ELO for GDPR

Solutions and functionalities for implementing the requirements of the new European General Data Protection Regulation (GDPR)

ELO Digital Office

Meet GDPR requirements with ELO

Dear readers,

The new Europe-wide General Data Protection Regulation, or GDPR, came into force on May 25 of this year, with compliance mandatory for all businesses — small and large.

For many, it is welcomed as a long-overdue measure to protect individuals from fake news and data misuse in this cyber age. For others, it is an overly complex piece of regulation that presents enormous implementation challenges, particularly to smaller businesses.

There is no question about the importance of data privacy and security, and yet it is no secret that these aspects are often neglected. The rise in the number of reported data breaches illustrates this only too well. However, there is a large degree of uncertainty surrounding GDPR and what it will mean for businesses moving forward.

This most certainly evolves from the threat of potential fines of up to 20 million euros, or 4% of annual global turnover, but also because the regulation is seen as difficult to interpret and contains little information about what it means in practice. Articles 13 and 14, which govern the obligation to inform the data subject prior to collecting personal data, are a good example of this. In practice, it may be difficult or even impossible to meet these requirements.

Having attended a number of keynotes and workshops on GDPR by legal experts and privacy activists, I can safely say that everyone left feeling more uncertain than before. This is largely because there was no clear guidance on how to implement the regulation.

That said, I would like to point out what a great job the authorities are doing helping to explain the specifications and offering useful tips, despite the lack of manpower resources.

We have put together this brochure as a practical and compact guide to the most important requirements of the new EU-wide regulation. At the same time, we want to show you how **ELO for GDPR** meets the functional and technical requirements for successfully implementing GDPR across your organization.

I hope you enjoy reading this guide and that it provides a great deal of insight on GDPR!

Karl Heinz Mosbach
CEO, ELO Digital Office GmbH

Contents

› Despite the efforts to create a uniform Europe-wide data protection standard under GDPR, the opening clauses leave room for the legislators in the EU member states to implement the regulation in accordance with national regulations. Therefore, there are differences at national level as to how the provisions will be implemented, interpreted and enforced. As the brochure has been translated from German, national regulations for other EU member states have not been addressed.

The information in this brochure is of a general, non-binding nature and does not constitute legal advice. Although it was compiled with the utmost care, it does not claim to be correct, complete, and/or up-to-date, nor does it consider special circumstances in individual cases. It is advisable to seek legal advice if you require specific information for your company's requirements.

ELO disclaims all liability in respect of the information in this brochure.

What is the GDPR?

GDPR: Company directors are responsible

Although GDPR is to a large extent an issue for IT managers and data protection officers, overall responsibility lies with the top management level. These persons are held accountable for ensuring compliance.

The new legislation therefore attaches personal liability to company directors, firstly for the high fines that supervisory authorities could impose, and secondly because employees could also sue the company for non-material damages in the event of negligence and serious breaches of GDPR.

› **The bottom line:**
Data privacy requires a top-down approach!
Taking the necessary measures is easy, ignoring them amounts to gross negligence.

Fines and liability risks

Although a wave of litigation is not expected to follow the introduction of GDPR, the risks are still high, particularly in the event of serious violations. Companies are liable to pay fines of up to 4% of annual global turnover and must report any data breaches to the authorities within 72 hours.

The damage from Facebook's data scandal involving Cambridge Analytica would have been a potential $1.6 billion financial penalty. This example illustrates just how much power the supervisory authorities have, including the ability to conduct unannounced audits. The future will show to what extent GDPR will affect businesses. Companies that do not comply run the risk of being issued warnings from competitors or being sued for immaterial damages by injured parties such as former employees or irate customers.

Although there is a general optimism that these cases will be limited, it could go the other way: The market for law firms specializing in data privacy could potentially become huge.

For this reason alone, it is essential that businesses implement the necessary measures to comply with GDPR.

When are companies allowed to process personal data?

The general rule is that companies are not allowed to process personal data unless the data subject has provided their consent. This is the case if ...

1. ... the data subject has voluntarily given specific and unequivocal consent to the processing of his or her personal data.

This can be done by signing a form or simply ticking a declaration of consent (opt-in) check box on the company's website. It is important that the form and purpose of data collection/processing (privacy policy) must be clear and unambiguous to the consenting person and that the consent can be revoked at any time. In the case of newsletter subscriptions, companies must ensure that they use the double opt-in method to verify the e-mail address (additional e-mail confirmation).

The name, date, time, and IP address (or location) need to be logged in the system. The same applies to business cards if a company intends to file them or input the details into an address database.

Information:
Companies are not under any obligation to obtain new declarations of consent for existing databases, provided that the information was collected in line with the old EU Data Protection Directive (95/46/EC).

2. … the company has a legitimate interest for storing and using data, such as a contractual obligation.

This is part of every customer relationship. Data subjects must have provided consent to have their data processed for a specific purpose. Companies are not permitted to pass on any data to third parties without the data subject's explicit consent. If personal data needs to be passed on (e.g. to a parcel service) for fulfilment of a contract, this is of course permitted. However, the company must make a clear indication of this in its privacy policy. In addition, companies are required to conclude a written data processing agreement with all companies that process data on behalf of a controller. Where data is processed (e.g. by cloud services, external service providers, shop providers, etc.), both sides are responsible.

3. … processing is necessary for the purposes of the legitimate interests pursued by the controller.

Accordingly, companies are allowed to process personal data (e.g. direct mail on new products, customer evaluations, etc.) but this does not apply if such interests are overridden by the interests or fundamental rights of the data subject which require protection of personal data. Companies are also permitted to collect and analyze data for a specific purpose, such as to be able to provide a customer with proper advice. In these cases, the data subject is not required to give consent for the collection and storage of such data.

4. The data subject must be informed in all cases!

When personal data is collected, the controller must provide the data subject with information about the company's privacy policy (Articles 13 and 14 GDPR) in advance. These measures are easy to implement online, but how can they be put into practice in everyday situations, such as making a dental appointment over the phone? Independent data institutes have issued a recommendation that businesses only need to include and make clear reference to their data protection regulations on the company website and, in the case of the dental practice, hand out an information sheet to the data subject on the first visit. That said, there is still uncertainty surrounding Articles 13 and 14 of the new law.

5. Other cases

Companies have a lawful basis for processing if it is required to:

- fulfil statutory obligations
- protect the vital interests of the data subject
- perform a specific task in the public interest

- **Written contracts between controllers and processors:**
  Whenever a controller uses a processor to process personal data, there must be a written contract. This does not apply if processing is occasional (e.g. shipping services, support/ maintenance). Although it is a contractual agreement, it only needs to be in electronic form (scanned or as a PDF document).

GDPR defines personal data that refers to an identified or identifiable natural person in two categories:

a) General data such as name, address, telephone number, e-mail and IP address, etc
b) Personal, sensitive data such as religion, illnesses, biometric data, etc. Under GDPR, these categories of data are particularly sensitive.

Protecting data subjects' rights

Compliance with the obligations under GDPR to protect data subjects poses a challenge for many companies. This applies mainly to:

1. Right of access

Under GDPR, every data subject has the right to obtain information on what personal data has been stored within one month of it being obtained. Companies often lack the tools and resources to be able to provide this information quickly on request. Hence, appropriate technical and organizational measures need to be taken to ensure that these requirements are met. The controller must verify the identity of the data subject before disclosing any data.

2. Right to data portability

This allows data subjects to obtain data that a controller holds on them and to use it for their own purposes. Of course, this isn't a problem if it concerns only basic data such as contact details. When it comes to extensive customer files, patient records, construction files, and e-mail traffic, however, companies are faced with an entirely different scenario as this requires a great deal of manual input, technical support, and of course financial resources. If data is transferred in a ZIP file or on a data carrier, for example, companies must ensure that it is encrypted and that the password is transmitted separately, e.g. by SMS or by post.

3. Right to erasure

In principle, every data subject has the right to request the deletion or removal of personal data, provided that it does not need to be stored in accordance with statutory retention periods or other regulations. The typical retention period for countries in Europe is from five to ten years for general documents and tax papers. If companies are unable to delete information for technical reasons, such as in the case of tape backups, controllers must restrict or block access to this data.

There are a number of statutory provisions that explicitly specify a deletion period, provided that the data subject has not consented to their data being stored. Job applications can usually only be held for three months, for example. However, this does not apply to reimbursement of associated expense claims, which must be retained for ten years for tax purposes. If we look at current practice, it is evident that companies have made very little progress when it comes to deleting specific data, primarily due to the time and resources required to do so. As a result, many organizations are hoarding vast amounts of old data that are unnecessary or have no legal weight. GDPR will put an end to this practice. Controllers are required to implement solutions that delete personal data once the retention period has expired as well as to maintain a record of all activities (Article 19). Under GDPR, data subjects are also entitled to have their data rectified or to object to their data being processed.

Other rights of the data subject:

- **Right to rectification**
- **Data subject must be informed**
- **Right to object**
- **Right to restrict processing**

IT security measures

The security of IT systems is not something that companies have only needed to consider since GDPR came into force, but this aspect is getting more attention as a result, not least because of the data breach penalties that companies could end up facing. The implementation of appropriate technical and organizational measures is mandatory, yet a large number of SMEs still have serious vulnerabilities in their systems, perhaps because their firewalls are out of date or there is no history of backups, meaning that changes can simply be overwritten. In addition, many organizations advocate open data or use server rooms for storage that can be accessed by anyone. The list of examples is endless.

These types of shortcomings are especially alarming given the implications of GDPR. Companies are recommended to review and document their IT security systems step by step and it might also be wise to invest in a GDPR audit by an expert. There are plenty of checklists and guides offering all sorts of information on this subject. In any case, companies must regard these measures as an absolute necessity, since loss or theft of data can cause far greater financial damage.

Documentation obligation

According to Article 30 GDPR, almost every company is obliged to keep a record of processing activities documenting where they process personal data (applications, databases, etc.). In addition, they are required to document the technical and organizational measures that have been taken to comply with and guarantee data protection regulations.

Smaller companies in particular may be put off by the amount of work involved. Naturally, it takes time to create such records, but it helps to adopt a structured, team-oriented approach. Moreover, companies are not on their own: Supervisory authorities are providing templates (e.g. for creating records of processing activities) that can be adapted as well as checklists and forms for implementing technical and organizational measures. And, if each department undertakes compliance measures on their own, the task is not so overwhelming. Besides meeting GDPR requirements, this documentation has another major benefit for companies in that it ensures they are transparent and have a clear audit trail of their data protection measures, regardless of whether the data is personal or sensitive within the organization.

Data protection impact assessment

In rare cases where new technologies are used to process special categories of data (sensitive data) on a large scale, the controller must carry out a data protection impact assessment. This essentially constitutes a risk analysis of IT security and processes.

Data protection officer

The obligation to appoint a data protection officer is regulated differently in EU countries. In Germany, companies must elect a data protection officer if at least ten employees process personal data on a regular basis as part of their job (e.g. sales, marketing, order center etc.). This does not apply to employees who are not regularly commissioned with processing (record, store, etc.) personal data (e.g. mechanics, etc.). If an organization needs a data protection officer, it can designate an existing employee who has been provided the relevant training or it can outsource the task to an external data protection specialist, which is a more suitable option for smaller businesses. Organizations are also required to publish the details of their data protection officer on their website and provide these details to their supervisory authority.

The most important organizational measures at a glance

- ☑ Document processing activities and technical and organizational measures
- ☑ Training and instruction of employees
- ☑ Corporate guideline (e.g. company directive) on data protection and processing personal data

  Recommendation: Organizations should separate personal data from company data. This includes measures such as not allowing employees to send private e-mails from their work e-mail account and ensuring that private e-mails are kept separate and deleted.
- ☑ Proof of data subject's consent (record of name, date, IP address, location, etc.)
- ☑ Written contract between controller and processor
- ☑ Revise privacy policies to ensure that obligations are covered and that rights of the data subjects are clearly articulated
- ☑ Review and optimize access authorizations, encryption, and security in general
- ☑ Appoint a data protection officer and provide these details to the supervisory authority

Cooperation with the supervisory authorities

Supervisory authorities are not just responsible for imposing fines, but also provide companies with advice on GDPR issues. However, GDPR also grants authorities extensive powers, such as to conduct unannounced inspections and audits. It is absolutely imperative that companies report data breaches (e.g. data theft) to the supervisory authority within 72 hours. Failure to disclose a breach merely increases the chances of facing an even bigger fine.

Help is at hand: ELO for GDPR

There is good news for all ELO users and companies that are planning to install the software: ELO is the ideal platform for implementing and complying with GDPR requirements. **ELO ECM Suite 11** provides numerous functions such as deletion deadlines, global fields for personal data, a processing database, standard forms, and much more: **ELO for GDPR** has all your company needs to ensure that personal data is handled correctly and kept secure.

Mark data as personal

Most companies are likely to hold personal data of one form or another in their systems, stored in places like e-mails, mail accounts, databases, or random file directories. Under GDPR, every data subject has the right to know what personal data is stored. As a result, companies are required to dedicate time and resources to granting such requests.

Version 11 of the ELO ECM Suite gets around this problem as the data model provides an option for marking data as GDPR relevant. It enables users to assign a unique personal identifier (name, employee number, customer number, etc.) to each document, file, and all metadata across administrative datasets, which means they can see what data is stored for a particular user in just one click. The technology features encryption to ensure that sensitive data, such as personal data, can only be accessed by authorized individuals.

Automatic deletion after a specified period

One of the additions to **ELO ECM Suite 11** is the global data field "End of deletion period", which, in combination with the field "End of retention period", triggers an automated deletion process. Companies can use these fields to delete data that is old or no longer relevant as well as to comply with the deletion obligations under GDPR. Deleting this data manually would be costly and time-consuming.

Thanks to ELO, this process is secure and automated, and each action is logged to ensure transparency and the ability to provide information. The software also takes statutory retention periods into account: In the case of general documents and tax papers that must be retained for ten years, a deletion request will not be honored until the retention period is over.

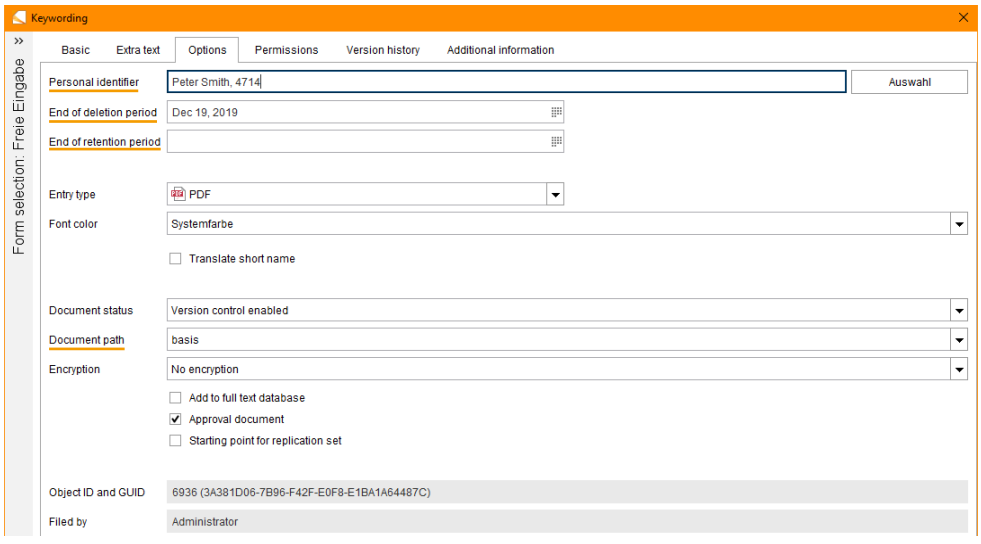


Image:
GDPR data fields in **ELO ECM Suite 11**

Security and purpose limitation

The new European data protection regulation builds on the notion of privacy by design. GDPR compliance is at the heart of ELO products. The standard versions of our specialized business solutions for candidate, visitor, and contract management, or the electronic personnel file, come equipped with numerous data protection functions. In addition, the standard permissions and classification system in ELO can be used to manage purpose limitation and access restrictions for all business processes and workflows. Organizations are expected to use encryption technologies to protect personal data that is highly sensitive. Unlike many other systems that require users to install additional encryption components manually, the ELO system offers such functionalities as a standard feature. Once personal data is encrypted, it is possible to restrict access to individuals or a selected set of users, for example. Even if a hacker manages to gain access to encrypted data, the use of the highly secure 128-bit encryption method renders this data useless.

ELO form database for easier documentation

GDPR brings increased documentation obligations to businesses: This includes documentation of the technical and organizational measures implemented for data and process security, the data processing agreement that must be concluded when a controller passes data on to third parties or detailed documentation of where and how personal data is used in the company.

To make this easier for companies, **ELO for GDPR** offers a variety of sample forms that businesses can easily adapt to suit their own needs. This is essentially a database of sample forms in ELO that enables users to automatically create documentation with the help of predefined standard texts and also provides a simple change management tool. Another advantage of this database is the option to evaluate and analyze data in a dashboard using the **ELO Analytics** component. In just a single click, users can generate an overview that shows them which areas special categories of personal data, customer or patient data are processed in.

Create system documentation automatically

Many companies struggle when it comes to documenting technical and organizational measures such as keeping a record of permissions structures and who has access to what data, or exact descriptions of processes, such as for when data needs to be deleted, how approval workflows are structured, and so on. **ELO for GDPR** provides automatically created documentation to help you implement these compliance requirements.

ELO export function for data portability

The new European data protection regulation also governs the right to data portability: The data subject has the right to be informed about which personal data a controller has stored about them, but also has the right to have this data transferred to another controller, such as when switching to a new mobile phone provider.

ELO provides an automated export function for documents and metadata, which enables companies to easily export personal data in encrypted form so that it can be sent by e-mail, downloaded or stored on a portable device. Users also have the option to generate a transmittal letter, which documents in detail which data was transmitted in which version.

ELO for GDPR – Overview of functionalities

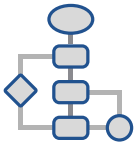
Encryption technology/ authorization protection

Tag data as personal

All processes are logged

Personal data is separated from the rest

Automated deletion (life cycle)



Workflow/ Approval/ Permissions

Export function for data portability

Dashboard for: Reporting and metrics

Central dashboard for GDPR-relevant management of data

Considering the vast requirements associated with the new data protection regulation, it quickly becomes clear that without an appropriate IT solution, it is easy to get lost in the GDPR jungle.
Companies need to be transparent and accountable, particularly if an audit has been announced. ELO provides a **GDPR dashboard** that helps those responsible maintain their data management processes and visualize the most important aspects of compliance, such as the scope of personal data, areas of processing, audits conducted, change and patch management, and much more. It can also be used as the main data management cockpit for the data protection officer and management.

ELO e-mail management

E-mail inboxes and system backups are one of the leading causes of data hoarding with organizations keeping personal data for far longer than is required by law. Thanks to the **ELO e-mail management system**, this is no longer a problem: Users can assign e-mails to a specific business processes and ensure that they are automatically deleted in accordance with data protection regulations once the retention period has expired.

ELO Business Solutions are GDPR compliant

ELO Business Solutions provide customers with ready-to-use solutions for streamlining projects. Besides helping drive your business forward, they ensure your processes are in line with GDPR.

Digital HR solutions from ELO: personnel file and candidate management

HR is an area in every company that is particularly impacted by GDPR due to the highly sensitive personal data that is collected and retained. SMEs in particular often lack a professional HR management solution. **ELO HR Personnel File** and the candidate management tool **ELO HR Recruiting** can be used as standalone modules or can integrate with existing HR systems, bridging the gap between personnel processes and IT. The solutions combine HR business logic and standardized processes to make workflows more efficient and more secure.

Digital contract management: ELO Contract

Contracts with customers always contain some form of personal data. Contract documents are often managed at different locations (hard disks, file directories, mobile devices, etc.), and it is not is always clear where copies of a contract are stored and who filed them there. **ELO Contract** not only provides departments with an efficient tool for managing contracts in a single location and in accordance with statutory retention policies, but also helps them to comply with the obligations set out in GDPR.

Digital visitor management: ELO Visitor

The professional digital visitor management solution from ELO not only streamlines the guest process, but also meets the basic requirements of GDPR. The tool enables employees to quickly create visitor ID badges, track your visitors and monitor where they are, store safety instructions, and much more. Personal data that is collected during the visit, such as the guest's name, company, or vehicle registration plate, needs to be deleted after a specified time: **ELO Visitor** ensures compliance with the regulation.

Do you have any questions about the ELO product portfolio and our solutions for compliance with GDPR?

› Contact one of our local branch offices:
www.elo.com/en/locations
or send us an e-mail:
info@elo.com

ELO for GDPR

Solutions and functionalities for implementing the requirements of the new European General Data Protection Regulation (GDPR)

ELO® is available from:

USA
ELO Digital Office Corporation,
50 Milk Street, 16th floor,
Boston, MA 02109, USA;
info-usa@elo.com

Europe
ELO Digital Office GmbH, Tübinger Strasse 43,
70178 Stuttgart, Germany; info@elo.com

Asia
PT ELO Digital Office Indonesia, AKR Tower (Gallery West), 16 A Floor,
Jl. Panjang No.5 Kebon Jeruk, Jakarta Barat 11530, Indonesia; info@elo.co.id

Asia–Pacific
ELO Digital Office AU/NZ Pty Ltd, Level 12, 65 Berry Street,
North Sydney NSW 2060, Australia; info@elodigital.com.au

ELO Digital Office