - info@oxygis.eu