antares

EU GDPR checklist

[5 important issues of the EU GDPR

In 2018, the new EU General Data Protection Regulation (EU GDPR) came into effect. This had far-reaching consequences for companies that process personal data. All related structures and processes had to be adapted in line with the stricter requirements.

In addition to new regulations on data protection, corporate liability has also been extended. In the event of a breach, companies may be subject to very high fines, which in extreme cases can be up to 4% of the annual turnover.

This checklist is intended to provide a summary of the key points of this EU GDPR.*

[Data protection management and information security

We help you to integrate a data protection management software - with antares RiMIS® ISMS and antares RiMIS® DPMS. We support you with the certification according to ISO 27001 and on the basis of IT baseline protection. The certification shows that your company has implemented appropriate measures to secure its IT systems.

By integrating the requirements from the EU GDPR into your information security management system, you show your customers and partners that all necessary data protection measures have been taken. An efficient DPMS not only supports you in identifying data protection and information security risks at an early stage and minimizing them sustainably, but also in safeguarding your corporate assets. Manage risks in a targeted manner and keep an eye on all countermeasures at all times!

* This checklist is for information purposes only and is expressly not to be understood as legal advice. We assume no liability for the accuracy and completeness of the information presented.

[Data protection principles

The processing of personal data is generally prohibited unless the data subject has consented or it is expressly permitted by law. Data protection principles must be observed at all times, as violating them can result in heavy fines. This is the case, for example, if consent has been given by the data subject, but superfluous data is collected and it thus contradicts the principle of data economy.

Legality

Any data processing that is not covered by the consent of the data subject requires legal permission. If there is no statutory permission, the data may not be processed.

Example: There is no general legal permission for sending newsletters. Consent must be obtained separately from each recipient in advance.

Data economy

Data processing must be appropriate to the purpose and limited to what is necessary.

Example: When an order is placed, no telephone number may be collected if it is not necessary for order processing.

Earmarking

Data processing may only be carried out for previously defined, explicit and legitimate purposes. In the event that the purpose is achieved, the data must be deleted immediately.

Example: In the registration form for a newsletter, the purpose (e.g. sending product recommendations or tips) must be specified.

Data safety

When processing data, appropriate technical and organizational measures must be taken to ensure protection against data misuse.

Example: Anyone working with sensitive data (e.g., medical records or passwords) must ensure that unauthorized persons do not have access to it.

Transparency

The data subject must be able to understand the data processing. This includes, for example, which data is collected in relation to their person.

Example: Anyone who collects data without the knowledge of a website visitor must at least explain this in the privacy policy.

[5 top issues of the EU GDPR

1. Scope of application of the EU GDPR (Art. 2-3)

The regulations of the EU GDPR apply to all companies that are established in an EU member state. It does not matter whether the data processing takes place inside or outside the EU.

Outside the EU, the regulations apply if the data processing is in connection with offering goods/services or tracking the user behavior of EU citizens.

Likewise, companies that outsource their data processing to countries outside the EU (e.g. rent servers in the USA) are affected.

What is personal data?
Personal data is any information relating to an identified or identifiable natural person.

This not only includes address data or the email address, but also explicitly online data, such as IP address, cookies or information about a person's device.

In addition, a person will also be „identifiable" in the future if his or her data has been anonymized but can be traced back when combined with other information.

2. Consent for processing and use of personal data (Art. 6)

In addition to the express permission of the data subject, processing of personal data is also permissible if legally prescribed grounds for permission apply.

The permissive facts according to the EU GDPR are:

- The consent of the data subject has been obtained;
- There is a legitimate interest in the data processing and the data subject's interests worthy of protection do not conflict with this;
- The data processing is necessary
  - for the performance of a contract;
  - for pre-contractual measures in response to a request;
  - for the fulfillment of a legal obligation of the responsible party.

What must be considered when obtaining a consent form?

Consent can be given in writing, electronically or verbally and must be proven by the collecting company in case of doubt. At this point, the data subject should also receive information about who processes his or her data and for what purpose, in addition to a reference to his or her right of revocation.

Further specifications may arise for special situations. For example, there should be no pre-clicked checkboxes when registering for a newsletter, since consent must be given explicitly and thus actively. In addition, the double opt-in procedure should be used for registrations.

3. Order processing (Art. 28, 32)

In the future, any type of commissioned processing will fall within the scope of the EU GDPR. A processor (=contractor) is defined as an entity that processes personal data on behalf of the controller (=client).

In doing so, the processors follow the instructions of their principals. However, they must guarantee that they comply with the requirements of the EU GDPR.

Example: Providers of cloud services must guarantee that suitable technical and organizational measures are in place to meet the requirements of data protection and data security. This includes, for example, certificates such as the ISO/IEC 27001 standard.

Further examples from practice:

- Payroll accounting in the cloud
- Using a CRM application in the cloud
- Sending newsletters via a cloud provider

Until now, the contractor was bound by the client's instructions and the client thus remained fully responsible. The new EU GDPR now also obliges the contractor, which means that the contractor is also liable in the event of a breach.

The following obligations apply to processors:

- Documentation requirements (procedure directory)
- Implementation of technical and organizational measures to ensure data security
- Appointment of a data protection officer
- Reporting obligations in the event of data breaches

These principles apply without restriction only if the client and contractor are located within the European Union (EU) or the European Economic Area (EEA) and the data processing takes place in this area. If one of the aforementioned entities is not based in the EU and the data leaves the area of the EU/EEA in the course of the order, then the regulations of the EU GDPR on third country transfers must be observed.

Our tip: Play it safe! Have the EU GDPR compliance of your service providers confirmed or use providers that are already certified.

How do you commission the processor?

Under the EU GDPR, it is no longer necessary to conclude a written contract for commissioned data processing. It is sufficient to include the mutual rights and obligations in the respective contract.

4. Directory of processing activities (Art. 30)

The EU GDPR stipulates that companies must maintain a directory of all processing activities.

There is a restriction for companies with less than 250 employees, which only do not have to keep a directory in the following cases:

- The processing carried out does not involve any risk to the rights and freedoms of the data subjects.
- The data processing is carried out only occasionally.
- No sensitive data is used.

A directory of processing activities should include the following information:

- Name, contact details, representative, data protection officer
- Purpose of processing
- Category description of data subjects and personal data
- Categories of recipients to whom the data have been or will be disclosed (also in other EU countries)
- Deadlines for the deletion of the categories of data
- Description of technical and organizational measures

Our tip: Appoint a team to create a procedure directory as soon as possible. In doing so, weak points in the data processing process of your own company can be uncovered and remedied.

5. Appointment of a data protection officer (Art. 37-39)

Companies with at least 10 employees that process personal data automatically must appoint a data protection officer. In companies with fewer than 9 employees, the management can assume the duties of the data protection officer.

The exception applies to extremely sensitive data such as a person's origin, health or political views. In these cases, even small companies must appoint a data protection officer.

What are the tasks of a data protection officer?

The core task is to regularly and systematically monitor the processing of personal data. The resulting recommendations should be implemented by the management.

This checklist serves as an aid in this regard*: www.lda.bayern.de/media/dsgvo_fragebogen.pdf.

Example of a directory of processing activities:

Nr.	Jointly responsible	Purpose	Affected groups	Data categories	Recipients	Transfer to third countries	Deletion deadline	Technical & organizational measures (TOM)
01		Marketing & sales	a. Active and former customers b. Interested parties c. Website visitors	To a & b: Contact and list data, product prospects, communication history, credit information To a: Master and contract data of the purchase history To c: Pseudonymized profiles according to § 15 TMG (German Telemedia Act)	Marketing, sales, extern service providers	Transmission of pseudonymized tracking data to US service providers	To a & b: In the event of revocation by the person concerned or 2 years after termination of the customer relationship To c: After 6 months by aggregation	

* This file (German) is provided by the Bavarian State Office for Data Protection Supervision.

[Introducing ourselves

What we do

We are a medium-sized, independent company specializing in professional software. Since our foundation in 1994 we have been developing and marketing strategic information systems.

Many years of expertise in the areas of analysis, planning and corporate management as well as governance, risk and compliance are guarantors for the development and expansion of the advanced antares software solutions.

Who we are

State-of-the-art technology, innovation and user-optimized solutions characterize our products. Passion, reliability and professionalism are the guidelines in dealing with our customers and partners. Competent and reliable support is our top priority. To ensure this, we work consistently on the further development of our established software solutions, provide professional project management and also offer comprehensive services - from training and webinars to coaching.

What we offer

We now count more than 300 companies of all industries and sizes among our customers, including well-known companies from the industrial, retail and service sectors. They all benefit from an experienced BI company with flat hierarchies, professional partnership and customer proximity.

What is our goal

Our goal is to provide our customers with a secure, user-friendly information base so that informed and confident decisions can be made.

antares

[Software for reliable decisions

[Software for reliable decisions

antares Informations-Systeme GmbH
Stuttgarter Str. 99
D-73312 Geislingen

Tel. +49 7331 3076-0

www.en.antares-is.de
info@antares-is.de