

Guideline

Data protection information pursuant to Art. 13 GDPR (data collection directly from the data subject) and pursuant to Art. 14 GDPR (data collection via third parties)

This template helps you to structure your privacy policy. When drafting data protection notices, go through the following information sheet and describe the relevant points as clearly as possible.

Important: This information sheet does not constitute legal advice. The contents do not claim to be complete and are not guaranteed. It merely serves as an introduction and provides an initial overview of data protection regulations.

Responsible body within the meaning of data protection law

The company providing information about the processing is indicated as the controller.

Example:

Mein Unternehmen GmbH

Beispielstr. 123

12345 Musterhausen

Tel: +00 12 34 56 78

E-mail: datenschutz@meinunternehmen.com

Contact details of our data protection officer *(if available)*

If your company has a data protection officer, please enter the contact details here.

Example:

Petra Datenschutz

Beispielstr. 123

12345 Musterhausen

Tel: +00 12 34 56 78 - 90

E-mail: datenschutzbeauftragte@meinunternehmen.com

Purposes and legal bases of processing

Describe here the purposes for which the data is collected and the legal basis on which the processing takes place.

Your data is collected in order to ... *[list purposes, with indents if necessary]*.

Your data will be processed on the basis of Art. 6 para. 1 letter *[insert the relevant legal basis here]* GDPR in conjunction with *[if necessary, state the specific legal basis]*.

Example:

Your data is collected in order to record your participation in our training course in our system. Your data will be processed on the basis of Art. 6 (1) (c) GDPR. The processing is necessary for the fulfilment of a contract.

Categories of personal data

At this point, list the categories of personal data that you process. You can answer this question in the form of bullet points or in free text.

Example 1:

We process the following categories of personal data about you:

- *Contact details*
- *Data on professional qualification*
- *Bank details*

Example 2:

We only process data that is related to your training. This may include general personal data (name, address, contact details, etc.), details of your professional qualifications and schooling, details of further professional training and any other data required to fulfil contractual, accounting and tax obligations.

Sources of the data

You should provide information about where you obtained the data of the data subject. As a rule, you will usually receive the data directly from the data subject themselves. If this is not the case, you should explain here where the data comes from.

Example:

We process personal data provided by you for the purpose of establishing and implementing the contractual relationship.

Recipients or categories of recipients of personal data

You must provide information about who has access to the data subject's data. These are usually different departments in the company or third parties - e.g. processors or other organisations or institutions to which you transfer the data.

Example:

We only pass on your personal data within our company to those areas and persons who need this data to fulfil contractual and legal obligations or to implement our legitimate interest.

If you use third-party providers or pass the data on to third parties, please also name them here.

Example:

Your personal data is processed on our behalf on the basis of order processing contracts in accordance with Art. 28 GDPR. In these cases, we ensure that the processing of personal data is carried out in accordance with the provisions of the GDPR. The categories of recipients in this case are providers of internet services and providers of customer management systems and software.

Your personal data will be transmitted to:

- Provider 1
- Service provider 2
- ...

Transfer of personal data to a third country

The transfer of personal data to a third country is a special case. This includes countries outside the EU or the EEA or international organisations. If you intend to transfer data to a third country, please inform the data subjects in this section.

Indicate to whom the data is transferred, in which country and what measures you have taken to protect the data. Important: The use of a service provider such as Google or Microsoft also constitutes a transfer to a third country (in this case the USA).

Also provide information on how the processing of this data is protected. Is there an adequacy decision by the EU Commission? If not (transfers pursuant to Art. 46/47 or Art. 49 (1) subparagraph 2), refer to appropriate safeguards and the possibility of obtaining a copy of the documents that ensure these safeguards.

Example 1:

A transfer to a third country is not intended.

Example 2:

We use services provided by Microsoft. Data processing is carried out on servers in the EU. However, a transfer of the data to the USA is not excluded. The European Commission has adopted an adequacy

decision for the USA through the "EU-U.S. Data Privacy Framework" in accordance with Art. 45 para. 1, para. 3 GDPR. Based on the new agreement, data can flow freely and securely between the EU and the participating US companies.

Duration of data storage

You must provide information about the duration of data storage.

Example 1 (short form):

Your data will be deleted no later than 3 years after completion of the last training course.

Example 2 (detailed wording, example for Germany):

We process your personal data as long as this is necessary for the establishment, execution or handling of the training relationship or for the exercise or fulfilment of the rights and obligations arising from the training contract.

In addition, we are subject to various retention and documentation obligations, including those arising from the German Commercial Code (HGB) and the German Fiscal Code (AO). The retention and documentation periods stipulated there are two to ten years.

Finally, the storage period is also based on the statutory limitation periods, which, for example, according to Sections 195 et seq. of the German Civil Code (BGB), are generally three years, but in certain cases can be up to thirty years.

Your rights

The rights arise from the GDPR. At this point, it is important to be able to implement the rights as the controller if a data subject contacts us with a request for information.

Example:

According to the EU General Data Protection Regulation, you have the following rights:

If your personal data is processed, you have the right to receive information about the personal data stored about you (Art. 15 GDPR).

If incorrect personal data is processed, you have the right to rectification (Art. 16 GDPR).

If the legal requirements are met, you can request the erasure or restriction of processing and object to processing (Art. 17, 18 and 21 GDPR).

If you have consented to the processing by means of a corresponding declaration, you can revoke your consent at any time for the future. The legality of the data processing carried out on the basis of the consent until the revocation is not affected by this.

If you have consented to the data processing or a contract for data processing exists and the data processing is carried out using automated procedures, you may have a right to data portability (Art. 20 GDPR).

Right of objection

Insofar as your personal data is processed in accordance with Art. 6 para. 1 lit. f GDPR to safeguard legitimate interests, you have the right to object to the processing of this data at any time in accordance with Art. 21 GDPR for reasons arising from your particular situation. We will then no longer process this personal data unless we can demonstrate compelling legitimate grounds for the processing. These must outweigh your interests, rights and freedoms, or the processing must serve the assertion, exercise or defence of legal claims.

To protect your rights, you can contact us using the contact details provided.

If you make use of your above-mentioned rights, we will check whether the legal requirements for this are met.

To exercise your rights, please contact the company data protection officer (if available, otherwise name a responsible contact person).

Necessity of the provision of personal data

At this point, you should briefly explain the consequences of not providing the data for the purpose described.

Example:

The provision of your personal data for the proper implementation of a training programme is voluntary. However, we can only provide an effective training programme if you provide the personal data required for the acceptance and implementation of the training programme when concluding the training contract.

Automated decision-making (if in use)

If automated decision-making or profiling is used, the particular scope of the use and the intended effects as well as the logic or algorithm used must be stated.

Example: There

is no automated decision in individual cases within the meaning of Art. 22 GDPR.