



Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDPR Good Practices

The representative in the European Union
according to Art. 27 GDPR

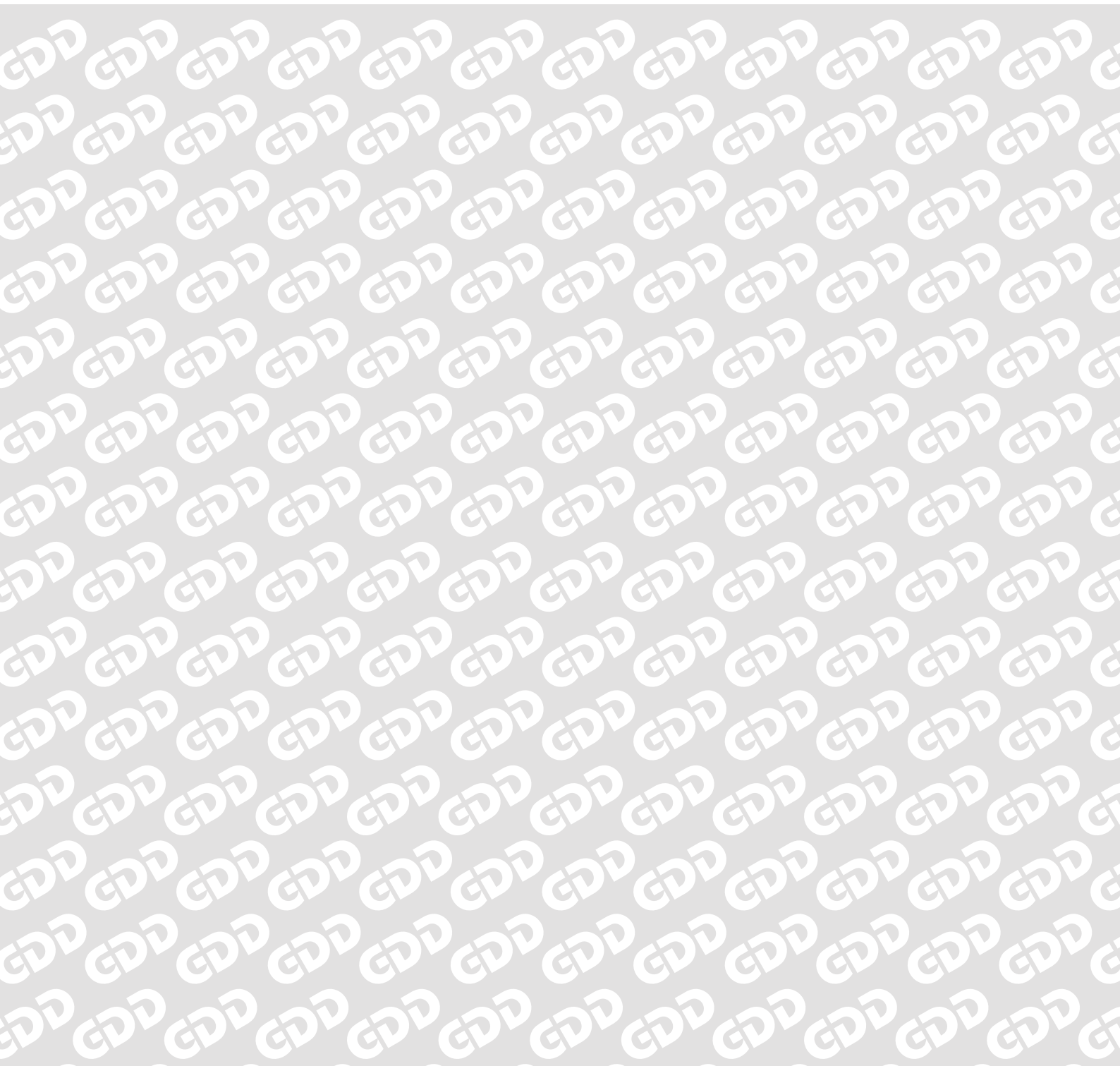


TABLE OF CONTENTS

1. Purpose	4
2. Duty to designate	4
3. Exemptions from the obligation to designate	4
3.1. Exemption according to Art. 27 para. 2 GDPR: Occasional, not extensive processing of sensitive data without risk	4
3.1.1. „Occasionally“	4
3.1.2. „Non-extensive processing“ of sensitive data	4
3.1.3. „No risk“	5
3.2. Exemption according to Art. 27 para. 2 letter b GDPR: Authorities and public bodies	5
4. The concept of the representative	5
4.1. Definition	5
4.2. Legal status	5
4.3. Designation	6
4.4. Publicity of the designation	6
4.5. Legal mandate	6
5. Establishment	7
6. Tasks and duties	7
7. Liability	7
8. Conclusion	8

The representative in the European Union according to Art. 27 GDPR

Controllers outside the European Union (EU)/European Economic Area (EEA) are bound by the provisions of the General Data Protection Regulation (GDPR) if they offer goods or services to data subjects within the EU (Art. 3 para. 2 letter a GDPR), monitor the behaviour of data subjects within the EU (Art. 3 para. 2 letter b GDPR) or if the law of a Member State is applicable due to international law (Art. 3 para. 3 GDPR). In the cases of Art. 3 para. 2 of the GDPR, the controller or the processor must always appoint a representative in the EU in writing pursuant to Art. 27 para. 1 GDPR.

In the following, these Guidelines are dedicated to the legal framework of the designation and is intended to serve as guidance for data controllers, processors and service providers.

1. Purpose

The purpose of Art. 3 GDPR is to provide both the data subjects and the supervisory authorities with a contact point. Art. 3 para. 2 GDPR extends the territorial scope of application for certain cases to third countries in which the supervisory authorities of the Member States have no competence and in which there would be a risk that the obligations of the controllers and processors located there would come to nothing. Thus, the representative is an important instrument for the effectiveness of law enforcement as well as for the protection of data subjects' rights under Art. 12 et seq. GDPR.

2. Duty to designate

Pursuant to Art. 27 para. 1 GDPR, there is an obligation to designate for all data controllers or processors who are subject to Art. 3 para. 2 GDPR. I.e.,

- >> there is no establishment within the EU/EEA,
- >> personal data of persons within the EU are processed,
- >> goods and/or services are offered in the EU/EEA or
- >> the behaviour of data subjects within the EU/EEA is monitored.

3. Exemptions from the obligation to designate

However, Art. 27 para. 2 GDPR also provides for certain exceptions to the basic obligation to designate. Accordingly, the legal obligation does not apply if only occasional processing of no or only a few sensitive data takes place (Art. 27 para. 2 letter a GDPR) or in the case of data processing by authorities and public bodies.

3.1. Exemption according to Art. 27 para. 2 GDPR: Occasional, not extensive processing of sensitive data without risk

The exception contains several indeterminate legal terms, which must first be explained in more detail. In addition, the associated requirements for the exception must be fulfilled cumulatively.

3.1.1. „Occasionally“

The term „occasional“ is not defined in terms of size or frequency; rather, the assessment must always be made on a case-by-case basis. In any case, the size of the company and the relationship of this specific processing activity to the main data processing activities must be taken into account, so that the requirement of „occasionally“ can rather be equated with „now and then“ or „from time to time“ (compared to the core activity). Similarly, „occasionally“ excludes regularity, which further narrows down the use cases for this exemption to all non-scheduled processing activities.

3.1.2. „Non-extensive processing“ of sensitive data

The exception covers personal data under Art. 9 para. 1 GDPR, which regulates the processing of data relating to racial and ethnic origin, political opinion, religious or philosophical beliefs or trade union membership, etc., and Art. 10 of the GDPR, which regulates the processing of data relating to criminal convictions and offences. What remains undefined here is how the requirement „not extensive“ is to be understood. Here the legislator has rather a qualitative approach. This means that the assessment of the scope of the sensitive data processed depends on the amount/number of personal data processed and the intensity of the data analysis.

3.1.3. „No risk“

As a final condition for the exception, the processing must not lead to a risk for the data subject. However, this is a utopian requirement, since the processing of personal data implies an inherent risk for the data subject. It must therefore be assumed at this point that at least a low risk is justifiable. Recital 75 of the GDPR provides information on risks to the rights and freedoms of the data subject that must be included in the assessment:

- >> Physical, material or immaterial damage;
- >> Discrimination;
- >> Identity theft or fraud;
- >> Financial loss;
- >> Defamation of character;
- >> Loss of confidentiality of personal data subject to professional secrecy;
- >> Removal of pseudonymisation;
- >> Other significant economic or social disadvantages.

The criteria must be checked by the controller or processor located in the third country during the risk analysis.

3.2. Exemption according to Art. 27 para. 2 letter b GDPR: Authorities and public bodies

If authorities or public bodies located outside the EEA carry out the data processing, they also do not fall within the scope of Art. 27 GDPR and do not have to appoint a representative. This also applies to private companies that perform tasks in the public interest or process data on behalf of public authorities.

4. The concept of the representative

4.1. Definition

The term representative is legally defined in Art. 4 para. 17 GDPR as a natural or legal person established in the EU who has been appointed in writing by the controller or processor pursuant to Art. 27 GDPR and is to represent the controller and the processor with regard to the obligations in the GDPR.

4.2. Legal status

Although the European legislator chose the term „representative“, a representative according to Art. 27 GDPR is legally rather to be classified between the messenger and the representative in the sense of the German Civil Code (BGB). An equation with the representative from German civil law is out of the question, since not all elements of Sect. 164 para. 1 BGB are fulfilled. The representative according to Art. 27 GDPR can be limited in his power of representation by the controller, because he/she only acts according to the conditions of his/her mandate and is therefore not free in his/her actions. In his function, the representative is to act as a contact point for data subjects and authorities. However, any legal consequences for data protection violations, such as fines or claims for damages, are still only directed at the relevant controller or processor. In its function as a contact point, the question arises, especially with regard to the time limit according to the GDPR (e.g. Art. 12 para. 3 sentence 1 GDPR for requests to assert the rights of data subjects according to Art. 15 - 22 GDPR), as of when a data subject request belongs to the sphere of activity of the controller or processor. Requests from a data subject or a supervisory authority are considered to have been received by the controller or processor as soon as they have been received by the representative pursuant to Art. 27 GDPR. The representative has the authority to receive declarations on behalf of the controller/processor and is

regularly given the authority to make declarations on behalf of the controller/processor as part of the appointment. The representative thus assumes the position of „a receiving agent and a messenger of declarations“.

4.3. Designation

With regard to the appointment, different terms are used within the articles and recitals of the GDPR. Thus, Art. 4 para. 17 GDPR speaks of the **written appointment**, Art. 27 para. 1 GDPR of the **designation** and Recital 80 GDPR of the **explicit appointment**. Whether the title is „appointment“ or „designation“ may not be decisive. What is relevant is that precise details of the person (legal or natural), address and function as Union representative are made in writing. Recital 80 sentence 3 GDPR additionally provides for a **written mandate of the representative (see section 4.5)**. The requirement for this to be in writing also raises the question of whether the written form requirement is thereby fulfilled in the sense of Sect. 126 BGB. This would have the consequence that a handwritten signature is required in the document. However, since the GDPR is a legal provision under European law and the provisions of the GDPR are to be interpreted in the sense of European Union law, the strict requirement of Sect. 126 BGB will probably not have to be followed and the text form pursuant to Sect. 126b BGB will be sufficient.

4.4. Publicity of the designation

With regard to publicity, the question arises in this context as to whether there is an active obligation to notify the supervisory authorities or data subjects of the designation/appointment of the representative. However, this can neither be inferred from Article 27 GDPR nor from the recitals. Accordingly, the GDPR does not contain a „self-triggering notification obligation“ regarding the appointment of the representative.

The fact that there is a representative pursuant to Art. 27 of GDPR must be brought to the atten-

tion to data subjects according to the information obligations pursuant to Art. 13, 14 GDPR. Here, the legislator stipulates that the controller must also provide the contact details of his representative in addition to his own contact details.

4.5. Legal mandate

The contractual relationship between the controller/processor and the representative must be considered separately from the legal act of designation/appointment. It is similar to the appointment of the data protection officer (Art. 37 GDPR) and is usually a service contract. In terms of content, the following aspects should be considered:

- >> Relationship between designation/appointment and mandate
- >> Contract period
- >> Period and form of notice
- >> Content of the mandate, e.g.:
 - > Definition of the legal provisions regarding the tasks of the representative (e.g. accessibility for supervisory authorities and data subjects)
 - > Organizational instructions with regard to inquiry management (supervisory authority/data subjects)
 - > Processing and notification deadlines in relation to the controller/processor and supervisory authorities/data subjects
 - > Possible further obligations outside of the legally required
- >> Costs/Remuneration
- >> Liability
- >> Control rights (in writing/in person) of the controller/processor
- >> Obligation to disclose documents to the controller/processor
- >> Obligation to confidentiality, possibly also in relation to other sensitive information/trade secrets (NDA)

5. Establishment

The GDPR stipulates in Art. 27 para. 3 that a representative must be established in the Union. Despite this wording, it is also permissible for the representative to have an establishment in the EEA states (Norway, Iceland, Liechtenstein). According to paragraph 1 of the preamble of Decision No 154/2018 of the EEA Joint Committee and its Art. 1, the GDPR is to be incorporated into the EEA Agreement and applies to the purposes of the Agreement.

It is by no means necessary to appoint a representative in each Member State; rather, Art. 27 para. 3 GDPR literally refers to a representative.

What is not regulated, however, is what is to be understood by the term „establishment“.

Recital 22 of the GDPR states that an establishment requires the „actual exercise of an activity by a fixed establishment“. The Data Protection Commissioner of Hamburg (HmbBfDI) commented on this in his 27th Activity Report: A „minimal infrastructure“ is sufficient, in the case described in the Activity Report, a postal address in a shared office, as long as „communication functions smoothly and meetings can be held [within this establishment] if necessary“. This at least contradicts the view that a mere letterbox is sufficient. However, if one follows the view of the HmbBfDI, this also does not require a permanent presence of employees, as long as the communication channels are guaranteed.

6. Tasks and duties

According to the definition in Art. 4 para. 17 GDPR, the representative's task is to represent the controller or the processor with regard to their obligations under the GDPR. According to Art. 27 para. 4 GDPR, the representative must also act as a **contact person and point of contact** for the supervisory authorities and the data subjects. This can be done in addition to or in place of the representative. However, Art. 27 para. 5 GDPR clarifies that the

performance of the duties does not change the legal obligation of the controller/processor.

When communicating with data subjects and supervisory authorities, it is important that

- >> inquiries will be answered in the possible way,
- >> the deadlines within the GDPR are met through internal organization and
- >> communication is possible in the respective national language.

Apart from Art. 4 para. 17 and Art. 27 GDPR, there are other obligations within the GDPR. According to Art. 30 para. 1 GDPR, the representative is obliged to keep a **register of processing activities** for all processing activities that fall within the scope of his/her tasks. **Art. 31 GDPR** also obliges the representative to **cooperate with the supervisory authorities** in the performance of their duties. In accordance with **Art. 58 para. 1 letter a GDPR**, the representative must be able to provide all necessary information within the scope of the supervisory authority's **power of investigation**.

7. Liability

Possible liability of the representative presupposes that the infringements must be the representative's own and not attributable to the controller/processor. The representative is not liable for derived infringements. Thus, according to Art. 83 para. 4 letter a GDPR, the representative cannot be held liable for breaches of the obligations under Art. 27, 30, 31 GDPR, because these provisions explicitly address the controller or processor. A liability of the representative according to Art. 83 para. 4 letter a GDPR would violate the legal concept of prohibition of analogy.

If a representative does not provide the required information pursuant to Art. 58 para. 1 letter a GDPR, a fine may be imposed on him/her personally

of € 20 million or, if higher, 4% of the previous year's global group turnover pursuant to Art. 83 para. 5 letter e GDPR.

8. Conclusion

The requirements for the representative in the Union according to Art. 27 GDPR are not very high. They are also not linked to any requirements in terms of data protection expertise, as provided for in the GDPR for the data protection officer. In practice, however, it will still prove advantageous if a representative has at least solid knowledge in the area of data protection law, since he/she must, for example, also maintain his/her own directory for processing activities in accordance with Art. 30 GDPR.

It is important that controllers/processors make clear contractual arrangements within the internal relationship with the representative in order to ensure smooth communication with the representative as well as between the representative and the supervisory authority or the data subjects. It must be ensured that enquiries are passed on immediately to the controller/processor so that they can be answered in due time or that the representative is entrusted with answering them. The controller/processor remains responsible for the actions of the representative, so that if a deadline based on the GDPR is exceeded, the controller/processor cannot invoke that the deadline was not met due to misconduct or negligence on the part of the representative.



Gesellschaft für Datenschutz
und Datensicherheit e.V.

Editor:

Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)

Heinrich-Böll-Ring 10

53119 Bonn

Tel.: +49 2 28 96 96 75 00

Fax: +49 2 28 96 96 75 25

www.gdd.de

info@gdd.de

Contact person: Dr. Tobias Jacquemain, LL.M.

Layout: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Status:

version 1.0 - december 2021