GDPR

Overview of the new privacy laws and best practices with ERGOBIT

ERGOBIT GmbH and subsidiaries

Since May 25th, 2018, the General Data Protection Regulation (GDPR) is into effect, opening a new era of data protection and privacy for everyone. While you've certainly heard and read a lot of information about GDPR, it can be difficult to understand exactly **what it means for your business**, in practical terms, and **what you should do** to be compliant with the new rules.

At ERGOBIT, we are committed to follow best practices in terms of security and privacy. We strive to provide the same level of protection to all users and customers, without distinction on their location or citizenship. **And we apply those best practices for all data, not just personal data**.

So ERGOBIT GmbH and its subsidiaries are compliant with GDPR.

Summary

1 What you need to know about GDPR

Hint
If you can, the best way to understand GDPR is to Read the Official text.
It's a bit long (99 articles over 88 pages), but quite readable for non-experts.

GDPR is a EU **Regulation**, that aims to **harmonize** and **modernize** existing privacy legislation, such as the EU Data Privacy Directive that it replaces. It lays down rules for the protection of natural persons with regard to the processing of their personal data, and the free flow of personal data within Europe.

It is a **Regulation**, not a Directive, therefore applicable immediately in all EU member states, without requiring transposition into the domestic law of each country. EU countries have a limited margin of interpretation for the finer points, but **fundamental rules will be the same for everyone**, everywhere in EU.

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

In a nutshell: Don't panic!

GDPR is not a world-breaking new legislation, and it is fundamentally a good thing for citizens and businesses.

It's Positive!

We want to emphasize that GDPR can be great for you and yours partners. Complying to the GDPR may initially represent a lot of work, but there are upsides to the new rules:

- Increased trust from your customers and users
- Simplification: same rules are applied in all countries across EU
- Rationalization and centralization of your organizational processes

The purpose of GDPR is to give individuals more oversight on their personal data. ERGOBIT already put in place the correct strategies and systems, and do manage your data with security and safety now and in the years to come. Moreover, ERGOBIT will support all their customers and partners to be compliant.

1.1 What are the risks if you aren't compliant?

The maximum penalty for non-compliance is an administrative fine of 20 million euros, or 4% of your global annual turnover, whichever is higher. A smaller maximum of 10 million euros or 2% of your global annual turnover is applicable for lesser infringements.

These maximums are meant to be **dissuasive** for businesses of all sizes, but GDPR also requires the fines to be kept **proportionate**.

Supervisory authorities (also known as Data Protection Authorities: DPAs) must take into account the circumstances of each case, including the nature, gravity, and duration of the infringement. These DPAs are also granted powers to **investigate** and **impose corrective actions**, which include the limitation of the infringing activities, without necessarily imposing a fine.

Another risk if you do not comply is the loss of trust from your employees, partners, customers and prospects, who care about the way you process their data!

1.2 Key principles of GDPR

Scope

The regulation applies to any **processing** of **personal** data by **any organization**:

1. If the controlling or processing organization **is located in the EU**
2. If the organization **is not located in the EU**, but the processing involves personal data of data subjects located in the EU, and is related to commercial offerings or behavior monitoring.

The scope therefore includes non-EU companies, which was not the case with older legislation.

Roles

The regulation distinguishes two main types of entities:

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

As our clients owns the database hosted in our Cloud, they are the **data controller** of their database while ERGOBIT is the **data processor**.

Personal Data

GDPR gives a broad definition of personal data: **any information relating to an identified or identifiable natural person.** An identifiable person is one that can be identified, **directly or indirectly**, by means of their names, emails, phone numbers, biometric information, location data, financial data, etc. Online identifiers (IP addresses, device IDs, …) are also in scope.

This applies **in business contexts too**: *info@ergobit.org* is not considered personal, but *john.smith@ergobit.org* is, because it can be used to identify a physical person within a company.

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

Data Processing Principles

In order to be compliant, processing activities must observe the following rules:
(as listed in Article 5 of GDPR)

1. **Lawfulness, fairness and transparency**: to collect data, you must have a *legal basis*, a clear *purpose*, and you must *inform* the subject about it.
    - Have a simple and clear Privacy Policy, and refer to it everywhere you collect data
    - Verify the legal basis for each of your data processing activities

2. **Purpose limitation**: once collected for a purpose, request permission if you want to use it for a different purpose.
   e.g. - You can't decide to sell your customer data if it was not collected for that purpose.

3. **Minimization**: you must only collect the data necessary for your purpose.

4. **Accuracy**: reasonable steps should be taken to make sure that data is kept updated, with regard to the purpose
   e.g. - Be sure to handle bounced emails, and correct or delete the addresses.

5. **Storage limitation**: personal data should only be kept for the duration needed to fulfill its primary purpose.

e.g. - Define time limits for erasure or review of the personal data you process, depending on their purpose.

6. **Integrity and Confidentiality:** data processors must implement appropriate access control, security and data loss prevention measures, in accordance with the types and extents of data being processed.
   e.g. - Make sure your backup system is working, have proper security controls in place, use encryption to protect sensitive data such as passwords, ...

7. **Accountability**: data controllers are responsible for, and must be able to demonstrate compliance with all above processing principles.
   - Establish and maintain a data mapping reference for your organization, describing the compliance of your processing activities
   - Inform your customers via a clear Privacy Policy

Legal Basis

In order to be lawful under GDPR (*first principle*), processing of personal data must be based on **one of six possible legal bases**, as listed in Article 6 (1):

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

One major change brought by GDPR over previous data privacy regulation is the stricter requirements for obtaining valid **consent**.

Data Subject Rights

Existing data privacy rights for individuals are further expanded by the GDPR. Organizations must be prepared to handle requests from data subjects in a timely manner (within 1 month), free of charge:

1. **Right to Access** - Individuals have the right to know *what* and *how* their personal data is being processed, in full transparency;

2. **Right to Rectification** - Individuals have the right to obtain *correction* or *completion* of their personal data;
3. **Right to Erasure** - Individuals have the right to obtain *deletion* of their personal data for legitimate reasons (consent withdrawn, no longer necessary for the purpose, etc.);
4. **Right to Restriction** - Individuals can request that the controller *stops processing* their personal data, if they do not want or cannot request full deletion;
5. **Right to Object** - Individuals have the right to *object* to certain processing of their personal data at any time, for example for direct marketing purposes;
6. **Data Portability** - Individuals have the right to request that personal data held by a controller be *provided to them*, or to another controller.

2 How you should prepare for GDPR

Disclaimer
We cannot provide legal advice; this section is only provided for informational purposes. Please reach out to your legal counsel in order to determine exactly how GDPR affects your company.

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

1. Establish a **Data Mapping** of the data processing activities of your organization to *get a clear picture of the situation*. Data Protection Authorities often provide spreadsheet templates to help in 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 treatment; the technical and organizational *security measures* implemented, and the *subcontractors* (processors) involved. You will need to maintain this data mapping regularly, as your processes evolve.
2. Based on step 1, choose a **Remediation Strategy** for any processing where you do not have a legal basis (e.g., missing consent) or where you do not have appropriate security measures in place. Adapt your processes, your internal procedures, your access control rules, backups, 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 are the rights of individuals with regard to their data.
4. Review your **Contracts** with a legal counsel, and adapt them to GDPR.
5. Decide how you will answer the various kinds of **Data Subject Requests**.
6. Prepare your **Incident Response Procedure** in case of data breach.

Depending on your situation, other elements could be added to the list, such as the appointment of a Data Protection Officer. Consult your internal processing experts and your legal counsels to determine any other relevant measure.

Remember!
Establishing a clear mapping of your processes will make everything easier on the road to compliance!

3 How is ERGOBIT compliant with GDPR

At ERGOBIT, implementing privacy and security best practices is not a new idea. As an ERP integrator and Cloud hosting company, we're constantly revising and improving our systems, tools and processes, in order to maintain a great and secure platform.

Our GDPR Roles

Our responsibilities in terms of personal data protection depend on our various data processing activities:

Our Roles	Data Processing	Kind of data
Data **Controller** & Processor	**On ERGOBIT Cloud**	Personal data provided to us by our direct customers and prospects, our partners and all **direct users of ergobit.cloud** (names, emails, addresses, passwords ...)
Data **Processor**	**On ERGOBIT Cloud**	Any personal data stored in the databases of our customers, hosted in the ERGOBIT Cloud or transferred to us for the purpose of using one of our services. The owner of the database is the **data controller**.

Our GDPR documents

As a **Data Controller**, our activities are covered in our Privacy Policy, which has been updated for GDPR. This policy explains as clearly as possible *what* data we process, *why* we process it, and *how* we do it. Closely related to this, our Security Policy explains the security best practices we implemented at ERGOBIT, at all levels (technical and organizational) in order to guarantee that your data is processed in a safe and secure manner.

In addition to those policies, our activities as a **Data Processor** are subject to the acceptation of our ERGOBIT Terms of Service. This agreement has been updated in order to add the necessary Data Protection Clauses (often referred to as a "Data Processing Agreement"), as required by the GDPR.
As a Customer of ERGOBIT GmbH you don't have anything to do to accept these changes, **you already benefit from the new guarantees**, and we will consider that you agree if we don't hear anything from you!

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

4 How does ERGOBIT help you implement GDPR best practices?

Using our cloud platform and the applications we deliver to manage your business **cannot be sufficient for GDPR compliance**, *because the regulation applies to your whole organization.*
However, because ERGOBIT centralizes your data, reduces data redundancy, and implements granular access rights and security controls, it can be a great help to comply with the GDPR.

Here are some ways we think we can help you in the context of GDPR, for your ERP applications and databases.

Disclaimer: as always, consult your legal counsel in order to determine how you should comply with GDPR and data subject requests. At all times, keep in mind that you may be processing personal data outside of SAP or Odoo as well.

Right to Access (Art. 15) and Right to Data Portability (Art. 20)

- ERGOBIT provides some tools for the data subjects to access and update their personal information in self-service mode:
    - **The customer portal** allows users to browse contractual documents: address and contacts, invoices, quotations, orders, tasks, helpdesk tickets, purchases, subscriptions, delivery orders, payments as well as communications around these documents.
    - **The mailing lists** allows users to review and manage their contract data
    - **The forum profile** allows your forum users to review all their activities at a glance
- If you need to export all data, or to communicate private data that is not accessible through the portal, some manual steps are needed.
  Usually, you can reach all relevant documents directly from top bar on the contact form of the users, where they are linked. You can then export all information with the “Print as

PDF" feature of your browser, or with the *Action>Export* menu, from the list of contacts or the list of their documents.
Both options provide GDPR compliant electronic formats.

- In addition to that, you might have information not linked to the contact form, that the data subject might have entered in a separate context. You should also review those, searching by name or email address, for example
    - Events subscriptions
    - Leads & Opportunities in your CRM

Reminder: In addition to being able to export as PDF via your browser, our systems have a tool to export any record, or list of records, in a CSV or Excel file, as well with the related documents linked to this record. To use it, go to the list view of any screen, select the record(s) and click on Action > Export, then choose "Export All Data". The tool then allows you to choose fields you want to export.

Right to be forgotten (Art. 17)

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

- **The data is not necessary anymore according to the** *purpose*;
- **They withdraw consent for a processing that was based on** *consent only;*
- **The processing is otherwise** *unlawful*.

If you determine that the request is legitimate, and you have confirmed the identity of the subject, you can attempt to delete the corresponding *contact* from the SAP or Odoo system. This is safe: the system will block the operation if a business document still refers to the contact (invoice, contact, delivery order, forum post, etc.). In that case, you should decide whether you have other obligations to keep these documents, and must decline the erasure request.

If you have no legal reason to keep the personal info, but cannot, or do not want to delete a document or contact, consider anonymizing it instead. You can rename the contact and change its recognizable data (email, address, etc.), or you can re-assign documents to a generic *Anonymous* contact. Once properly anonymized, this data will not be *personal data* anymore.

Restriction of Processing (Art. 18) and Consent Withdrawal (Art. 7)

Users will often ask to be unsubscribed from commercial emails. If your mailings were sent via SAP or Odoo, users can do it themselves using the footer's unsubscribe link. But you can also manually tick the "opt-out" field on a contact or lead/opportunity. Records marked "opt-out" are automatically excluded from mass-mailing campaigns, but can still receive direct messages from users (e.g. quotations, invoices).

Right to Rectification (Art. 16) and Data Accuracy (Art. 5 (1) d)

Invalid/changing email addresses are a common source of data error. When email integration is properly configured, SAP as well as Odoo handles email bounces in your mass-mailings, and increments a *Bounce* field with the number of bounced messages. You can periodically review your contacts or prospects with a custom search on *"Bounce* greater than *0"* and cleanup/delete them.

Followers of Discuss channels are automatically unsubscribed after 10 bounces.

In terms of rectification, users and customers can also correct their own personal data (name, email, address) through our customer portal.

Consent (Art. 7)

When you collect personal data via SAP or Odoo's default mechanisms (e.g. contact form, mailing-list subscription, event subscriptions), you have to establish a *purpose* and *legal basis* for the processing. This greatly depends on how you will use the data.

If the purpose is specific and obvious (e.g., store registered event participants to keep them informed about the tenure of the event; subscribe someone to the mailing list they chose), you do not need to ask for their explicit consent (the personal data is *necessary for a contract* - Art. 6 (1) b). However, you still need to make the purpose clear to the user, and refer to your Privacy Policy page where you give more information. You can use tools like Odoo's website builder to edit the forms and add the required mentions.

However, if you plan to use the collected data for other purposes, you need to obtain explicit consent for each purpose from the user. The recommended way is to add checkboxes to your form to get the consent for each specific purpose (e.g., "Please send me discounts and promotions on similar products via email").

Privacy by Design (Art. 25)

Security by Design is at the heart of our Cloud R&D work at ERGOBIT, and we apply security best practices to make our software modules sale, robust and resilient for everyone.

Access Control - The default group-based access control mechanism of all software we deliver allows you to restrict access to personal data according to each user's role and needs. (e.g., a project manager might not need access to Job Applications). If you review the user groups assignations and maintain them properly when roles change in your organization, you have a strong privacy basis. You can easily add or modify user groups to tailor them to your organization.

Record Rules - To fine tune access to personal data, you can use the concept of Record Rules, which let you restrict access to documents according to any criterion based on field values. Record Rules can block read and/or write operations, and they work on a per-document basis.

Passwords – All user passwords are stored with industry-standard secure hashing. It is also possible to use external authentication systems such as Microsoft OAuth 2.0, Google or LDAP, in order to avoid storing user passwords at all.

Employee Data - One area where SAP and Odoo databases are likely to include sensitive personal data is the *Private Information* tab of the employee form and their contracts. This part of the Employees Directory is only visible to HR personnel ("HR Officer" group), who need it for their job. This protection has been recently extended to the personal address of employees, which are stored as Contacts, by adding a new address type ("Private") that is visible only to HR personnel.

Security of Processing (Art. 25 & 32)

If you use ERGOBIT Cloud services, we implement security and privacy best practices at all levels. You can find more about it in our Security Policy.
If your system is implemented on-premise, we deploy it according to our security guideline, but once the system is handed over, you are responsible for following security best practices.


ergobit
consulting