GET GDPR COMPLIANT

GDPR compilance and solutions

A Swedwise guide in association with OpenText

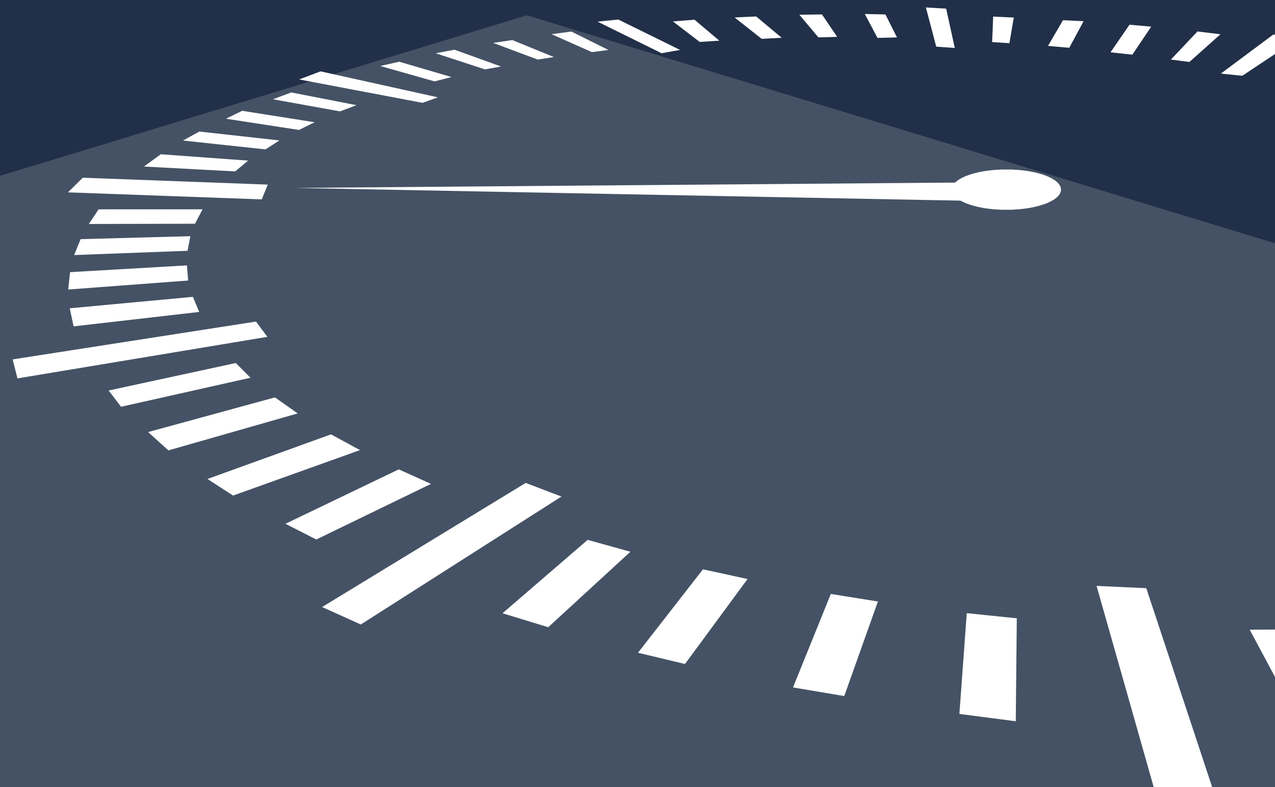
opentext™ | Partner
Reseller Silver

SWEDWISE

GDPR - The story so far

From May 25, 2018, all companies' daily work with personal information must comply with the GDPR (General Data Protection Regulation) regulations. The amount of information and the fact that it exists in many different places pose a significant challenge for many to control, maintain, and share information in a correct manner.

In the first six months since the law came into effect, over 1,200 reports of violations were submitted to the Swedish Data Protection Authority.

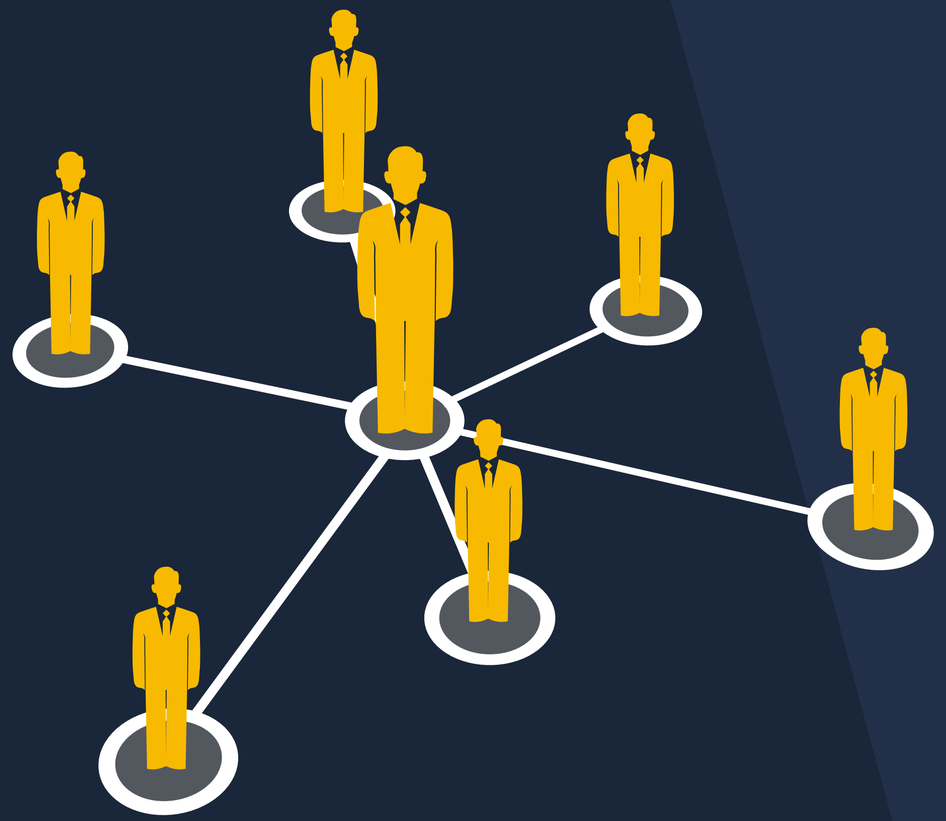


Is your organization affected by GDPR?

All companies and organisations that collect and process personal data of EU citizens must comply with GDPR regulations and may be liable for the penalties that may arise from non-compliance. Personal data covered by GDPR includes information about customers, suppliers, service providers, and others that the organization deals with. It also applies to information on how it exchanges data with trading partners and other networks.

It is essential to remember that organisations outside the EU are also subject to GDPR and the penalties and consequences for non-compliance. All organisations that collect personal information about EU citizens must follow the rules specified by GDPR.

What does GDPR define as personal data?



As specified in the regulation, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

GDPR is intended to cover all personal information routinely shared by citizens during trade-related activities with any entity.

Notable Changes under GDPR:

STRICTER RULES FOR CONSENT.

GDP requires individuals to give clear, informed consent before their information can be processed. Consent cannot be assumed based on inactivity.

INCREASED RIGHTS FOR DATA SUBJECTS.

Individuals have more rights under GDPR, including the right to have their personal data erased, have incorrect data corrected, be completely removed from digital marketing, and request their data to be moved to another data service.

NOTIFICATION OF DATA BREACHES.

Organisations must inform those affected by a breach within 72 hours after the breach occurs.

SERIOUS FINES.

Fines can amount to €20 million or 4% of the annual global revenue, whichever is greater.

INCREASED ACCOUNTABILITY

There are several new governance requirements for the affected organisations, including conducting assessments of the impact of personal information and appointing a data protection officer.

How does GDPR affect legal departments??

Legal departments must review GDPR to fully understand all requirements including new or changed processes, roles, responsibilities, and training requirements. This is not just a matter of compliance and legal requirements. It will rather require a coordinated effort with all parts of the organisation that handle personal data. Ultimately, all responsibility lies with the legal department, but almost all departments will be affected and have a responsibility to comply with the regulation.

As previously mentioned, the penalties are high. You are dealing with a regulation that gives individuals the "right to be forgotten". If you guarantee that this right has been fulfilled but still have stored information about that individual, those responsible will be held accountable.

All organisations must carefully review every policy and process that involves personal data and ensure that the organization complies with all requirements regarding privacy and data protection.

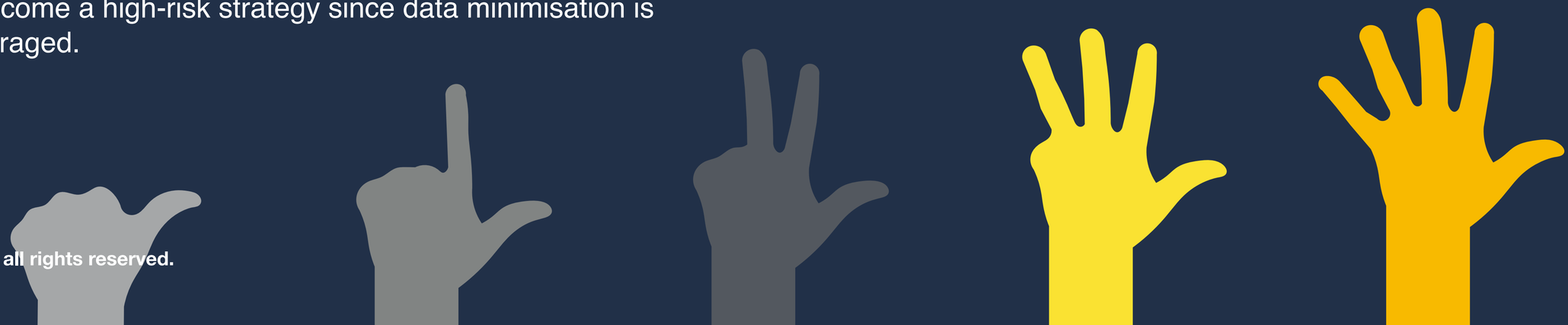
How does GDPR affect Marketing departments?

Looking at it in the long term, GDPR can be seen as good news for marketers. It is a step towards reducing targeted marketing messages. Brands will actively have to seek customers' consent to market to them. Such consent must be given with the customer's full knowledge and active participation to comply with GDPR guidelines.

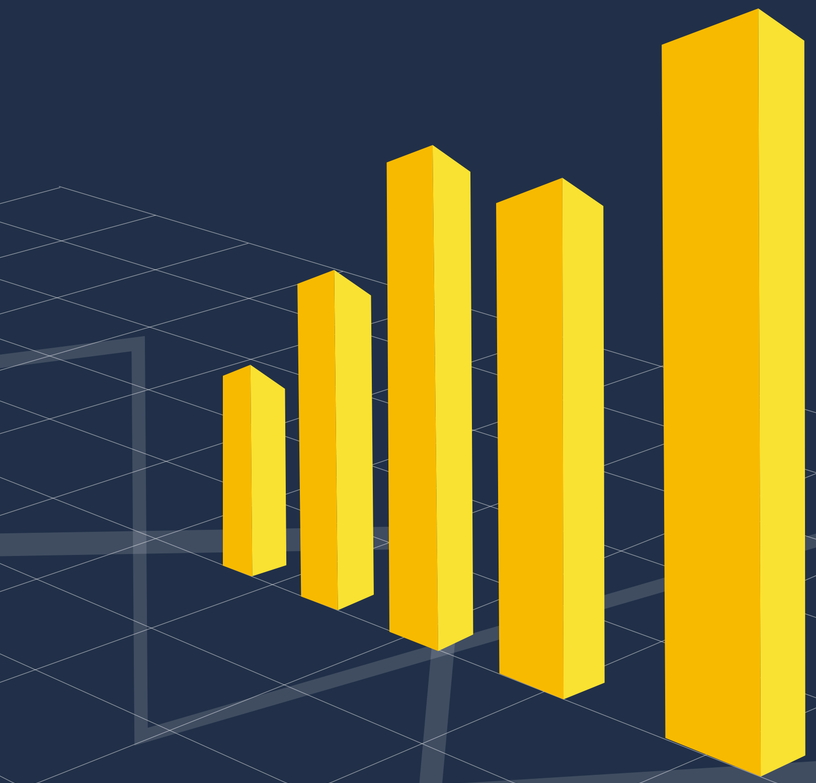
Marketers will need to come up with and develop tailored ways to follow the rules while continuing to deliver the effective, personalised product recommendations, services, and customer experiences that customers demand. The classic approach of "collecting as much customer data as possible now and figuring out uses later" will become a high-risk strategy since data minimisation is encouraged.

GDPR aims to reduce or eliminate many of the misleading consent strategies that exist today and that marketers use to simply reach as many contacts as possible. Instead, companies are encouraged to obtain consent for marketing from the individual.

When GDPR is implemented correctly, it will lead to a reduction in poorly identified potential new customers, automated fraud from computers, and ultimately an elimination of the haphazard approach that many have exploited so far.



How does GDPR affect records management?



Like many regulations, GDPR places demands on documentation and archive management so that organisations can effectively report on and demonstrate compliance with the regulation. Organizations are expected to establish and maintain clear guidelines for registering and storing personal information if such guidelines do not already exist, or to update existing guidelines to reflect GDPR requirements.

Updating systems that classify information, data storage methods, and processing systems will likely be required to ensure that requirements for data mobility, deletion, or correction are not only possible but also effective. GDPR also requires specific data and logs to be retained, including data protection assessments, consent history, processing activity history, and any data breaches.

Information owners will need to review, update, and create guidelines that comply with GDPR and will likely need to increase their vigilance to ensure ongoing operations.

How does GDPR affect IT departments?

GDPR is all about your IT functionality. The regulation controls the flow of data through your organisation from the moment it is collected to the point at which a customer's data is erased, and all processing of that information in between.

Under GDPR, effective processes and systems must be in place to meet the requirements for data movement, deletion, and correction whenever necessary. Data protection principles must now be mandatory discussion topics with partners when evaluating future IT functions along with suppliers and resellers.

IT decision-makers must ensure that cloud providers meet the requirements set forth by GDPR, such as their ability to respond to requests for data to be deleted, changed, or moved, as well as making it clear where data centers are located and if personal data will be transferred outside regional borders.

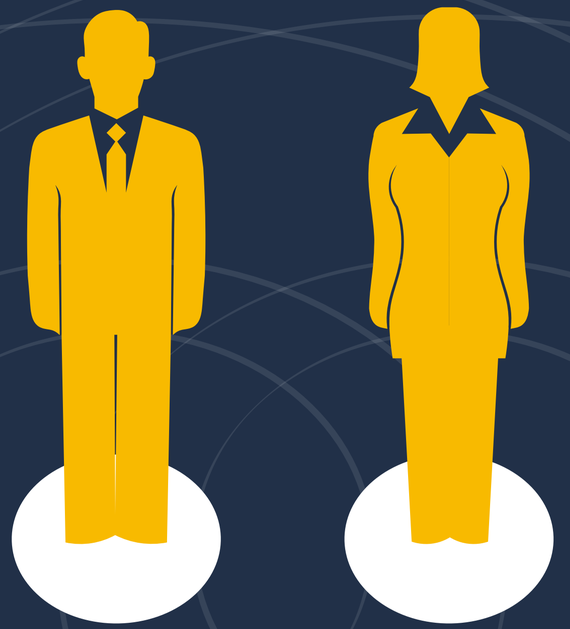
A serious challenge that IT organizations everywhere will face is the need to document all data processing processes and to have the information easily compiled when required. Finally, IT and IT security will play a major role in ensuring that any data breaches are reported and that processes for this are in place and followed.

How does GDPR affect HR departments?

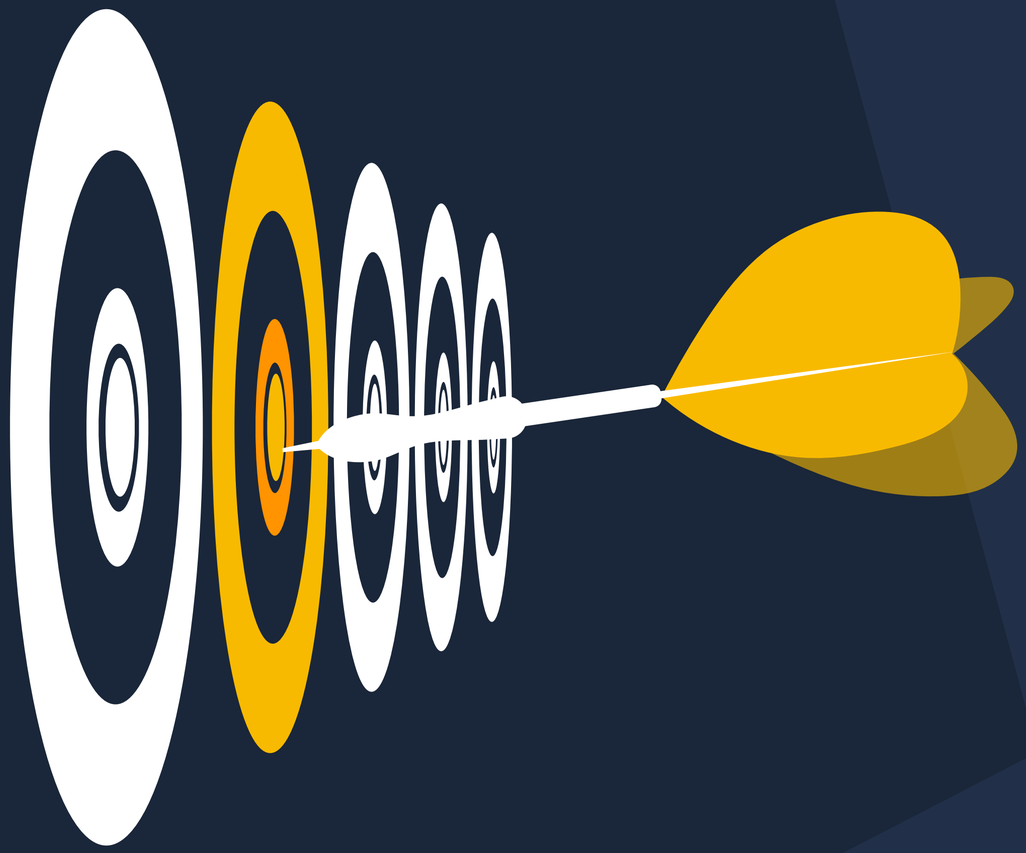
How does GDPR affect HR departments? One of the regulations in GDPR allows EU states to create additional laws specific to how personal information about employees is handled. This makes the handling of employee data even more complicated than the handling of customer data.

In the relationship between the employer and the employee, the employer can be seen as having the upper hand and consent from the employee is therefore not technically given of their own free will. Employers may not need to collect consent from employees under GDPR in the way that they must do for customers because employees have the ability to rely on legitimate business needs and interests, or as expressed in the regulation, "other legal grounds" such as personnel-related matters. However, consent must be given if the process extends beyond normal, legitimate personnel matters.

GDPR requires open consent for customer data, but an employee who wishes to continue working does not have the same power of freedom and openness about their personal data. Things like criminal background checks, drug tests, and other investigative data lead to even more new challenges, as does the requirement for mobility which may allow employees to demand that their data be transferred to a new employer after they have finished their employment. HR departments will need to seek legal advice to fully understand how to handle and comply with GDPR.



Comply with GDPR regulations



- Ensure an appropriate level of security, including confidentiality
- Protect personal data from unauthorized access.
- Secure data that is being transferred.
- Provide the right to delete personal information.
- Provide the right to correct inaccurate personal information.
- Provide the right to move personal information.
- Minimize the amount of data collected and processed.
- Follow strict records management.
- Ensure data protection is built into the design of processes as a default.

How Swedwise can help you with GDPR

Swedwise helps companies GDPR-proof their information and document management. With our solutions, customers experience simplified routines and processes.

The solution OpenText Content Suite provides, according to Gartner (Oct 2018), an industry-leading document solution to meet GDPR requirements for Swedish companies. A central storage and management of all company documents.

- Integrate content into business processes and manage it as a valuable asset for the company.
- Deliver and share material to give it its full value.
- Enhance the security and integrity of information throughout the process.
- Integrate seamless solutions with other strategic providers.
- Manage large volumes of information.

opentext | Partner Reseller Silver

SWEDWISE

OpenText Content Suite

DEVELOP, CONTROL AND SECURE YOUR INFORMATION.

Today's businesses and organizations handle an ever-increasing volume of information. This often happens in collaboration, both internally and externally, in different constellations and with different recipients. There is often a lack of time, the inbox is full, and it is difficult to determine if a person has the right version of a document.

EASY TO STORE, SEARCH AND SHARE

We have extensive experience using OpenText™ Content Suite, which is the cornerstone of the OpenText™ Enterprise Information Management (EIM) toolbox.

Content Suite is designed to manage information flows and is part of a comprehensive Enterprise Content Management (ECM) system. With Content Suite, security is enhanced by ensuring compliance and document standards.

opentext | Partner Reseller Silver

SWEDWISE

Contact us

Swedwise has many years of deep expertise in delivering OpenText solutions.

For more information and discussion, please contact David Hedström at +46 730 82 31 80.

About Swedwise

Swedwise is an IT company headquartered in Karlstad and with offices in Stockholm and Gothenburg. Swedwise works to develop and digitize their customers' processes.

We deliver both small and complex integration solutions that simplify the management of their customers' business data. Their customers are found in both the private and public sectors.

opentext™ | Partner Reseller Silver

SWEDWISE