Regulation (EU) 2016/679 - General Data Protection Regulation

Guide

Compiled by Dr Matthias Schmidl (revised by

Marek Gerhalter, LL.M.) Status: September

2022

Contents

Foreword

This guide summarises information on the General Data Protection Regulation (GDPR), which is intended to make it easier to work with the GDPR and provide assistance on specific issues.

This **is not exhaustive information**. The guide cannot replace advice from specialised institutions or legal advice.

The guidelines **do not constitute binding information** that could bind the data protection authority in any proceedings, but rather reflect the level of knowledge and experience of the employees at the present time.

The guidelines are regularly evaluated and updated in order to incorporate new developments (especially at European level).

The following innovations in particular have been included in this update:

- New guidelines and recommendations of the European Data Protection Board
- New case law of the European Court of Justice and recent references for a preliminary ruling

Introduction

The GDPR (full title: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*) was published on 04.05.2016 in OJ No. L119 p. 1, entered into force on the 20th day after its publication and has been in force since 25 May 2018.

It repeals the Data Protection Directive 95/46/EC (GDPR) and has formed the backbone of general data protection in the EU since 25 May 2018.

The regulation is directly applicable and does not require any further national implementation.

The GDPR contains numerous "opening clauses" that oblige and/or authorise national legislators to regulate certain matters in more detail by law.

There is therefore still a national data protection law in Austria in addition to the GDPR (see point 11 of the guide for more details).

The objectives of the GDPR are

- standardised legal protection for all affected parties in the EU
- standardised rules for data processing within the EU
- Ensuring strong and uniform enforcement

The data protection terminology is new in certain areas.

For example, the previous client becomes the "responsible party" and the service provider the "responsible party".
"Processor" (although the terms are not always congruent). Some key

aspects are highlighted below.

1) Structure of the GDPR

The GDPR comprises 173 recitals and 99 articles. It is

divided into 11 chapters:

- Chapter I: General provisions (Art. 1 to 4)
- Chapter II: Principles (Art. 5 to 11)
- Chapter III: Rights of the data subject (Art. 12 to 23)
- Chapter IV: Controller and processor (Art. 24 to 43)
- Chapter V: Transfers of personal data to third countries or international organisations (Art. 44 to 50)
- Chapter VI: Independent supervisory authorities (Art. 51 to 59)
- Chapter VII: Co-operation and coherence (Art. 60 to 76)
- Chapter VIII: Legal remedies, liability and sanctions (Art. 77 to 84)
- Chapter IX: Provisions for specific processing situations (Art. 85 to 91)
- Chapter X: Delegated acts and implementing acts (Art. 92 to 93)
- Chapter XI: Final provisions (Art. 94 to 99)

2) Chapter I

Material scope of application (Art. 2):

The GDPR applies to the **fully or partially automated processing of personal data** as well as to the **non-automated processing of personal data** that is stored or is to be stored in a **file system**[1] .

The GDPR **does not** apply to the following areas:

- Activities that do not fall within the scope of Union law
- Activities within the framework of the Common Foreign and Security Policy
- Data use in the context of exclusively personal or family activities
- Activities of competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[2]

Territorial scope of application (Art. 3) :[3]

As with the Data Protection Directive 95/46/EC (GDPR), the GDPR is primarily linked to the use of data in the context of an **establishment of** a controller or a

[1] On the concept of a "file system", see also the judgement of the ECJ of 10 July 2018, C-25/17.
[2] The GDPR-PJ applies to these areas; the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Directive-Police Justice - GDPR-PJ) was published in Official Journal L119 p. 89 on 4 May 2016 and entered into force on the day following its publication. The national implementation of the GDPR-PJ is essentially carried out through the provisions of the 3rd main section of the DPA.
[3] See EDPB Guidelines 3/2018 on the spatial scope of application, available in German at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_en.pdf.

Processor to[4] ; if this **establishment is in the Union territory**, the GDPR is applicable.

According to Art. 3 para. 2, the GDPR also applies if the data processing is carried out by a controller or processor **not established in the territory of the Union** and the data processing is related to this

- offer goods or services to data subjects in the Union (regardless of payment) or
- observe the behaviour of data subjects insofar as their behaviour takes place in the Union.

The GDPR also applies if the controller or processor is not established in the territory of the Union, but in a place that is subject to the law of a Member State under international law.

Definitions (Art. 4):

The definitions of the GDPR (Art. 4) often adopt the definitions of the GDPR, but also contain new terms, such as

- Profiling (Art. 4 Z 4)
- Pseudonymisation (Art. 4 No. 5)
- Breach of the protection of personal data (Art. 4 no. 12; data breach)
- genetic and biometric data as well as health data (Art. 4 no. 13 to 15)
- Head office (Art. 4 No. 16)
- Representatives, companies and group of companies (Art. 4 No. 17 to 19)
- Supervisory authority and supervisory authority concerned (Art. 4 (21) and (22))
- Cross-border processing (Art. 4 no. 23)
- Authoritative and justified objection (Art. 4 no. 24)

[4] On the concept of establishment, see the judgements of the ECJ of 1 October 2015, C-230/14, Weltimmo, and of 28 July 2016, C-191/15, VKI; on the concept of "in the context of the activities of an establishment", see the judgement of the ECJ of 13 May 2014, C-131/12, Google.

- Information society service (Art. 4 no. 25)
- international organisation (Art. 4 no. 26)

3) Chapter II

The principles of data processing are largely identical to those of the GDPR.

The content of Art. 6 - Lawfulness of processing - is linked to Art. 7 of the GDPR. Accordingly, the concept remains that the processing of data is unauthorised unless there is a justification (prohibition with exceptions).

Building on the case law of the ECJ on Art. 7 of the DSRL[5] , it can be assumed that Art. 6 also contains an **exhaustive list of permissible interferences** and that the Member States cannot standardise any additional grounds for interference.

The purpose limitation principle according to Art. 5 para. 1 lit. b is modified by Art. 6 para. 4. Accordingly, the use of data for purposes other than those for which they were originally collected is also permitted under strict conditions.[6]

Art. 7 sets out the conditions for consent[7][8] (and in more detail than the GDPR did previously)[9] , Art. 8 makes explicit reference to the conditions for a child's consent in relation to information society services; this takes account of the fact of progressive digitalisation and the use of social networks, including by minors.

[5] See most recently the judgement of 19 October 2016, C-582/14, Breyer.
[6] This approach was criticised by Austria during the legislative process; see *Fercher/Riedl*, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht in *Knyrim* (ed.), Datenschutz-Grundverordnung [2016] p. 22 ff; see also *Kotschy*, Zweckbindungsprinzip und zulässige Weiterverarbeitung, Debattenbeitrag zur Datenschutz- Grundverordnung (Version 23.06.2016), available at http://bim.lbg.ac.at/de/themen/datenschutz- grundverordnung.
[7] For more information, see EDPB Guidelines 5/2020 on consent, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
[8] See also the decision of the data protection authority of 31 July 2018, GZ DSB-D213.642/0002-DSB/2018.
[9] See *Dürager/Kotschy*, Neuerungen zur Zustimmung (Einwilligung) nach der DS-GVO, Debattenbeitrag zur Datenschutz-Grundverordnung (Version 02.12.2016), and *Dürager/Kotschy*, Neuerungen zur Zustimmung: Besteht nach der DS-GVO ein generelles Koppelungsverbot?, Debattenbeitrag zur Datenschutz-Grundverordnung (Version 09.01.2017), both available at http://bim.lbg.ac.at/de/themen/datenschutz-grundverordnung.

Like Art. 8 of the GDPR, Art. 9 contains the requirements for the use of sensitive data (= special categories of personal data). It should be noted that information that indirectly allows conclusions to be drawn about the characteristics of a data subject listed in Art. 9 GDPR also qualifies as "sensitive" personal data.[10]

Art. 10 specifies the conditions under which personal data relating to criminal convictions and offences may be processed.[11] The ECJ has ruled on the term "criminal offence", which is to be interpreted autonomously under EU law, that this not only includes criminal offences in the sense of criminal law (i.e. offences that are classified as "criminal" under national law), but also administrative offences (such as violations of road traffic regulations) under certain conditions.[12] The assessment must be made on a case-by-case basis using the criteria established by the ECJ. If data relating to an administrative offence qualifies as data within the meaning of Art. Art. 10 GDPR and is processed by the competent authorities for the investigation and prosecution of criminal offences, the scope of application of the GDPR-PJ or the 3rd main section of the DPA would apply.

Art. 11 finally standardises the not insignificant fact that data must not be retained merely in order to be able to identify a person (e.g. in order to be able to comply with a request for information).

---

[10] Cf. the judgment of the ECJ of 1 August 2022, C-184/20, para. 123 et seq.

11 By definition, this "criminal data" is not considered sensitive data. However, they were already subject to special protection in Austria; cf. section 8 para. 4 DSG 2000 and the case law of the Administrative Court (decision of 22 October 2012, no. 2009/03/0162).

[12] Judgment of the ECJ of 22 June 2021, C-439/19, para. 87 et seq.

4) Chapter III

Chapter III regulates the **data protection** rights to which a data subject is entitled.

The rights of data subjects, i.e. the rights that data subjects can derive from the GDPR or the DPA, are as follows

- from the constitutional provision of § 1 DSG or
- from Art. 12 to 22 GDPR

As far as the GDPR is concerned**, Art. 12 GDPR** is to be used as a **horizontal provision** for the exercise of all data subject rights because it specifies the modalities of exercise.

Accordingly, the following applies:

The controller must facilitate the exercise of the data subject's rights as far as possible by

- provides information and messages in easy-to-understand language (especially for children);
- information and notifications in writing, if necessary electronically;
- also p r o v i d e s information and communications orally, provided that the identity of the person concerned has been proven in another way.

Measures taken in response to a request for access, rectification or erasure, an objection or a request for restriction of processing or data portability must be communicated to the data subject without undue delay and in any case **within one month**. This period may be **extended by a further two months** in justified cases; the data subject must be informed of the extension of the deadline by the controller within the first month, stating the reasons. If an application is submitted electronically by a data subject, the data subject shall be informed electronically wherever possible, unless the data subject indicates otherwise.

If the request of a data subject is not granted, the data subject must be informed of this in writing **within one month**, stating the relevant reasons. They must be informed of the possibility of lodging a complaint with the supervisory authority.

The exercise of data subject rights is **free of charge** for the data subject. In the case of **manifestly unfounded** or - particularly in the case of frequent repetition - **excessive requests** by a data subject, the controller may

- either **charge** an **appropriate fee** (taking into account the administrative costs for the information or notification or the implementation of the requested measure) or
- **refuse** to **take action** on the basis of the application.[13]

The burden of proof for the existence of these reasons lies with the person responsible.[14]

If the controller has **reasonable doubts about the identity of** the data subject, it may request additional information from the data subject to confirm their identity. The identity of the person requesting the information is usually verified in the form of a copy of an official photo ID[15] . However, proof in the form of a qualified electronic signature is also possible.[16] If a request for information is submitted by a lawyer on behalf of a client, the client's power of attorney must be attached to the request for information. This does not apply if a lawyer intervenes vis-à-vis domestic authorities and courts, because in this case the mere reference to the power of attorney granted is sufficient (Section 8 RAO).[17]

---

[13] See the decision of the data protection authority of 6 July 2018, GZ DSB-D123.051/0002-DSB/2018 (not legally binding) or the decision of the Federal Administrative Court of 2 March 2020, W214 2224106-1.

[14] Art. 57 para. 4 GDPR provides for a similar regulation for the complaints procedure before the data protection authority; see, for example, the findings of the Federal Administrative Court of 29 April 2020, W274 2228071-1 and 3 November 2020, W214 2233563-1

[15] The Administrative Court has ruled that proof of identity can be provided in the form of a public document. However, according to the case law of the VwGH, the submission of a confirmation of registration, for example, is not sufficient; decision of 04.07.2016, Zl. Ra 2016/04/0014.

[16] Art. 3 no. 12 eIDAS Regulation (Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ No L 257 of 28.08.2014 p. 73, as corrected by OJ No L 257 of 29.01.2015 p. 19); see also the decision of the Federal Administrative Court of 27.05.2020, GZ W214 2228346-1. [17] See again the decision of the Administrative Court of 04.07.2016.

However, if there is sufficient evidence to confirm the identity of the person requesting information beyond doubt, the person responsible may not request any further proof of identity (e.g. photo ID).[18]

Articles 13 and 14 - like Articles 10 and 11 of the GDPR - set out the **information obligations** of[19] towards data subjects. Accordingly, data subjects must be informed by whom, on what legal basis and for what purpose their data is processed and to whom it is transmitted. The ECJ attaches great importance to these information obligations because they create the conditions for data subjects to be able to exercise their rights (access, rectification, erasure, objection).[20]

In addition to the existing rights of **access** (Art. 15), **rectification** (Art. 16) and **erasure** (Art. 17; extended to the "right to be forgotten"), new rights have been introduced.

For example, Art. 18 provides for the **right to restriction of processing**, according to which a data subject can request the controller to restrict processing if, for example, the accuracy of the data is disputed.

Art. 20 grants a data subject the **right to data portability**[21] . This is intended to ensure that the personal data provided by a data subject and stored by a (private) provider in a specific technical environment can be transferred to a new technical environment without technical barriers for the data subject in the event of a change of provider in certain cases[22] .

---

[18] See to this the decision of the data protection authority dated 31/07/2019, GZ DSB-D123.901/0002-DSB/2019.
[19] See in more detail the Art. 29 Working Party's Guidelines on Transparency, WP 260, available in German at https://www.dsb.gv.at/dam/jcr:17cb6862-7bc0-4039-8c47-97bc09602214/Leitlinien%20f%C3%BCr%20Transparenz%20gem%C3%A4%C3%9F%20der%20Verordnung%202016-679.pdf. These guidelines were by the EDSA explicitly adopted: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.
[20] Cf. the judgement of the ECJ of 1 October 2015, C-201/14, Smaranda Bara et al.
[21] Cf. WP 242 rev. 01, Guideline of the Article 29 Working Party of 13 December 2016 on data portability, available at https://www.dsb.gv.at/dam/jcr:01ff1101-f5bf-494b-a7d2-64392db10b78/Guidelines%20on%20the%20right%20to%20data%C3%BCportability,%20pdf.pdf. These guidelines were by the EDSA explicitly adopted: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.
[22] Among other things, it is essential that the data processing is based on consent or is carried out to fulfil a contract and (cumulatively) is carried out using automated procedures.

The right to **object** (Art. 21)[23] differs significantly from the right to object under § 28 DSG 2000, and has special effect against direct advertising (Art. 21 para. 3).

Also as a horizontal provision, Art. 23 GDPR regulates the conditions under which data subjects' rights can be restricted.[24]

This may be necessary for reasons

a) national security;

b) national defence;

c) public safety;

d) the prevention, investigation, detection or prosecution of criminal offences or the execution of sentences, including the protection against and the prevention of threats to public security;

e) the protection of other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, such as monetary, budgetary, taxation, public health or social security;

f) the protection of the independence of the judiciary and the protection of judicial proceedings;

g) the prevention, detection, investigation and prosecution of violations of the professional rules of regulated professions;

h) the control, monitoring and regulatory functions that are permanently or temporarily associated with the exercise of official authority;

i) the protection of the data subject or the rights and freedoms of others;

j) the enforcement of civil law claims.

---

[23] The right to object also applies to the use of data by public authorities; cf. the judgement of the ECJ of 9 March 2017, C-398/15, Manni.

[24] Cf. EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 1.0 of 13 October 2021, available in English at https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf.

In Austria, this has been utilised above all in the material data protection adaptation laws[25] .

However, according to the case law of the ECJ, such restrictions are subject to review by the ECJ insofar as restrictions that Member States may impose also fall within the scope of Union law.[26]

[25] See in particular the Material Data Protection Amendment Act 2018, Federal Law Gazette I No. 32/2018, and the 2nd Material Data Protection Amendment Act 2018, Federal Law Gazette I No. 37/2018, where use was made of restrictions within the meaning of Art. 23 GDPR.
[26] Cf. the judgement of 21 December 2016, C-203/15, Tele 2 Sverige AB, and C-698/15, Watson.

5) Chapter IV

The GDPR places greater obligations on controllers and processors than the GDPR and the DPA 2000.

Art. 27 obliges controllers and processors that are **not established in the territory of the Union** to appoint a **representative** in a Member State. The representative is the point of contact for data subjects and supervisory authorities in addition to or instead of the controller/processor.[27]

The DPA notification procedure and the DPA itself no longer exist (**cancellation of the DPA notification obligation**). Instead, Art. 30 obliges controllers and processors to keep a **record of processing activities**[28] , which must be submitted to the supervisory authority upon request. This obligation does not apply to companies or organisations with fewer than 250 employees, unless

- the processing they carry out poses a risk to the rights and freedoms of data subjects,
- the processing is not only occasional or
- special categories of data are processed in accordance with Art. 9 (1) (sensitive data) or the processing of personal data relating to criminal convictions and offences within the meaning of Art. 10.

In addition, data controllers are obliged to carry out a **data protection impact assessment**[29] before commissioning a new data processing system that is likely to result in a high risk to the rights and freedoms of natural persons and, if necessary, to liaise with the supervisory authority as part of a data protection plan.

---

[27] On the representative's responsibility, see again EDPB Guidelines 3/2018 on the territorial scope of application, available in German at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_en.pdf, p. 19 et seq.

[28] See in more detail *Horn*, Possible extensions of the processing directory pursuant to Art. 30 GDPR to a comprehensive compliance tool, JusIT 5/2017 p. 183 et seq.

[29] Cf. WP 248 rev.01, Guidelines of the Art. 29 Working Party of 4 April 2017 on data protection impact assessments, available at https://www.dsb.gv.at/dam/jcr:ba295358-cf65-41a6-911d-a88cae94ba20/Guidelines%20on%20data-protection-impact-assessment-wp248-rev-01_en.pdf.

consultation procedure (Art. 35 and 36). The obligation to carry out a data protection impact assessment also applies under certain conditions to the legislative procedure itself, whereby the question of the extent to which the omission of a mandatory risk impact assessment affects the effectiveness of a standard is currently the subject of a preliminary ruling procedure before the ECJ.[30]

Data controllers are obliged to **report personal data breaches to the supervisory authority** (Art. 33) and, where applicable, to **notify data subjects** of the breach (Art. 34).[31] Operators of public communications services are subject to the same reporting obligations in accordance with Section 164 TKG 2021.[32]

Also new is the mandatory **appointment of a data protection officer** in certain areas (Art. 37 to 39)[33] , who carries out his or her duties as data protection officer without being bound by instructions and reports directly to the highest management level. A data protection officer iSd. GDPR is particularly protected and may not be dismissed or penalised for fulfilling his or her duties. To this end, Member States may also provide for stricter regulations on the protection against dismissal of data protection officers, provided that these do not impair the realisation of the objectives of the GDPR.[34]

The following	Responsible persons/processors appoint a data protection officer:	have	mandatory

[30] Case C-61/22.

[31] See EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Version 2.0 of 14. December 2021, retrievable in English language at https://edpb.europa.eu/system/files/2022- 01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf .

[32] Federal Act enacting a Telecommunications Act (Telecommunications Act 2021 - TKG 2021), Federal Law Gazette I No. 190/2021; see also Regulation (EU) No. 611/2013, OJ L 173/2013, p. 2.

[33] Cf. in addition WP 243 rev. 01, Guideline of the Art. 29 Group of 13 December 2016 on Data Protection Officers, available at https://www.dsb.gv.at/dam/jcr:a279307b-ce48-416e-9c28-5bae42e0038c/Guidelines_on_Data_Protection_Officers.pdf.These guidelines were expressly adopted by the EDPB: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[34] Cf. the judgment of the ECJ of 22 June 2022, C-534/20, para. 34 et seq.; for example, a national regulation would be inadmissible if it were to cover any data processing carried out by a controller or processor.
prohibits the dismissal of a data protection officer who no longer possesses the professional qualities required to fulfil his or her duties or who does not fulfil his or her duties in accordance with the GDPR.

- Authorities and public bodies (with the exception of courts, insofar as this does not concern the monocratic administration of justice);
- if the core activity is the regular and systematic monitoring o f persons;
- if the core activity consists of the extensive processing of sensitive data in accordance with Art. 9 and criminal data in accordance with Art. 10.

A preliminary ruling procedure is currently pending before the ECJ on the question of whether a certain function within the organisation of a controller/processor is compatible with the function of a data protection officer.[35]

Art. 40 et seq. further expand the system of **codes of conduct** already provided for in Art. 27 of the GDPR. Accordingly, associations and other organisations representing categories of controllers or processors can draw up data protection codes of conduct and submit them to the supervisory authority for approval. Compliance with approved codes of conduct is monitored by a particularly **suitable body**, which must be **accredited** by the supervisory authority.[36]

Articles 42 and 43 stipulate that controllers and processors can have certain processing operations certified in order to prove that the processing is carried out in accordance with the GDPR (data protection seal, certification mark). **Certification** is carried out either by the supervisory authority itself or by certification bodies that are specifically accredited for this purpose by the supervisory authority or the national accreditation body in accordance with Regulation (EC) No. 765/2008.[37] In Austria, accreditation is carried out exclusively by the data protection authority (§ 21 para. 3 DSG).

---

[35] Case C-453/21.
[36] Further information is available at https://www.dsb.gv.at/aufgaben-taetigkeiten/genehmigung-von-verhaltensregeln.html.
[37] See EDPB Guidelines 1/2018 on certifications and certification criteria under Art. 42 and 43 GDPR, available in German at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en_0.pdf, and Guidelines 4/2018 on the accreditation of certification bodies under Art. 43 GDPR, available in German at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf.

Codes of conduct and certifications can also be used as an instrument for the transfer of personal data to recipients in third countries if certain additional requirements are met (see Chapter V below).

6) Chapter V

Chapter V regulates the more detailed conditions for **data traffic with recipients in third countries[38] or international organisations .[39]**

In addition to compliance with the general processing principles, such a data flow is only permitted under the following additional conditions:

- Existence of an adequacy decision by the European Commission (Art. 45)[40]
- Existence of appropriate safeguards (Art. 46). These include, in particular, standard data protection clauses issued by the European Commission[41] , standard data protection clauses adopted by a supervisory authority (Art. 46 para. 2 lit. d) and binding corporate rules (BCRs[42] Art. 47), as well as new mechanisms such as codes of conduct[43] (Art. 40) and certifications[44] (Art. 42).

[38] Third countries in this sense are all countries outside the EU or the EEA.
[39] These are organisations established on the basis of an international treaty or a corresponding agreement between two or more subjects of international law, such as e.g. the United Nations. Private law organisations or non-governmental organisations (NGOs) without a mandate under international law, on the other hand, are not covered by this term.
[40] A list of the currently in validity in force adequacy decisions is available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection- personal-data-non-eu-countries_en.
[41] See Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199/2021, p. 31; the clauses adopted under Directive 95/46/EC can only be used until 27 December 2022.
[42] Cf. WP 256 and WP 257 of the Art. 29 Group, working documents with an overview of the components and principles of binding internal data protection regulations, available in German at at https://ec.europa.eu/newsroom/article29/items/614109 and https://ec.europa.eu/newsroom/article29/items/614109. These have been adopted by the EDPB: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf.
[43] Cf. EDPB, Guidelines 04/2021 on Codes of Conduct as tools for transfers, Version 2.0 of 22 February 2022, available in English at https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf.
[44] Cf. EDPB, Guidelines 07/2022 on certification as a tool for transfers, Version 1.0 of 14 June 2022, available in English at https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf (these are under public review until 30 September).

Art. 49 provides for exceptions in certain cases, whereby a restrictive application of the exceptions provided for therein is required.[45]

The rationale behind Chapter V is that the data transferred to the recipient in the third country or international organisation should be subject to an equivalent level of protection as in the EU. Most transfers should not require authorisation.[46]

Public security officers must note that, pursuant to Sections 58 and 59 of the Data Protection Act, there are **special provisions** for transfers to recipients in third countries or international organisations in connection with the processing of personal data for the purposes of the security police, including state security, military self-protection, the investigation and prosecution of criminal offences, the execution of sentences and the enforcement of measures.

Note:

In the decision of 16 July 2020, C-311/18, known as "Schrems II", the ECJ declared the "Privacy Shield Decision" (Implementing Decision (EU) 2016/1250 of the European Commission), which is decisive for the majority of data transfers to the USA, **invalid**, as the US legal system does not currently standardise a level of protection that is equivalent in substance.[47] The ECJ based its decision in particular on the existence of extensive powers of intervention and access by U.S. authorities, which are not limited to what is absolutely necessary, to

[45] Cf. the EDPB Guidelines 2/2018 on the exemptions under Article 49 of the GDPR. Regulation 2016/679, available in German at https://www.dsb.gv.at/dam/jcr:db22aec8-5c71-4ae4-9c30-b06d07f79335/Leitlinien2-2018%20zu%20den%20Ausnahmen%20nach%20Artikel49%20der%20Verordnung2016-679.pdf.

[46] Exceptions to the exemption from authorisation exist, for example, in the case of provisions in administrative agreements pursuant to Art. 46 para. 3 lit. b GDPR; see the decision of the DPA of 16 May 2022, GZ 2022-0.296.352.

[47] The European Commission and the USA issued a joint declaration on the creation of a new transatlantic data protection agreement on 25 March 2022, available in German language at https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2087; the US Parliament is currently discussing the draft American Data Privacy and Protection Act, which aims to enshrine basic data protection rights for consumers along with effective supervisory and enforcement mechanisms, available at https://www.congress.gov/bill/117th- congress/house-bill/8152/text.

personal data that is transferred from the EU to the USA, as well as inadequate legal protection options for data subjects.[48] At the same time, it ruled that the standard contractual clauses in accordance with European Commission Decision 2010/87/EU as amended by Decision 2016/2297 are compatible with EU law. In certain cases, however, they must be replaced by so-called
"additional safeguards", i.e. in addition to the agreement of standard data protection clauses, controllers may have to take additional measures t o ensure compliance with an equivalent level of protection.[49] These considerations are transferable to the "new" standard data protection clauses pursuant to Implementing Decision (EU) 2021/914.

Adequacy decisions: In 2021, the European Commission adopted adequacy decisions for the United Kingdom of Great Britain and Northern Ireland and for the Republic of Korea (South Korea).

[48] For detailed information on this, see the EDSA FAQs at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.
[49] See in detail the EDPB's Recommendations 01/2020 on measures to supplement transfer tools to ensure the level of protection of personal data under Union law, available in German at https://edpb.europa.eu/our-work-tools/public-consultations-art- 704/2020/recommendations-012020-measures-supplement-transfer_en; see also the summary on the website of the data protection authority at https://www.dsb.gv.at/aufgaben- taetigkeiten/internationaler-datenverkehr.html.

7) Chapter VI[50]

There is at least one independent supervisory authority in each Member State. In Austria, the **data protection authority** has this function.

The tasks and powers are significantly expanded by the GDPR (Art. 57 and 58).

Art. 58 standardises three types of powers:

- Investigatory powers (including the right to enter certain premises)
- Remedial powers (these are powers that enable the supervisory authority to put an end to unlawful behaviour, e.g. by issuing specific orders or imposing fines of up to EUR 20 million or 4% of the total annual global turnover generated in the previous financial year)
- Authorisation and advisory powers.

Pursuant to Art. 55 para. 3 GDPR, **courts** are exempt from supervision by the data protection authority if they are acting in the course of their judicial activities. In this case, legal protection is primarily governed by Sections 83 ff GOG.[51] Conversely, judicial bodies are subject to supervision by the data protection authority if they act within the framework of the monocratic administration of justice.[52] Whether a court is acting in a judicial capacity must be assessed on a case-by-case basis.[53] The ECJ has ruled that the term "judicial activity" covers all processing operations carried out by courts, provided that their

---

50 Cf. in detail *Schmidl*, Aufgaben und Befugnisse der Aufsichtsbehörden sowie Rechtsschutzmöglichkeiten nach der DSGVO, ÖBA 1/17 p. 27 ff; *Flendrovsky*, Die Aufsichtsbehörden, in *Knyrim* (ed.) loc. cit. p. 281 ff.

51 Due to Federal Law Gazette I No. 22/2018, the provisions of the GOG are also to be applied analogously by the administrative courts, the Administrative Court and the Constitutional Court. The same has also been provided for provincial administrative courts, cf. e.g. Section 40a para. 2 of the Lower Austrian Provincial Administrative Courts Act, LGBl. 0015-0 as amended.

52 Cf. in more detail *Schmidl* in *Gantschacher/Jelinek/Schmidl/Spanberger*, Kommentar zu Datenschutz- Grundverordnung1[2017] Art. 55 Note 3; *Nguyen* in *Gola* (ed.), Datenschutz-Grundverordnung [2017] Art. 55 para. 13.

53 See the decisions of the data protection authority of 22 January 2019, GZ DSB-D123.848/0001-DSB/2019, and of 4 February 2019, GZ DSB-D123.937/0001-DSB/2018.

control by a supervisory authority could directly or indirectly influence the independence of the members or the decisions of the courts.[54]

Whether **legislative bodies** (National Council, Federal Council, Ombudsman Board, Court of Auditors) are subject to supervision by the data protection authority is currently the subject of preliminary ruling proceedings before the ECJ.[55] This is to be distinguished from the fundamental obligation of legislative bodies to the GDPR, which was affirmed by the ECJ.[56]

[54] Judgment of the ECJ of 24 March 2022, C-245/20 (X and Z v. Autoriteit Persoonsgegevens), para. 34.
[55] See C-33/22.

[56] Judgment of the ECJ of 9 July 2020, C-272/19 (VQ v. Land Hessen), para. 63 et seq.

8) Chapter VII[57]

As **cross-border situations** are the norm in the digital age, the GDPR also provides for increased **cooperation between the individual supervisory authorities.** In the event of a cross-border situation, a coordinated decision is to be reached with the involvement of all supervisory authorities concerned, which is then to be notified to the controller or processor at the location of its main establishment. As a result, both the data subject and the controller/processor should be confronted with a single point of contact ("one-stop shop").[58]

The supervisory authority at the **headquarters of the main establishment** acts as the **lead supervisory authority**[59] , which coordinates the involvement of the (other) supervisory authorities concerned and prepares a draft decision and agrees it with the supervisory authorities concerned.

The recipient is obliged to implement the decision in all its establishments in the EU, unless it contests the decision.

Chapter VII also provides for the obligation of mutual administrative assistance (Art. 61) and the possibility of implementing joint measures by the supervisory authorities (Art. 62).

---

[57] See in detail *Leissler/Wolfbauer*, Der One Stop Shop in der DSGVO, in *Knyrim* (ed.) loc. cit. p. 291 ff; *Schmidl*, Kooperation der Aufsichtsbehörden bei grenzüberschreitenden Fällen, in *Knyrim* (ed.) loc. cit. p. 303 et seq.

[58] On cooperation between the lead and affected supervisory authorities, see EDPB, Guidelines 02/2022 on the application of Article 60 GDPR, Version 1.0 of 14 March 2022, available in English at https://edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf.

[59] Cf. WP 244, Guideline of the Art. 29 Group of 13 December 2016 on the determination of the lead supervisory authority, available at https://www.dsb.gv.at/dam/jcr:59cd262c-c7b4-45ad-b127-ad58767cdc33/Guidelines%20for%C3%BCr%20the%20determination%20of%20the%20lead%C3%BC%20Supervisory%C3%B6rde%20of%20a%20Responsible%20Person.pdf. These guidelines have been explicitly adopted by the EDPB: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

The cooperation procedure does not apply if the controller/processor is a public authority or a delegated legal entity (Art. 55 (2)).

The **European Data Protection Board (EDPB)** established under Art. 68 plays a key role[60] , in which the supervisory authorities of all Member States, the European Data Protection Supervisor and the European Commission are represented.

According to Art. 70, the committee has a variety of tasks, including the adoption of **guidelines** on certain topics of the GDPR, but also the submission of **opinions** and the **adoption of binding decisions** (Art. 64 and 65).[61] It is supported by a secretariat provided by the European Data Protection Supervisor.

[60] See also https://edpb.europa.eu/.
[61] The decisions adopted as part of the so-called "coherence procedure" are available at https://edpb.europa.eu/our-work-tools/consistency-findings_en.

9) Chapter VIII

Art. 77 standardises the **right to lodge a complaint** with a supervisory authority.

Binding decisions by the supervisory authority or failure to act on the part of the supervisory authority may be appealed **to a court** (Art. 78). The courts of the member state in which the authority is based are responsible for such complaints.

The procedure before the supervisory authority is free of charge for the complainant, unless the complaint is manifestly unfounded or - in particular due to its accumulation - excessive. In these cases, the supervisory authority may refuse to take action or impose reasonable costs.

Art. 79 standardises the right to effective judicial remedy against controllers or processors. According to the case law of the Supreme Court (OGH)[62] , **legal action** can be taken against controllers and processors in the private sector (these are essentially private individuals, groups of individuals and legal entities under private law, such as associations, limited liability companies, etc.) before the competent civil court.

This means that there is a **right to choose when it comes to legal protection:** Complaint to the data protection authority or legal action before a civil court. The question of which of these two legal remedies takes precedence and whether a complaint pursuant to Art. 77 para. 1 GDPR and a court action pursuant to Art. 79 para. 1 leg. cit. can be brought at the same time, a preliminary ruling procedure is currently pending before the ECJ.[63]

Pursuant to Section 29 para. 2 DSG, the regional court entrusted with the exercise of jurisdiction in civil law cases in whose district the plaintiff (or alternatively the defendant) has his habitual residence or registered office has local and subject-matter jurisdiction at first instance. The Supreme Court has ruled that the provision of Section 29

[62] See the decisions of 20 December 2018, GZ 6 Ob 131/18k, and of 23 May 2019, GZ 6 Ob 91/19d.
[63] Case C-132/21.

para. 2 FADP applies not only to claims for damages in the narrower sense, but also to other civil law claims under the FADP or the GDPR.[64]

Please note that - in contrast to a complaint procedure before the data protection authority - a civil action is in any case associated with costs (court fees) and you must be represented by a lawyer if the value in dispute exceeds 4,000 euros (and for a fee).

However, it is not possible to bring a civil action against authorities, offices, etc.. The only option here is to lodge a complaint with the data protection authority.

According to Art. 80, data subjects may be **represented before the supervisory authority** by **specialised bodies,** organisations or non-profit associations and may **bring an action for damages before the courts**. Member States may also provide that these bodies may lodge a complaint with the supervisory authority independently of an authorisation. However, it is not possible to assert claims for damages without a mandate.[65]

Please note that in Austria, the above-mentioned organisations cannot file claims for damages or complaints without a mandate (§ 28 DSG)![66]

Art. 82 standardises the possibility of claiming **compensation[67]** from the controller or processor for material and non-material damage suffered.[68] If several controllers or processors are involved in processing, each of them is liable for the total damage (Art. 82 para. 4).

Art. 83 contains fines and the grounds to be taken into account as aggravating or mitigating factors in the assessment of penalties. The European Data Protection Board

---

[64] Cf. the decision of the Supreme Court of 3 August 2021, 6 Nc 19/21b mwN.
[65] See EC 142, which is intended to prevent class actions.
[66] See also OGH 26 November 2019, GZ 4 Ob 84/19k
[67] Several requests for preliminary rulings are currently pending on the interpretation of Art. 82 GDPR and in particular on the question of whether the award of non-material damages requires an impairment of a certain intensity, see e.g. C-300/21.
[68] See also *Tretzmüller*, Private Enforcement - Immaterieller Schadenersatz bei Datenschutzverletzungen, in: *Jahnel* (ed.) Datenschutzrecht. Yearbook 17 (2017) p. 199 ff.

has issued - legally non-binding - guidelines with criteria for calculating the amount of fines.[69]

The **fines**, which are **administrative penalties**[70] , range up to EUR 20 million or, in the case of a company, up to 4% of the total worldwide annual turnover of the previous financial year, whichever is higher. It is up to the Member States to determine whether fines can also be imposed on authorities and public bodies.[71]

If the legal system of a Member State does not provide for fines, Art. 83 can be applied in such a way that the supervisory authority files a criminal complaint with a court and the fine is imposed by a court.

Art. 83 GDPR also allows fines to be imposed **directly on legal entities** (GmbH, AG, association, etc.). The ECJ is currently clarifying whether it is necessary for the supervisory authority to prove misconduct by a person authorised to represent it (managing director, board member, chairman, etc.) in order to attribute the fine to a legal entity.[72]

Art. 84 obliges the Member States to standardise additional sanctions, in particular criminal offences.

---

[69] See EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 1.0 of 12 May 2022, available in English at https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf (the public review ended on 27 June 2022).

[70] This is clear from a comparison of the language versions; the English version speaks of "administrative fines", the French version of "amendes administratives". Fines are therefore penalties and not a different sanction (cf. on fines in the area of public procurement, for example, the decision of the Administrative Court of 16 December 2015, no. Ro 2014/04/0065).

[71] For Austria, see VfSlg. 19.988/2015 on the inadmissibility of imposing an administrative fine on a supreme body. According to § 30 para. 5 DSG, no fines can be imposed on authorities and public bodies (see point 11 below).

[72] C-807/21.

10) Chapters IX to XI

Chapter IX defines special processing situations (e.g. freedom of expression, access to official documents, employment context). The member states are required to define these processing situations in more detail through legislation in order to bring them into line with the GDPR.

Art. 85 para. 2 gives member states the option to exclude the application of certain chapters of the GDPR in the case of processing for journalistic, scientific, artistic or literary purposes. The Austrian legislator has made use of this in Section 9 DSG, for example. The question of whether the provision of Section 9(1) of the Data Protection Act is unconstitutional is currently pending before the Constitutional Court under Article 140(1) of the Federal Constitutional Law.[73]

According to Art. 99, the Regulation entered into force on the twentieth day after its publication in the OJ (which was 24 May 2016) and has been in force since 25 May 2018.

[73] Constitutional Court, G 200/2022

11) The Austrian Data Protection Act

In order to implement the GDPR and the Data Protection Directive for the Police and Justice Sector (DSRL-PJ)[74] , the Austrian legislator passed the Data Protection Adaptation Act 2018[75] , which came into force on 25 May 2018. There were two amendments in 2018 (Federal Law Gazette I No. 23/2018 and Federal Law Gazette I No. 24/2018), the Data Protection Act was last amended with Federal Law Gazette I No. 14/2019 and changes are also expected in the future.

The centrepiece of the new regulation is the Federal Act on the Protection of Natural Persons with regard to the Processing of Personal Data (Data Protection Act - DSG). The previously applicable Data Protection Act 2000 was stripped of its simple legal provisions, while the constitutional provisions (in particular the fundamental right to data protection under Section 1) largely remain in place or have been adapted.

The DPA is divided into five main sections. The 1st main section standardises the implementation of the General Data Protection Regulation and supplementary regulations, the 2nd main section regulates the bodies (of data protection), the 3rd main section regulates the implementation of the GDPR-PJ, the
Section 4 contains the special penal provisions and Section 5 the final provisions.

Of particular relevance for controllers and processors is the **first main section**, which is divided into
is divided into **three sections**.

Section 1 contains **general provisions** (e.g. on the data protection officer or data secrecy).

Section 2 regulates **data processing for specific purposes** (e.g. for the purposes of scientific research and statistics).

---

[74] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA - Data Protection Directive-Police Justice (DSRL-PJ), OJ No. L 119, 04.05.2016 p. 89.
[75] Federal Law Gazette I No. 120/2017.

Section 3 regulates **image processing** (formerly "video surveillance"). However, the Federal Administrative Court (BVwG) has ruled that these provisions do not apply.[76] Image processing in the private sector is therefore governed by Art. 5 and 6 GDPR.[77]

Other key points are

- The **data protection authority** is established as a **supervisory authority with all powers** (**including the imposition of fines**[78]) under the GDPR and the GDPR-PJ.
- **Fines** can also be imposed directly **on legal entities** and not only on the responsible authorised representative (Section 9 of the Administrative Penal Act 1991 - VStG); no fines can be imposed on authorities and public bodies.
- The data protection authority makes binding decisions on all **complaints** (i.e. also on those for which civil proceedings were required under the previous legal situation in accordance with § 32 DSG 2000).
- Binding decisions by the data protection authority can be appealed to the **Federal Administrative Court** without restriction.
- **Data subjects** may be **represented** before the data protection authority and the Federal Administrative Court by non-profit institutions, organisations or associations that are active in the field of data protection; **there is no provision** for the **intervention** of institutions, organisations or associations **without a mandate** (i.e. without authorisation) .[79]
- In addition to the fines under the GDPR, **administrative offences** are also standardised, which are punishable by the data protection authority with a fine of up to EUR 50,000.

---

[76] See the decisions of 20 November 2019, GZ W256 2214855-1, and of 20 November 2019, GZ W211 2210458-1.

[77] See the information at https://www.dsb.gv.at/download-links/fragen-und-answer.html#Videoueberwachung_durch_Private_einschlieszlich_der_Privatwirtschaftsverwaltung_der_oeffentlichen_Hand_.

[78] On the admissibility of administrative authorities imposing substantial fines, see the Constitutional Court's ruling of 13 December 2017, GZ G 408/2016 et al.

[79] See OGH 4 Ob 84/19k.

- The **lists** to be maintained by the **data protection authority** (necessity of carrying out a data protection impact assessment, requirements for certification bodies, criteria for the accreditation of a body) are to be published in the form of an **ordinance** in the Federal Law Gazette (BGBl.).[80]

[80] See the page https://www.dsb.gv.at/verordnungen-in-osterreich. The Data Protection Impact Assessment Exemption Regulation (DSFA-AV), Federal Law Gazette II No. 108/2018, and the Regulation on processing operations for which a data protection impact assessment must be carried out (DSFA-V), Federal Law Gazette II No. 278/2018, and the Regulation on the requirements for a monitoring body for codes of conduct (ÜStAkk-V), Federal Law Gazette II No. 264/2019, have already been issued.

12) Frequently asked questions

a) General information

When did the GDPR come into force?

Since 25 May 2018.

Can I myself with questions concerning the DSGVO and the DPA to to the data protection authority?

The data protection authority shall provide the parties with information on the content of their pending proceedings before the data protection authority.

Pursuant to Art. 57 para. 1 lit. e GDPR, the data protection authority is obliged to provide any data subject with information on the exercise of their rights under this regulation upon request. However, this support is not suitable to replace a lawyer and must not anticipate the outcome of proceedings.

We therefore ask for your understanding that no legal judgements on the application and interpretation of legal provisions or substantive advisory services can be made in the context of a written enquiry. Binding decisions can only be made at the end of a specific procedure.

What is a "public body"?

The data protection authority cannot carry out a specific case-by-case examination to determine whether a body is to be regarded as a public body or not.

- In principle, it is the responsibility of the controller to carry out this categorisation in accordance with the applicable legal basis. In addition to various German-language commentaries (see point 13 of this guide) and the guideline of the Art. 29 Working Party on the Data Protection Officer[81] , which provide points of reference for the interpretation of the term "public sector body", the

[81] Available at https://www.dsb.gv.at/europa-internationales/europaeischer_datenschutzausschuss_edsa.html.

Data Protection Act[82] . A definition can be found in **§ 30 para. 5 DSG**, which can be used. According to this definition, "public bodies" can be considered, in particular, bodies established under public or private law that act on the basis of a legal mandate, as well as corporations under public law.

If the controller in question does not fulfil these criteria, it will be difficult to classify it as a public body.

Will there still be a national data protection law after the GDPR comes into force?

Yes, the Austrian parliament has passed the Data Protection Amendment Act (see also point 11 of the guide). The Data Protection Act (DSG) remains in force.

Does data protection law also apply to legal entities?

Legal entities (e.g. an association, a limited liability company, a public limited company, a cooperative) are obliged by the GDPR to comply with certain requirements.

As a rule, however, they cannot invoke the **GDPR** to assert rights (such as access, erasure, objection, etc.) because the GDPR only protects natural persons. The ECJ only allows the GDPR to be invoked if the name of a natural person appears in the company/name of the legal entity (e.g. Max Mustermann GmbH).[83]

§ Section 1 DSG - unlike the GDPR - still also protects legal entities in Austria.[84]

[82] Available on the Parliament's website at www.parlament.gv.at.
[83] Cf. the judgment of the ECJ of 9 November 2010, verb. C-92/09 and C-93/09 (Schecke and Eifert), para. 53 et seq.
[84] See also the decision of the data protection authority dated 25 May 2020 regarding GZ: 2020-0.191.240.

This means that legal entities can assert the following rights in "domestic cases" (i.e. cases without a foreign connection):

- Secrecy
- Information
- Correction
- Cancellation

How can I distinguish the DSFA-AV from the DSFA-V?

If the question arises as to whether or not a data protection impact assessment should be carried out, the two DPA regulations and the explanatory notes (available on the DPA website) should be read first.

Only if a processing activity **does not** appear in the **DPIA-AV** does the question of a data protection impact assessment arise.

The DSFA-V gives priority to the DSFA-AV (cf. § 2 DSFA-V, which states:
"*If [...] there is no data processing in accordance with the [DSFA-AV], a data protection impact assessment must in any case be carried out in accordance with the following provisions*").

b) I am a data subject - my rights

What rights am I entitled to (data subject rights) and where can I assert them?

The GDPR introduces a new catalogue of rights, some of which are the same as the rights to which we were previously accustomed. Please note that, as a rule, only natural persons are entitled to these rights.

In almost all cases, the controller must be requested to grant the right before a complaint is possible. The data protection authority offers non-binding forms for this purpose on its website .[85]

[85] Available at https://www.dsb.gv.at/dokumente.

1. The **right to information (Art. 15 GDPR)**. The data subject may request confirmation as to whether data concerning them is being processed, including negative information. If data is processed, the data subject has the right to the following information:

    a. Processing purposes;

    b. Data categories;

    c. Copy (e.g. printout) of the processed data content;

    d. Data recipients or categories of recipients;[86]

    e. planned storage period (or criteria for its determination);

    f. Existence of a right of rectification, cancellation, restriction right of cancellation, restriction or objection;

    g. Existence of a right of appeal to a supervisory authority;

    h. available information about the origin of the data;

    i. Existence of an automated decision-making (including profiling), logic and scope of such procedures.[87]

    The deadline for providing information is shortened to one month by the GDPR. An extension to three months may be possible.

    The right of access is a right to information about the data subject's own data.[88] A copy of the processed data content must be designed in such a way that the data protection rights of other persons are not violated. The scope of the right of access under Art. 15 para. 3 GDPR is currently the subject of preliminary ruling proceedings before the ECJ.[89]

[86] Note the currently pending preliminary ruling proceedings before the ECJ in case C-154/21.
[87] Note the preliminary ruling proceedings currently pending before the ECJ on Art. 22 in case C-203/22.
[88] See the decisions of the DSB of 18 April 2019, GZ D122.913/0001-DSB/2019; and of 12 November 2020, GZ 2020-0.697.744.
[89] Case C-487/21.

2. The **right to rectification (Art. 16 GDPR)** relates to data content.[90] New in the GDPR is the right to completion of data - possibly by means of a supplementary note. The deadline for rectification is shortened to one month by the GDPR. An extension to three months may be possible.

3. The **right to erasure (Art. 17 GDPR)** (including the "right to be forgotten"). The right to erasure presupposes that one of the following circumstances exists or has occurred:

    a. Discontinuation of the processing purpose

    b. Revocation of the consent of the data subject

    c. Effective objection to data processing

    d. initial unlawfulness of the data processing

    e. Legal obligation to erasure (e.g. law, judgement, decision)

    f. Lack of consent from a child's legal guardian

    New: If the data controller has made the data public (e.g. on the Internet), he must take all reasonable measures, including technical measures, to inform responsible data recipients (in particular search engine operators) that the data subject wishes the deletion or removal of links, copies or replications (= "right to be forgotten").

    The right to erasure may be restricted by the right to freedom of expression, by legal obligations of the controller, interests of legal defence and public interests (public health, scientific and archiving purposes).

    The deadline for erasure is shortened to one month by the GDPR. An extension to three months may be possible.

[90] The DSB is of the opinion that mere orthographic (spelling) errors are not covered by the right to rectification. This was confirmed by the Federal Administrative Court in its ruling of 5 February 2021, W211 2226025-1 and is currently being reviewed by the Administrative Court as part of an appeal procedure.

4. New: The **right to restriction of processing (Art. 18 GDPR)**. This is a time-limited or conditional right. The requirements are:

    a. the accuracy of the data is disputed;

    b. the lawfulness of the data processing is disputed, but the data subject himself refuses to delete the data;

    c. the data subject requires the data, the processing purpose of which has ceased to exist, for the assertion of legal claims;

    d. the data subject has objected to the data processing.

    Data in respect of which the right to restriction of processing has been exercised may only be processed with the consent of the data subject, to assert legal claims, to protect the rights of others or for reasons of important public interest.

    In cases a. and d., the restriction is limited to the duration of the examination of the main claim (for cancellation). The data subject must be informed before the restriction is lifted.

    Data recipients must be informed about restrictions unless this is impossible or would involve disproportionate effort. The data subject may request to be informed about the recipients of the data.

    The period for restricting processing is one month. An extension to three months may be possible.

5. New: The **right to data portability (Art. 20 GDPR)**. It is intended to ensure that the data subject can receive back their own data that they themselves have disclosed to a (private) controller ("provided") or transfer it to a new controller. This includes, for example, self-created profiles in social networks. Data controllers should ensure direct, technical portability wherever possible, but this is not mandatory. The data of persons other than the data subject are not subject to this right. It can only be asserted if the basis for the

data processing is either the consent of the data subject or a contract.

6. The **right to object (Art. 21 GDPR)**. By exercising this right, the data subject may, in the case of data processing that takes place without their express or implied consent (e.g. on the basis of a legal authorisation or due to overriding legitimate interests asserted by the controller), request an examination of the reasons put forward by them for terminating the processing. Objection to data processing for the purposes of direct advertising and associated profiling (automatic evaluation of a person and their behaviour, e.g. assessment of purchasing power, classification in a marketing target group) is possible at any time without giving reasons. You can also object to the sending of electronic mail for advertising purposes (SMS, e-mails, etc.) by registering in the so-called "ECG list".[91] An entry in the so-called "Robinson list" can be made against the sending of postal advertising material.[92] If the objection is justified, the data must be deleted.

   The deadline for deciding on an objection is one month. An extension to three months may be possible.

7. **Rights relating to automated individual decision-making and profiling (Art. 22 GDPR)**. The GDPR prohibits such decisions (e.g. when imposing administrative penalties, tax regulations, decision job applications, granting loans, concluding contracts in general, categorisation in a marketing target group), but provides for some exceptions. Exceptions are legally prescribed cases of application, explicit and verifiable consent of the data subject and due diligence obligations when concluding a contract. For the provision to apply, the entire decision-making process does not have to be exclusively automated. It may only be based under special conditions and never exclusively on sensitive data (special categories of data pursuant to Art. 9 para. 1 GDPR). The

[91] See Art. 174 Para. 4 No. 4 TKG 2021 in conjunction with Art. 7 Para. 2 E-Commerce Act; the "ECG list" is maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR).
[92] The "Robinson list" is maintained by the WKO.

Above all, the data subject can request that the automated decision be reviewed by a human being and has a special right to information regarding the logic of the automated decision-making process.

The deadline for deciding on rights relating to automated decision-making is one month. An extension to three months may be possible.

c) I am Responsible person/processor - My obligations

Am I a controller or processor?

Defining your own role is essential.

The controller within the meaning of the GDPR is the person who determines which data is processed for which purposes and by which means ("data controller"). Being the controller does not depend on the organisational or legal form, but on functional aspects.[93] The data controller also has the sole decision as to whether data is changed, corrected or deleted. He/she is the addressee of data subjects' rights and must fulfil them.

UU, there is **joint responsibility** (Art. 26 GDPR), i.e. two or more controllers take the above-mentioned decisions.[94] It is not necessary for the tasks and duties to be equally distributed; however, it is crucial that each party involved can at least make decisions, even if only minimally (see in particular the judgements of the ECJ of 5 June 2018, C-210/16, and of 10 July 2018, C-25/17).

---

[93] See also the ruling of the Federal Administrative Court W258 2221952-1/3E of 31 March 2020; see also EDPB, Guidelines 07/2020 on the terms "controller" and "processor" in the GDPR, version 2.0 of 7. July 2021, retrievable in German language at https://edpb.europa.eu/system/files/2022- 02/eppb_guidelines_202007_controllerprocessor_final_en.pdf.

[94] With regard to court-certified experts, see for example the findings of the Federal Administrative Court of 27 September 2018, GZ W214 2196366-2 and 23 January 2020, GZ W214 2196366-3.

A **processor**, on the other hand, processes data "on behalf of", i.e. on the **instructions** and under the **supervision** of a controller. Data processing for its own purposes is not intended.

The following persons/entities are generally **not processors**:

- Members of the liberal professions (i.e. lawyers, doctors, tax consultants, etc.) - these are subject to their own professional rules or the relevant legal provisions provide for independent data processing
- Telecommunications companies - these are subject to the provisions of the TKG 2021, which obliges them to process data on their own responsibility
- Credit reference agencies - these are subject to the Trade Regulation Act and process data independently for the purpose of providing information about a person's creditworthiness
- Operators of Internet search engines - these decide themselves on the purposes and means of processing as part of the automatic, continuous and systematic "crawling" of information published on the Internet and are therefore to be regarded as data controllers

Whether someone is a controller or processor cannot be answered in general terms and must be assessed on a case-by-case basis.[95]

Does the GDPR only apply to large companies?

No. The GDPR applies to small and one-person companies as well as to associations, public authorities and public bodies. There are some exceptions for small and one-person companies (e.g. in Art. 30 para. 5 GDPR regarding the maintenance of a register of processing activities).

I have obtained the consent of data subjects (e.g. customers) for data processing. Does the GDPR change this?

Provided that the consent obtained fulfils the requirements of Art. 7 GDPR, nothing changes. Consent must be obtained again if necessary.

---

[95] In the case of professional detectives, for example, it depends on whether the respective assignment has such a level of detail that the final decision, in particular on the time of data collection and the means, is made by the client; see the decision of the Federal Administrative Court of 25 June 2019, GZ W258 2188466-1.

What is covered by consent?

Consent is one of several options for processing data in accordance with the law (**legal basis for data processing**). With consent, the data subject agrees to their data being processed for a specific purpose. Consent can be revoked at any time.

However, the following are not covered by consent

- Deviations from necessary data security measures (e.g. consent to messages being transmitted in a certain - insecure - manner)
- Involvement of processors (this decision is the sole responsibility of the controller)

Such consent cannot be legally effective.

It should also be noted that for some processing operations, "normal" consent is not sufficient and the data subject must give their consent explicitly.[96]

What do I have to inform data subjects about when collecting their data? Are there any exceptions?

If you collect the data directly from the respective data subjects, you must provide the data subjects with all information as stipulated in Art. 13 GDPR. An exception to the obligation to provide information only applies if the data subjects already have this information.

If you want to process data that you have not collected from the data subjects themselves, you must provide the data subjects with all information as stipulated in Art. 14 GDPR. This may be omitted if the data subjects already have the information, the provision of the information is impossible or involves a disproportionate effort, the processing is provided for by law or the data is subject to professional secrecy (see Art. 14 para. 5 GDPR).

[96] This is provided, for example, for certain processing operations of special categories of personal data (Art. 9 para. 2 lit. a GDPR), for automated decisions in individual cases (Art. 22 para. 2 lit. c GDPR), or for the transfer of personal data to an unsafe third country in exceptional cases (Art. 49 para. 1 lit. a GDPR).

Please refer to the EDPB guidelines on transparency (see Chapter III above for more details).

Excursus:

In this context, it should be noted that consent to cookies can also be "voluntarily for the specific case, in an informed and unambiguous manner". "Silence, already ticked boxes or inactivity" cannot constitute consent within the meaning of the GDPR.[97]

What are the obligations for controllers and processors?

Below you will find a brief overview of the most important obligations imposed on controllers and processors by the GDPR:

- ***Register of processing activities (Art. 30 GDPR)***

Controllers must keep a written record of all processing activities (= data applications) for which they are responsible. This list must in any case contain: the name and contact details of the controller, data of a joint controller (if any), data of the controller's representative (if any), data of the data protection officer (if any), the purposes of the processing, the description of the categories of data subjects and the categories of personal data (= groups of data subjects and types of data), categories of recipients (including recipients in third countries or international organisations); if possible: deletion deadlines, description of technical and organisational measures.

The register can be kept internally in any language. However, if it is submitted to the data protection authority**, the register must be submitted in German**, as the data protection authority cannot take foreign-language documents into account in its proceedings (official language German pursuant to Art. 8 para. 1 of the Federal Constitutional Act; see also the ruling of the Administrative Court dated
17 May 2011, no. 2007/01/0389).

[97] See the decision of the ECJ of 1 October 2019, C-673/17.

Processors must also keep a written record of all categories of activities carried out on behalf of the controller. The controller and its processor or, if applicable, their representative must make the list available to the data protection authority upon request.

Companies or organisations with fewer than 250 employees are not obliged to keep a register unless the processing they carry out poses a risk to the rights and freedoms of the data subjects, the processing is not occasional or special categories of data are processed in accordance with Art. 9 para. 1 GDPR (data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the identification of a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) or processing of personal data relating to criminal convictions and offences within the meaning of Art. 10 GDPR.

For information:

As of 25 May 2018, the obligation to notify the Data Processing Register in accordance with Sections 17 et seq. of the Data Protection Act 2000 (DSG 2000) no longer applies. DVR notifications are no longer required (see also the information under point 11).

Since the creation and maintenance of a register is the exclusive responsibility of controllers/processors in accordance with Art. 30 GDPR, the data protection authority also leaves it up to them to decide how they want to organise the content of their register. The data protection authority does not provide any specifications or templates in this regard. Former DPA notifications can be used as a template for a register, but this is not mandatory.

- ***Cooperation with the supervisory authority (Art. 31 GDPR)***

The controller and the processor, or their representative if applicable, must co-operate with the data protection authority at its request. Failure to comply with this obligation is punishable by a fine of up to 10 million euros.

- ***Security of processing (Art. 32 GDPR)***

The controller and its processor must ensure an adequate level of protection through appropriate technical and organisational measures, which may include
be demonstrated, among other things, by approved codes of conduct (Art. 40 GDPR) or on the basis of approved certification procedures (Art. 42 GDPR).

- ***Notification of personal data breaches to the supervisory authority (Art. 33 GDPR)***

A controller must notify the data protection authority in the event of a personal data breach if there is a risk to the rights and freedoms of data subjects; this must be done immediately and, if possible, within 72 hours of becoming aware of the breach. In addition, the necessary information (description of the breach, number of data subjects or data records, measures, probable consequences, documentation, etc.) must be provided to the data protection authority. The data protection authority provides a model notification form on its website .[98]

- ***Notification of a personal data breach to the data subject (Art. 34 GDPR)***

A controller must notify data subjects of data breaches caused by it if there is a high risk to the rights and freedoms of data subjects; this must be done without undue delay (exceptions are possible here).

- ***Data protection impact assessment (Art. 35 GDPR)***

Where a form of processing, in particular when using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons due to the nature, scope, context and purposes of the processing, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data beforehand.

A data protection impact assessment is required in the following cases in particular:

[98] Available at https://www.dsb.gv.at/dokumente

- systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and which in turn serves as the basis for decisions that produce legal effects concerning natural persons or similarly significantly affect them;
- extensive processing of special categories of personal data pursuant to Art. 9 para. 1 GDPR or of personal data relating to criminal convictions and offences pursuant to Art. 10 GDPR or
- Systematic, comprehensive monitoring of publicly accessible areas.

The data protection authority must draw up and publish a list of processing operations for which a data protection impact assessment must be carried out in any case (see the Data Protection Impact Assessment Regulation - DSFA-V, Federal Law Gazette II No. 278/2018). It has also published a list of processing operations for which no data protection impact assessment must be carried out (the Data Protection Impact Assessment Exemption Regulation - DSFA-AV, Federal Law Gazette II No. 108/2018[99]). Legislation may also provide for a mandatory data protection impact assessment.

The data protection impact assessment must at least contain the following:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purpose;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the mitigating measures planned to address the risks, including safeguards, security measures and procedures to ensure the protection of personal data and to demonstrate that

[99] Available at https://www.dsb.gv.at/verordnungen-in-osterreich.

this Regulation is complied with, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

A single data protection impact assessment can be carried out to analyse several similar processing operations with similarly high risks.

Note:

- The guidelines of the Art. 29 Working Party on Data Protection Impact Assessment[100] list nine criteria that may be decisive for carrying out a data protection impact assessment.
- The aforementioned guideline contains references to already established procedures for data protection impact assessments.
- For existing processing operations (data applications), a data protection impact assessment does not have to be carried out if these processing operations have already been authorised by the data protection authority at an earlier point in time in the course of a DPA registration as part of a prior checking procedure pursuant to Section 18 of the Data Protection Act 2000 (DSG 2000). However, this does not apply to automatic registration via DVR-Online or in cases in which the data protection authority has registered a data application but no prior check has actually been carried out (this applies to notifications prior to 1 September 2012 that are not subject to prior checking or notifications in which the client has mistakenly ticked the existence of prior checking).
- However, if there is a change to existing processing operations, a data protection impact assessment must be carried out if the requirements of Art. 35 para. 1 GDPR apply. It is generally recommended to subject existing data processing operations to a regular evaluation to determine whether the requirements have changed. If so, a data protection impact assessment should be carried out if all requirements are met.

[100] Available at https://www.dsb.gv.at/dam/jcr:ba295358-cf65-41a6-911d-a88cae94ba20/Leitlinien%20zur%20Datenschutz-Folgenabschaetzung-wp248-rev-01_en.pdf. These guidelines have been explicitly adopted by the EDPB: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

to be carried out. In addition, it is recommended to also document from which no data protection impact assessment was carried out.

- The data protection impact assessment can be carried out in any language and recorded internally in writing. However, if it is submitted to the data protection authority (e.g. in a consultation procedure), the data protection impact assessment must be submitted in German, as the data protection authority cannot take foreign-language documents into account in its procedures.

➢ ***Prior consultation (Art. 36 GDPR)***

The controller must consult the data protection authority before the start of processing if a data protection impact assessment pursuant to Art. 35 GDPR indicates that the processing would result in a high risk, unless the controller takes measures to mitigate the risk.

If the data protection authority comes to the conclusion that the planned processing would not be in accordance with the GDPR, in particular because the controller has not sufficiently identified or mitigated the risk, it will submit written recommendations to the controller (and, if applicable, the processor) and may exercise its powers under Art. 58 GDPR.

The controller must provide the data protection authority with the following information as part of a consultation:

- where applicable, information on the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular in the case of processing within a group of companies;
- the purposes and means of the intended processing;
- the measures and safeguards provided for the protection of the rights and freedoms of data subjects under the GDPR;
- the contact details of the data protection officer, if applicable;
- the data protection impact assessment pursuant to Art. 35 GDPR and
- any other information requested by the supervisory authority.

In addition, controllers may be required by law to consult with and obtain prior authorisation from the supervisory authority when processing for the performance of a task carried out in the public interest, including processing for social security and public health purposes.

- ***Appointment of a data protection officer (Art. 37 GDPR)***

The controller and the processor must appoint a data protection officer if:

- the processing is carried out by a public authority or body, with the exception of courts acting in their judicial capacity;
- the core activity of the controller or processor consists of carrying out processing operations which, by virtue of their nature, their scope and/or their purposes, require extensive regular and systematic monitoring of data subjects, or
- the core activity of the controller or processor is the extensive processing of special categories of data pursuant to Art. 9 GDPR or of personal data relating to criminal convictions and offences pursuant to Art. 10 GDPR.

Other controllers or processors may appoint a data protection officer on a voluntary basis. A group of companies or public organisations may appoint a joint data protection officer. The contact details of the data protection officer must be published and communicated to the data protection authority.

Do I need a data protection officer?

You must first decide for yourself whether you "need" a data protection officer. For the majority of companies, the appointment will generally be optional. A data protection officer is only mandatory under the GDPR for authorities or public bodies (with the exception of courts, unless they are acting within the framework of the administration of justice) and for companies that are primarily active in a specific business area. The corresponding regulations can be found in Art. 37 GDPR.

When is it mandatory to appoint a data protection officer (in my company)?

The controller or processor must appoint a data protection officer if

a. the core activity consists of carrying out processing operations which, by virtue of their nature, their scope and/or their purposes, require extensive regular and systematic monitoring of data subjects, or

b. the core activity consists of the extensive processing of special categories of data (pursuant to Art. 9 GDPR) or of personal data relating to criminal convictions and offences (pursuant to Art. 10 GDPR).

What position[101] does the data protection officer have and does he or she necessarily have to be an employee?

The position of the data protection officer is regulated in more detail in Art. 38 GDPR. Accordingly, the data protection officer does not receive any instructions in the fulfilment of his or her tasks and may not be dismissed or disadvantaged because of the fulfilment of his or her tasks. The data protection officer reports directly to the highest management level. Furthermore, the controller and the processor must support the data protection officer in the fulfilment of his tasks and provide him with the resources necessary for the fulfilment of these tasks.

The data protection officer may be an employee of the controller or the processor or fulfil their tasks on the basis of a service contract (Art. 37 (6) GDPR).

For **federal ministries and their subordinate agencies or institutions**, Section 5 DSG stipulates that the data protection officer must be a member of the staff of the respective ministry, agency or institution.

---

[101] See also the guidelines in relation to data protection officers, available at https://www.dsb.gv.at/dam/jcr:a279307b-ce48-416e-9c28-5bae42e0038c/Guidelines_in_relation_to_data_protection_officers.pdf. These guidelines have been explicitly adopted by the EDPB: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

Social insurance institutions or self-governing bodies for which the federal government only has a supervisory right are not covered by Section 5 DSG.

Can a data protection officer be the responsible officer according to § 9 VStG?

In the opinion of the data protection authority, the **data protection officer** has **an advisory function**. Binding directives are to be issued by the management level. The data protection authority is therefore of the opinion that a data protection officer **cannot** be appointed as the responsible officer.

Does the data protection officer need specific (academic) training?

No. In accordance with Art. 37 (5) GDPR, the data protection officer is appointed on the basis of his or her professional qualifications and, in particular, the expertise he or she possesses in the field of data protection law and practice, as well as on the basis of his or her ability to fulfil the tasks of the data protection officer in accordance with Art. 39 GDPR.

Do political parties and trade unions need a data protection officer?

Yes, political parties and trade unions do not fall under the concept of
"public sector body", but its core activity consists of the extensive processing of sensitive data in accordance with Art. 9 GDPR (here: political opinion and trade union membership, possibly also religious or ideological beliefs).

Does an individual doctor or lawyer need a data protection officer?

No. Although extensive processing of sensitive data or criminal data in itself would be a prerequisite for the need to appoint a data protection officer, the GDPR provides for simplifications for the individual doctor or lawyer in this regard. According to recital 91, the processing of personal data should **not be considered to be extensive** if the processing concerns personal data of patients or clients and is carried out by an individual doctor, other health professional or lawyer.

What are rules of behaviour?

Pursuant to Art. 40 GDPR, codes of conduct provide a more detailed interpretation of the legal situation by specifying the application of the GDPR in certain areas. Associations and other organisations representing categories of controllers or processors can draw up such codes of conduct and submit them to the supervisory authority for approval. A body accredited by the supervisory authority must be entrusted with monitoring compliance with approved codes of conduct. Compliance with the code of conduct in accordance with Art. 40 GDPR can be used as a criterion to demonstrate the fulfilment of the controller's or processor's obligations.

The Data Protection Authority has already approved codes of conduct and provides general guidance on codes of conduct on its website.[102]

What is certification and who carries it out?

Data protection specific certification procedures, data protection seals and data protection certification marks serve as proof of de facto compliance with the requirements of the GDPR for certain processing operations. Certification is issued by the data protection authority or bodies accredited by it for this purpose on the basis of the certification criteria of an approved certification procedure. The maximum validity of a certification is three years; a (multiple) extension by a maximum of three years is possible.

What does the GDPR mean for the use of cloud services?

Most cloud services (especially storage) are a form of order processing. It should be noted that the use of cloud services may result in the transfer of data to a third country, for which a separate legal basis is required (e.g. standard data protection clauses). If a cloud service provider is used, secure data processing by this provider must be guaranteed. If there is a breach of the protection of personal data in the cloud (e.g. due to a hacker attack or similar), the responsibility under data protection law (including

[102] See https://www.dsb.gv.at/aufgaben-taetigkeiten/genehmigung-von-verhaltensregeln.html.

The data controller (i.e. the person/organisation using the cloud services) is responsible to the outside world for any claims for damages.)

What am I liable for?

Any (natural) person who has suffered material or non-material damage as a result of a breach of the GDPR is entitled to compensation from the controller or processor. Each controller who was involved in the processing is fully liable. The processor is liable if it did not fulfil its specific obligations or did not (fully) follow the controller's instructions. In the internal relationship, the claimed party can recourse to other parties in proportion to their responsibility.

This is intended to ensure effective legal protection.

No liability shall arise if neither the person responsible nor the client is responsible for the circumstance through which the damage occurred.

What is the legal situation for associations?

The GDPR makes little reference to certain legal and organisational forms. Organisations that process personal data are controllers.

The Data Protection Impact Assessment Exemption Regulation **(** DSFA-AV), Federal Law Gazette II No. 108/2018, exempts the member administration of associations and associations of individuals (DSFA-A03 Member Administration). However, this exception is limited to the maintenance of membership directories, the recording of membership and sponsorship fees and communication with members or sponsors.

Associations with a religious, ethnic or other ideological background may process special categories of personal data. According to Art. 9 para. 2 lit. d GDPR, such data may be processed by a foundation, association or other non-profit organisation with a political, ideological, religious or trade union orientation:

- on the basis of suitable guarantees;
- within the scope of their legitimate activities;

- provided that the processing relates solely to the members or former members of the organisation or to persons who have regular contact with it in connection with its purpose, and
- the personal data is not disclosed externally without the consent of the data subjects.

The other provisions of the GDPR also apply to associations without restriction (in particular the obligation to inform data subjects in accordance with Art. 13 GDPR and the maintenance of a register of processing activities in accordance with Art. 30 GDPR).

How long can I store data?

In some cases, there are legal time limits within which data must be stored (e.g. 7 years in accordance with § 132 of the Federal Fiscal Code - BAO).

If no statutory time limit is provided for, it is up to the controller to determine **independently** how long data is stored (see, for example, Section 51 (3) of the Austrian Medical Practitioners Act).

The following factors may be decisive:

- pending or imminent litigation (the mere assumption that legal action could be taken is not sufficient)
- Time that has elapsed since the data was collected (the older the data, the less relevant it is)
- Data are for fulfilment of a contract (no more) required (e.g. insurance contract)

A **blanket** (i.e. unspecified) retention period of at least 30 years (general limitation period according to the General Civil Code - ABGB for the assertion of certain rights) is not permitted.

Can I only send messages/documents electronically in encrypted form?

The GDPR does not stipulate that messages/documents may only be sent electronically in encrypted form (e.g. via encrypted e-mails).

However, encrypted transmission may be advisable depending on the circumstances (type of data, processing purposes, reliability of the system).

Important: Data subjects cannot be legally required to consent to certain types of transmission (e.g. transmission via messenger services or e-mail) by means of a declaration of consent.

Am I allowed to operate video surveillance/image processing?

You can find more information on this at https://www.dsb.gv.at/fragen-und-antworten > Video surveillance by private individuals (including private sector management by the public sector).

d) International data transfer to recipients in a third country or in an international organisation

What needs to be considered when transferring data to recipients in a third country or an international organisation? What happens to previous authorisations?

The GDPR provides far-reaching freedom of authorisation for international data traffic (Art. 44-50 GDPR). Care must be taken to ensure that all processing operations are first authorised domestically before data export is permitted (so-called "two-stage check").

The legal instruments for data export already known under Directive 95/46/EC have been retained and in some cases supplemented by new options:

Personal data may be transferred to recipients in a third country or in an international organisation if an adequate level of protection has been established there (Art. 45 GDPR). The determination is made by the European Commission and its adequacy decisions are published.[103]

[103] An overview including further information on the adequacy decisions pursuant to Art. 45 GDPR can be found at https://ec.europa.eu/info/law/law-topic/data- protection/international-dimension-data-protection/adequacy-decisions_en.

Furthermore, the transfer is permitted if a contractual agreement has been concluded between the data exporter and the data importer using standard data protection clauses or if binding corporate rules (BCRs) exist. These instruments already existed under Directive 95/46/EC, although the binding corporate rules were not explicitly codified until the GDPR. The new legal instruments include codes of conduct (Art. 40 GDPR) and certification mechanisms (Art. 42 GDPR). Art. 46 para. 3 GDPR contains the possibility of obtaining authorisation from the supervisory authority for further instruments (e.g. individual contractual clauses), whereby it should be noted that the consistency procedure pursuant to Art. 63 GDPR (i.e. in particular the involvement of the European Commission and the European Data Protection Board) must be applied in principle for such cases.

Art. 49 GDPR contains a number of exemptions for special cases, some of which correspond to the rules in the previous Section 12 DSG 2000 (consent, performance of a contract, public interest, defence of legal claims, vital interests) and some of which are new (transmission of an extract from a public register). However, a restrictive application is required for all these exceptions.

ATTENTION: There are guidelines of the EDPB on Art. 49 GDPR![104]

The GDPR means fewer official channels and more responsibility for the data controller. In particular, it is necessary to know your own data processing and its purposes and (if there is no adequacy decision by the European Commission for the third country in question) to decide for yourself which legal instruments or suitable guarantees (including any additional measures) are required for a data transfer to recipients in a third country or in an international organisation.[105]

---

[104] available in German at https://www.dsb.gv.at/dam/jcr:db22aec8-5c71-4ae4-9c30-b06d07f79335/Leitlinien2-2018%20zu%20den%20Ausnahmen%20nach%20Artikel49%20der%20Verordnung2016-679.pdf.

[105] See EDPB, Recommendations 01/2020 on measures to supplement transfer tools to ensure the level of protection of personal data under Union law, version 2.0

There are also obligations to inform data subjects if data is to be transferred to a third country or an international organisation (Art. 13 para. 1 lit. f and 14 para. 1 lit. f GDPR).

Authorisations already granted remain valid in principle (Art. 46 (5) first sentence GDPR).

ATTENTION: The so-called "Privacy Shield Decision" was declared **invalid** by the decision of the ECJ of 16 July 2020, C-311/18. The ECJ based its decision essentially on the fact that the US legal system does not standardise a level of protection that is equivalent in substance.[106]

NOTE ON STANDARD DATA PROTECTION CLAUSES: The European Commission has issued "new" standard data protection clauses in Implementing Decision (EU) 2021/914. The clauses issued by the European Commission under the GDPR can only be used until 27 December 2022, after which they lose their validity.

Does the GDPR also apply to international organisations such as the UN, the OSCE, etc.?

It depends primarily on the agreement that the international organisation concludes with the respective (European) host state (host state agreement = international treaty). In most cases, international organisations undertake to comply with the laws of the country in which they are based - and therefore also with the GDPR. However, the agreements usually contain provisions on privileges and immunities of international organisations and their employees, such as in particular the inviolability of the official seat, immunity from state prosecution (i.e. also from procedural acts of the data protection supervisory authorities), etc.

---

dated 18 June 2021, available in German at https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[106] For detailed information on this, see the EDSA FAQs at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

e) Brexit

What impact will Brexit have on the transfer of personal data to recipients in the United Kingdom?

The United Kingdom voted to **leave the European Union** in a referendum on 23 June 2016 and left at the end of 31 January 2020. Prior to this, a **withdrawal agreement**[107] was signed, which came into force on 1 February 2020 and regulates key aspects of the United Kingdom's withdrawal from the European Union and the European Atomic Energy Community.

The Withdrawal Agreement provided for a transition period until 31 December 2020, during which EU law (and consequently also the GDPR) continued to apply in principle for the United Kingdom and in the United Kingdom. There were therefore no direct consequences for data transfer during this period.

Shortly before the end of the transition period, a **trade and cooperation agreement**[108] was negotiated between the European Union and the United Kingdom, which has been provisionally applied since 1 January 2021 and finally entered into force on 1 May 2021.

With regard to data protection law, the Trade and Cooperation Agreement contains a further **bridging solution**, according to which the transfer of personal data from the European Union to recipients in the United Kingdom **is not considered a transfer to a third country within the meaning of Union law for a maximum period of six months after its entry into force**. This is subject to the condition that the data protection law currently in force in the United Kingdom does not change during that period and that the United Kingdom does not exercise any of its new powers in this area during that period.

The **bridging solution ended at the end of 30 June 2021**.

---

[107] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, OJ L 2020/29, p. 7 as amended. L 2020/443,
S. 3.

[108] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ L 2020/444, p. 14.

However, the European Commission has previously issued **two adequacy decisions** (one for the GDPR and one for the GDPR-PJ) for the United Kingdom, which **came into force on 28 June 2021**. In principle, the European Commission has **certified that** the United Kingdom has an **equivalent level of protection** as the European Union. Personal data can therefore be transferred **unhindered** from the European Union to recipients in the United Kingdom on the basis of these two adequacy decisions.

However, it should be noted that data transfers carried out for the purposes of immigration control practised by the United Kingdom are currently excluded from the material scope of the adequacy decision for the area of GDPR!

Both adequacy decisions are also time-limited and expire four years after their entry into force. The European Commission will monitor the legal situation in the United Kingdom during the four-year period and can intervene at any time in the event of changes to the level of protection in the United Kingdom and suspend, amend or revoke the adequacy decisions if necessary. The period of validity of the two adequacy decisions can also be extended by the European Commission.

f) Proceedings before the data protection authority

In which language can I submit documents to the data protection authority or in which language are proceedings conducted?

All documents that the controller/processor or the complainant must submit to the data protection authority as part of a procedure must be written **in German** (official language pursuant to Art. 8 para. 1 of the Federal Constitution Act; see also the ruling of the Administrative Court of 17 May 2011, no. 2007/01/0389). If this is not the case, the data protection authority is not obliged to accept these documents. Complaints submitted in a language other than German will be rejected after unsuccessful rectification (see the decision of 21 September 2018, GZ DSB-D130.092/0002- DSB/2018).

The obligation to submit German-language documents applies **in any case** to the **data protection impact assessment** pursuant to Art. 35 GDPR, which must be submitted to the data protection authority as part of the "consultation" pursuant to Art. 36 GDPR, for example, as well as to the **record of processing activities** pursuant to Art. 30 GDPR, which will generally form the basis for the data protection impact assessment.

What fines can the supervisory authority impose and for what?

The GDPR provides for fines. The fines are to be imposed by the data protection authority as administrative penalties on companies (business entities) or individuals acting as data controllers or processors. The number of criminal offences (infringements) has been extended. Negligence is also punishable.

The high fines provided for in the GDPR are intended to create an opportunity to put even very high-revenue players in their place. The data protection authority will apply its sanctioning options in accordance with the principle of proportionality.

In certain cases, the data protection authority may also issue a formal warning instead of imposing a fine. However, this is only done in cases where the infringement is not considered to be particularly serious.

ATTENTION: There is no right for the data protection authority to only issue a warning in the event of a first offence!

Less serious violations of the provisions of the GDPR may result in a fine of up to 10 million euros (no minimum fine) or, in the case of companies, up to 2 per cent of the global annual turnover of the last financial year. The higher amount applies.

Serious violations of the provisions of the GDPR can result in a fine of up to 20 million euros (no minimum fine) or, in the case of companies, up to 4 per cent of the global annual turnover of the last financial year. The higher amount applies.

Some examples:

Infringement/violation	Maximum fine	so far (max. fine)

Disregard of DSB decision	€ 20.000.000,– or 4 % of sales.	€ 25.000,--
Violation of the right to information	€ 20.000.000,– or 4 % of sales.	€ 500,--
Violation of the right of cancellation	€ 20.000.000,– or 4 % of sales.	€ 500,--
Unlawful data storage	€ 20.000.000,– or 4 % of sales.	Not punishable by law
unauthorised international transfer	€ 20.000.000,– or 4 % of sales.	€ 10.000,--
Lack of data protection officer	€ 10.000.000,– or 2 % of sales.	Not punishable by law
Non-execution of DSFA/DPIA	€ 10.000.000,– or 2 % of sales.	Not punishable by law
Inadequate data security	€ 10.000.000,– or 2 % of sales.	€ 10.000,--
No processing directory	€ 10.000.000,– or 2 % of sales.	€ 10,000 (mandatory reporting)
Lack of parental consent	€ 10.000.000,– or 2 % of sales.	Not punishable by law
Non-cooperation with DPO	€ 10.000.000,– or 2 % of sales.	Not punishable by law

An appeal against the imposition of a fine may be lodged with the Federal Administrative Court.

As a small company, do I have to expect a fine of 20 million euros?

No. The basis for determining the amount of the fine is the specific offence and the economic capacity of the person responsible. Any penalty must be effective, **proportionate** and dissuasive.

What powers does the data protection authority have?

The supervisory authority has three types of powers:

- Investigatory powers (including the right to enter certain premises after prior notice)
- Remedial powers (these are powers that enable the supervisory authority to put an end to unlawful behaviour, e.g. by issuing specific orders or imposing fines of up to EUR 20 million or 4% of the total annual global turnover generated in the previous financial year)
- Authorisation and advisory powers

Is the DPO responsible for parliament (National Council, Federal Council, provincial parliaments)?

As a rule, there is no jurisdiction. Due to the separation of powers, there can be no supervision of legislation by an administrative authority.

In exceptional cases, especially if the parliamentary bodies act as administrative bodies (e.g. when managing their own employees), the DPO may be responsible.

13) Further reading

Status: September 2022 (alphabetical, non-exhaustive list) GDPR:

- *Ehmann/Selmayr* (eds.), General Data Protection Regulation: GDPR[2] (commentary)
- *Feiler/Forgó*, EU General Data Protection Regulation (commentary)
- *Gantschacher/Jelinek/Schmidl/Spanberger* (eds.), Commentary on the General Data Protection Regulation
- *Gola* (ed.), General Data Protection Regulation[2] (commentary)
- *Jahnel* (ed.), General Data Protection Regulation (commentary)
- *Kühling/Buchner* (eds.), General Data Protection Regulation[3] (commentary)
- *Knyrim* (ed.), Practical Handbook on Data Protection Law[4] (Practical Handbook)
- *Knyrim* (ed.), General Data Protection Regulation (Practical Handbook)
- *Paal/Pauly* (eds.), General Data Protection Regulation[3] (commentary)
- *Pollirer/Weiss/Knyrim/Haidinger*, GDPR (text edition)
- *Simitis/Hornung/Spieker* (eds.), Data Protection Law (Large Commentary)
- *Sydow* (ed.), European General Data Protection Regulation[2] (commentary)

DSG:

- *Bergauer/Jahnel*, GDPR and DSG[3] (text edition)
- *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG (Commentary)
- *Jelinek/Schmidl/Spanberger*, Data Protection Act (Commentary)
- *Pollirer/Weiss/Knyrim/Haidinger*, DSG[4] (text edition with explanations)
- *Thiele/Wagner*, DSG (Commentary)