The Bavarian State Commissioner
for Data Protection

Joint controllership

Orientation guide

Publisher:

The Bavarian State Commissioner for Data Protection 80538
Munich | Wagmüllerstraße 18
Phone: +49 89 21 26 72-0
E-mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Processor:

Dr Verena Guttenberg

Version 1.0 | Status: 1 June 2024

This guide is provided in electronic form only. It can be found on the Internet at https://www.datenschutz-bayern.de under the heading "Data protection reform 2018" can be accessed here.

The PDF file is optimised for double-sided printing.

Foreword

The General Data Protection Regulation (GDPR)[1] provides for various roles in connection with the processing of personal data. In addition to individual responsibility and commissioned processing, joint responsibility within the meaning of Art. 26 GDPR is of key importance. This legal concept covers the case where two or more controllers jointly determine the purposes and means of processing. In practice, this will often be the case with processing based on the division of labour, whereby different forms and characteristics of joint responsibility are conceivable.

If the requirements of Art. 26 para. 1 sentence 1 GDPR are met, the parties involved in the processing are categorised by law as joint controllers and are subject to the obligations under Art. 26 para. 1 sentence 2, para. 2 and 3 GDPR. In particular, they must conclude an agreement that specifies in a transparent manner which of them fulfils which obligations under the General Data Protection Regulation. Although this involves some effort for the parties involved, it has the advantage that the responsibilities and (partial) responsibilities under data protection law can be clearly distributed - an added value for both the parties involved and the data subjects.

In the area of Directive (EU) 2016/ 680[2] Art. 26 GDPR applies in a modified form in implementation of Art. 21 Directive (EU) 2016/680 in accordance with Art. 2 sentence 1 and Art. 28 para. 2 sentence 2 of the Bavarian Data Protection Act (BayDSG).

These explanations present joint responsibility in the light of case law, in particular that of the European Court of Justice, and provide recommendations for action by Bavarian public authorities. It shows that the legal concept is much more common than is generally assumed. The guidance aims to help reduce possible "fears of contact": Joint controllership may still seem less "familiar" than the long-established processing of orders (data). However, with the necessary knowledge in the background, it is not only a practical and manageable tool, but also a very helpful one.

[1] 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 (General Data Protection Regulation, OJ EU L 119, 4 May 2016, p. 1, corrected OJ EU L 314, 22 November 2016, p. 72, and OJ EU L 127, 23 May 2018, p. 2).

[2] 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 (OJ EU L 119, 4 May 2016, p. 89).

Foreword

Please observe the following instructions for use:

– Publications of the Bavarian State Commissioner for Data Protection cited in the guidance are - unless otherwise stated - available on the website https://www.datenschutz-bayern.de in the "Data Protection Reform 2018" section.

– If you have any queries or suggestions for improvement, please use the mailbox orientierungshilfen@datenschutz-bayern.de set up for this purpose.

Table of contents

Foreword 3

Table of contents 5

Standard texts 7

I. Introduction 9
1. Joint controllership - what is it? 9
2. History of origin 9
3. Fundamentals 12

II. Prerequisites for joint responsibility 14
1. Controller within the meaning of Art. 4 No. 7 GDPR 14
a) Category of the person responsible 15
b) Decision-making authority 16
aa) Decision-making authority by virtue of legal provisions 17
bb) Decision-making authority based on implied responsibility 18
cc) Subsidiary: actual influence 19
c) Decision alone or together with others 20
d) Decision on the purposes and means of processing 21
aa) Purposes 21
bb) Medium 21
cc) Decision on the purposes and means 22
dd) Specification of the purposes and means by Union law or the law of the Member States 22
e) Purposes and means of processing personal data 24
f) Obligations of the person responsible 25
2. Joint participation in decision-making (on the purposes and means) 26
3. Determination of purposes and means (in joint participation) 31

III. Examples of joint responsibility 34
1. Legally ordered cases 34
2. E-Government 35
3. Official federated files 35
4. Cooperations between universities and research institutions 36
5. Judicial cooperation between courts, judicial authorities and service providers 36
6. events 36
7. Use of social media and communication services 36
8. Other constellations 37
9. Negative examples 37

IV. Differentiation from other processor roles 39
1. Differentiation from individual responsibility and non-responsibility 39
2. Delimitation to order processing according to Art. 4 No. 8, 28 GDPR 39
3. Differentiation from forms of organisation under civil law for majority groups of persons 41
4. Differentiation from the figure of the so-called "transfer of function" 42

5. Differentiation from employee excess 42
6. Differentiation from the terms "recipient" and "third party" 45
7. Differentiation of the various roles 47

V. Legal consequences of joint responsibility 48
1. No legal basis within the meaning of Art. 6 para. 1 GDPR 48
2. No processing privilege 48
3. Applicability of special regulations 50
4. Obligation to conclude an agreement 51
a) Mandatory content of the agreement pursuant to Art. 26 para. 1 sentence 2, para. 2 sentence 1 GDPR 54
b) Specifications in the agreement 54
d) Agreements for mixed contractual relationships 59
e) Form of the agreement 59
f) Transparency 60
g) Time 61
5. Relationship between the joint controllers and the data subjects 61
a) Requirement of the agreement to adequately reflect the respective actual functions and relationships vis-à-vis the persons concerned, Art. 26 para. 2 sentence 1 GDPR 61
b) Duty to inform 62
c) Art. 26 para. 3 GDPR 64
6. Legal effects of the agreement 64
a) Mutual obligation and liability 65
b) Binding effect vis-à-vis third parties 65
aa) Binding effect vis-à-vis the persons concerned, especially Art. 26 para. 3 GDPR 65
bb) Binding effect vis-à-vis supervisory authorities 67

VI. Excursus: Directive (EU) 2016/680 (combating criminal offences) 70

VII. Conclusion 71

Standard texts

General Data Protection Regulation (extract)

Art. 26 Joint controllers

(1) [1]Where two or more controllers jointly determine the purposes and means of the processing, they shall be joint controllers. [2]They shall specify in a transparent manner in an agreement which of them fulfils which obligation under this Regulation, in particular as regards the exercise of the rights of the data subject, and which of them complies with which information obligations pursuant to Articles 13 and 14, unless and to the extent that the respective tasks of the controllers are laid down by Union or Member State law to which the controllers are subject. [3]The agreement may specify a contact point for data subjects.

(2) [1]The agreement referred to in paragraph 1 shall duly reflect the respective actual functions and relationships of the joint controllers vis-à-vis data subjects. [2]The substance of the agreement shall be made available to the data subject.

(3) Notwithstanding the details of the agreement referred to in paragraph 1, the data subject may assert his or her rights under this Regulation with and against any of the controllers.

Recital 79

In order to protect the rights and freedoms of data subjects and with regard to the responsibility and liability of controllers and processors, a clear allocation of responsibilities is required by this Regulation, also with regard to the monitoring and other measures of supervisory authorities, including in cases where a controller determines the purposes and means of processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

I.
Introduction

1. Shared responsibility - what is ?

With Art. 26, the General Data Protection Regulation has introduced rules for the case that 1
two or more entities determine the purposes and means of processing personal data. With these rules, it formulates a framework for the relationships between these so-called joint controllers and thus satisfies a need for regulation that has arisen as a result of the promotion of division of labour and networking in the processing of personal data, partly due to digitalisation. The division of labour in the processing of personal data can be intransparent for the data subjects if they can no longer understand the data flows. They are also
This is associated with increasing risks because the possibilities for access and thus misuse and the attack options are expanding (for example along transport routes or on additional IT systems). However, data subjects should not suffer any disadvantages as a result of cooperation between several controllers. According to EC 79 GDPR, it is always necessary to ensure a clear allocation of responsibility and liability in such a case. The General Data Protection Regulation takes this requirement into account in particular through the fundamental obligation of the joint controllers to conclude a corresponding agreement (Art. 26 para. 1 sentence 2, para. 2 GDPR).

2 Shared responsibility is mainly characterised by the assignment of obligations to comply with data protection regulations, in particular with regard to the rights of the data subject and the right to data protection.
of the data subjects. Whether joint responsibility exists must always be examined in a differentiated manner in relation to specific data records or processes. In practice, the assessment is not always easy, especially when differentiating between a majority of unconnected controllers and commissioned processing, and is associated with some effort for the parties, especially due to the obligation to conclude an agreement in accordance with Art. 26 para. 1 sentence 2, para. 2 sentence 1 GDPR. However, the advantages of joint responsibility in accordance with Art. 26 GDPR result from the clear regulation and allocation of data protection responsibilities and competences - an added value in terms of (liability) law both for the joint controllers themselves and for the data subjects affected by the data processing.

2. History of origin

Joint controllership in relation to the processing of personal data 3
This was first recognised as a specific data protection role during the legislative process.

I. Introduction

procedure for Directive 95/46/EC[3] (so-called Data Protection Directive):[4] Art. 2 letter d sentence 1 of Directive 95/46/EC, similar to the current Art. 4 No. 7 GDPR[5] that the decision-making authority required for classification as a "controller" can be exercised alone or jointly with others.[6] However, Directive 95/46/EC did not contain any specific provisions on the relationship between joint controllers; in particular, it did not regulate the liability of joint controllers towards the data subjects. The consequence of this was that the data subjects had to find out in each case, depending on the specific circumstances of the individual case, against whom liability claims existed - against each of the joint controllers or against only one of the controllers.[7]

4 Consequently, there were no more detailed provisions on joint controllership in the provisions of national law transposing Directive 95/46/EC. This applies in particular to the Federal Data Protection Act in the version applicable until 24 May 2018 (BDSG-old).[8] Accordingly, the specific requirements and legal consequences of joint responsibility under the old data protection law were unclear.[9]

5 The closest thing to a regulation on joint responsibility was Section 6 (2) BDSG - old on so-called interconnected systems - for cases of automated data storage in such a way that several bodies are authorised to store data. In this constellation, if the data subject was unable to determine which body had stored the data, they could contact any of these bodies. The body contacted was then

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ EC L 281 of 23 November 1995, p. 31).

4 On the history of its development, see Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 8 et seq.

5 Art. 4 No. 7 GDPR: "For the purposes of this Regulation: [...] No. 7 "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

6 Article 2(d) of Directive 95/46/EC: "For the purposes of this Directive [...] (d) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of the processing of personal data are determined by n a t i o n a l or Community laws, regulations or administrative provisions, the controller or the specific criteria for its nomination may be provided for by national or Community law".

7 Article 29 Working Party, Opinion 1/2010 on the terms "c o n t r o l l e r " and "processor", status 2/ 2010, WP 169, p. 27, Internet: https://ec.europa.eu/justice/article- 29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

8 Federal Data Protection Act in the version published on 14 January 2003 (Federal Law Gazette I p. 66), last amended by the Act of 30 October 2017 (Federal Law Gazette I p. 3618) with effect from 9 November 2017, expired on 25 May 2018 due to the Act of 30 June 2017 (Federal Law Gazette I p. 2097).

9 Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 17; Hartung, in: Kühling/Buchner, DSGVO - BDSG, 4th ed. 2024, Art. 26 GDPR para. 3.

If necessary, the data controller is obliged to forward the data subject's enquiry to the actual data controller and to inform the data subject accordingly. § However, Section 6 (2) BDSG-old only concerned the specific individual case described. For this reason, the legal concept of joint controllership was sometimes criticised in practice or completely doubted and ultimately hardly accepted in Germany;[10] Instead, contract processing or a transfer of functions was regularly used.

In addition to the general definition of

r

esponsibility in Art. 4 No. 7 GDPR, the General Data Protection Regulation has

now introduced special requirements for joint controllers in Art. 26 GDPR, thereby establishing a framework for the relationships between the parties involved. However, Art. 24 of the Commission's draft regulation submitted during the legislative process initially only stipulated that several controllers should coordinate with each other as to who has to fulfil which obligations under the regulation. No provision was made for the allocation of liability.[11] In its position on the Regulation, the European Parliament went further and demanded that the agreement reached between the controllers should reflect the actual circumstances and that the persons concerned should be made aware of this.[12] In addition, there should be joint and several liability in the event of ambiguities regarding responsibility.[13] The European Council's draft, which was then drawn up on this basis[14] was supplemented in the subsequent trilogue[15] was supplemented in the subsequent trilogue by a provision stating that data subjects can assert their rights under the Regulation against any one of several controllers.[16] The concept of "(joint) controller" has essentially not changed in comparison to Directive 95/46/EC.
The criteria for assigning data protection roles have also remained largely unchanged. However, the introduction of Art. 26 GDPR by the European legislator deliberately assigns a more prominent role to joint controllers than to data processors.

[10] See Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Status 5/2022, Art. 26 GDPR para. 13 with further references.

[11] Art. 24 in the version of the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Internet: https://eur-lex.europa.eu/legal-con- tent/DE/TXT/?uri=CELEX:52012PC0011.

[12] Art. 24 sentence 2 in the version of the European Parliament's position adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Internet: https://eur-lex.europa.eu/legal- con- tent/en/TXT/?uri=CELEX:52014AP0212.

[13] Art. 24 sentence 3 in the version of the European Parliament's position (fn. 12). This corresponded to a demand made by the European Data Protection Supervisor in his opinion on the data protection reform package of 7 March 2012, para. 183, Internet: https://edps.europa.eu/data-protection/our- work/publications/o- pinions/data-protection-reform-package_en.

[14] Council of the European Union, document 9565/15 of 15 June 2015, Internet: https://data.consilium.eu- ropa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

[15] See Joint Declaration on the practical arrangements for the new codecision procedure (Article 251 of the EC Treaty, OJ EU C 145 of 30 June 2007, p. 5).

[16] Council of the European Union, document 15039/15 of 15 December 2015, 15039/15, Internet: https://data.consilium.europa.eu/doc/document/ST-15039-2015-INIT/de/pdf.

to date.[17] This has significantly increased the level of protection for the data subjects and their data.

7 Since Art. 26 GDPR is of paramount importance for the effective protection of data subjects, it is not surprising that the European Court of Justice (ECJ) has been called upon several times in recent years to define joint responsibility in more detail: For example, the Court has clarified the understanding of the term "(joint) controller" as the addressee of data protection obligations since its judgement in the "Google Spain and Google"[18] continuously expanded, above all with the judgements in the cases " Wirtschaftsakademie Schleswig-Holstein"[19], " Jehovah's Witnesses"[20] and "Fashion ID"[21]. These decisions are of fundamental importance for the understanding of Art. 26 GDPR. In this respect, they offer important points of reference, even though Directive 95/46/EC was still the decisive factor in each case: the definition of "controller" has essentially been adopted by the new law. Under the same premise, an opinion of the Article 29 Data Protection Working Party from 2010 is still ngsweisend.[22]

3. Fundamentals

8 If two or more controllers jointly determine the purposes and means of processing, they are "joint controllers" pursuant to Art. 26 para. 1 sentence 1 GDPR. "joint controllers").

9 Note: Art. 28 Regulation (EU) 2018/1725[23] makes a far-reaching analogy to Art. 26 GDPR.
comparable regulation for the institutions of the European Union and their agencies, Corporations and Joint Undertakings. A special feature can be found in Art. 2 8 (1) sentence 1 of Regulation (EU) 2018/1725, according to which, within the framework of a joint The EU institutions and national authorities may also maintain relations with each other. are necessary: "If two or more persons in charge or one or more persons in charge are authorised to together with one or more persons in charge who are not bodies or institutions Union, they shall jointly determine the purposes and means of the processing.

17 Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Status 5/2022, Art. 26 GDPR para. 11.

18 ECJ, judgement of 13 May 2014, C-131/12.

19 ECJ, judgement of 5 June 2018, C-210/16.

20 ECJ, judgement of 10 July 2018, C-25/17.

21 ECJ, judgement of 29 July 2019, C-40/17.

22 Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 27. The Article 29 Working Party was an independent European working party established on the basis of Art. 30 Directive 95/46/EC and Art. 15 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2022 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 332, 12.7.2022, p. 1).
EC L 201 of 31 July 2002, p. 37) dealt with the protection of individuals with regard to the processing of personal data until it was replaced by the European Data Protection Board (EDPB) pursuant to Art. 68 GDPR when the General Data Protection Regulation came into force on 25 May 2018.

23 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21 November 2018, p. 39).

jointly responsible parties." In this case, however, with regard to the joint controllers The processing carried out under our responsibility fully fulfils the obligations under Regulation (EU) 2018/1725 for all actors.

Joint controllership is a separate legal concept in the role model of the

G

eneral Data Protection Regulation. However, it does not give the persons or bodies covered by it a separate legal personality.[24] This has consequences in several respects:

(1) The role of the "joint controllers" under data protection law is - as with 11
the further roles of "controller", "processor", "recipient" and "third party" - a functional concept of its own character: It aims to assign responsibilities according to the actual circumstances and independently of a formal designation (functional concept),[25] whereby the interpretation of the role characteristics must primarily be in accordance with EU data protection law (concept of its own character).

(2) Art. 26 GDPR does not provide a legal basis for joint controllership 12
processing operations; rather, the permissibility of the processing operations in question must result from other provisions. Insofar as a joint controller processes personal data within the scope of joint responsibility, it therefore requires a legal basis for this processing in accordance with Art. 6 para. 1 GDPR, and additionally in accordance with Art. 9 para. 2 GDPR when processing special categories of personal data.[26]

(3) Joint controllers are also recipients among themselves within the meaning of Art. 4 13
No. 9 GDPR, which is why the transfer of personal data between joint controllers constitutes an independent processing operation within the meaning of Art. 4 No. 2 GDPR and as such requires its own legal basis.[27]

[24] Radtke, Joint responsibility under the GDPR, 2021, p. 429.

[25] Opinion of Advocate General Emiliou of 4 May 2023 in case C-683/21, para. 41.

[26] ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 96 f.

[27] ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 96 f.; Conference of Independent Federal and State Data Protection Authorities (DSK), Joint controllers, Art. 26 GDPR, Brief paper no. 16, status 3/2018, p. 1, Internet: https://www.datenschutzkonferenz-online.de/kurzpa- piere.html. For more details, see para. 124 et seq. below.

II. Requirements for joint responsibility

14 Categorisation as a joint controller within the meaning of Art. 26 GDPR comes into consideration if more than one actor is involved as a controller in determining the purposes and means of a processing operation. The General Data Protection Regulation does not recognise an upper limit regarding the possible number of controllers involved.

15 The starting point for the definition of "joint controllers" is the definition of "controller" in Art. 4 No. 7 GDPR.[28] Although the German language version uses different verbs ("entscheiden" and "festlegen") in Art. 4 no. 7 half-sentence 1 and Art. 26 para. 1 sentence 1 GDPR, other language versions do not recognise such differentiations.[29]

1. Controller within the meaning of Art. 4 No. 7 GDPR

16 Anyone who is to be a joint controller must also fulfil the requirements for a controller in isolation.[30] According to Art. 4 No. 7 half-sentence 1 GDPR
"'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

17 The concept of responsibility is generally understood broadly in order to ensure effective and comprehensive protection of data subjects.[31] Any person "who exerts an influence on the processing of personal data out of a legitimate interest and thus has a

[28] European Data Protection Board, Guidelines 07/2020 on the terms "controller" and "processor" in the GDPR, Version 2.0, as of 7/2021, para. 50, Internet: https://edpb.europa.eu/our- work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en; Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 7.

[29] For example, the English ("determine[s]"), French ("détermine[nt]") and Spanish language versions ("determine[n]").

[30] ECJ, judgment of 7 March 2024 (IAB Europe), C-604/22, para. 58, and ECJ, judgment of 5 December 2023, C-683/21, para. 41 with reference to ECJ, judgment of 29 July 2019, C-40/17, para. 74 (Fashion ID); European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 50; Lang, in: Taeger/Gabel, 4th edition 2022, Art. 26 GDPR - BDSG - TTDSG, para. 16. 50; Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 16. See also Radtke, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, p. 121, with explanations on the possibilities of the exceptional obligation of non-responsible persons (p. 160 ff.).

[31] Fundamental ECJ, judgment of 13 May 2014, C-131/12 (Google Spain and Google), para. 34. In connection with joint responsibility ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 28.

1. controller within the meaning of Art. 4 No. 7 GDPR

The person who "participates" in the decision on the purposes and means of this processing, i.e. contributes to the decision, is to be regarded as the controller.[32]

a) Category of Responsible

According to Art. 4 no. 7 half-sentence 1 GDPR, there is no restriction with regard to the

c

a t e g o r y of controller. 18 The controller may be a natural or legal person, public authority, agency or other body. The controller does not necessarily have to have legal personality.[33] The Bavarian Data Protection Act contains on the basic
In accordance with Art. 4 No. 7 half-sentence 2 GDPR, Art. 3 Para. 2 BayDSG specifies that the controller for the processing of personal data within the meaning of the General Data Protection Regulation within the scope of the Bavarian Data Protection Act is the public body responsible for the processing, unless otherwise specified. The determination of the Bavarian public bodies is generally derived from Art. 1 BayDSG. Special laws may contain deviating regulations.[34]

The General Data Protection Regulation does not distinguish between the public 19
and the non-public sector. This distinction is important because the national legislator can differentiate between public and non-public bodies in fulfilment of its regulatory mandates and regulatory options from the General Data Protection Regulation and subject different addressees to different regulations. For example, the Bavarian Data Protection Act contains regulations specifically for Bavarian public bodies, while the Federal Data Protection Act (BDSG) contains special regulations for federal public bodies and non-public bodies.

If the public sector body is an organisation, in

pr

actice20 the organisation as such is usually considered to be the controller, not a natural person or a specific unit within the organisation (such as the head or a member of the governing body or an employee).[35] Certain departments or units
organisational units of an organisation are to be classified as an independent public body under data protection law if the organisational unit is factually and/or personally independent with regard to the decision on the purposes and means of processing personal data, and if the transfer of personal data to other organisational units within the same authority is explicitly designed as a transfer.[36] "Legal entity" and "public body" within the meaning of the Bavarian Data Protection Act are therefore not always congruent. Natural persons can also be public bodies if they are other public bodies (Art. 1 para. 1 sentence 1 BayDSG, for example notaries) or

[32] ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 68.

[33] ECJ, judgment of 10 January 2024, C-231/22, para. 36.

[34] See only Section 67 (4) of the Tenth Book of the Social Code - Social Administrative Procedure and Social Data Protection (SGB X), Section 69 sentence 2 of the Federal Staff Representation Act, Section 27 sentence 1 of the Act on the Implementation of the Census in 2022 and Article 1 sentence 2 of the Act on the Implementation of the Civil Status Act (AGPStG).

[35] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 17.

[36] For example, the legally and functionally i n d e p e n d e n t Public Procurement Chamber South within the legal entity "Government of Upper Bavaria" or the Regulatory Chamber of the Free State of Bavaria with an office at the Bavarian State Ministry of Economic Affairs, Regional Development and Energy, cf. on the whole Engelbrecht, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 1 BayDSG, para. 13, 120 f.

insofar as they - in particular as authorised representatives - perform sovereign tasks of public administration (Art. 1 Para. 4 BayDSG, for example authorised district chimney sweeps).

21 This is to be distinguished from the case where public bodies designate a specific person or organisational unit to be responsible for carrying out a processing activity or to ensure compliance with data protection regulations. However, this natural person or organisational unit does not become the controller in the sense of data protection law as a result of the designation. Under data protection law, the public body remains the controller. However, it must accept responsibility for the actions of the designated person or organisation.

22 In general, and irrespective of any designation, those persons who have access to personal data within an organisation, i.e. in particular certain employees, are not considered "controllers", but rather "persons acting under the authority of the controller or processor" within the meaning of Art. 29 GDPR. They are therefore - not only, but in particular - subject to the controller's instructions with regard to data processing.[37] subject to the instructions of the controller. However, the General Data Protection Regulation does not define the term "employee". § Section 26 (8) BDSG defines employees as all employees, temporary workers, civil servants, judges, sol- dants, rehabilitants, trainees, volunteers of the federal or youth volunteer service, people working in workshops for the disabled, people working from home and all applicants. In the case of data transfer, the employees are not recipients of the data in accordance with Art. 4 No. 9 GDPR[38] and not third parties (Art. 4 No. 10 GDPR). Rather, the organisation and its employees form a single unit from a data protection perspective (for the special constellation of employee excess, see para. 101 et seq. below). The controller must ensure that appropriate technical and organisational measures are taken to ensure compliance with the General Data Protection Regulation in its area of responsibility.[39]

b) Decision-making authority

23 The body thus designated must "decide" in accordance with the definition in Art. 4 no. 7 half-sentence 1 GDPR. This means that it must exert influence on the processing itself by exercising decision-making authority, not merely on a preliminary stage of the processing.[40] The right to decide is to be understood in the sense of having the authority to decide on the purposes and means of processing . The decisive factor is therefore who decides on the specific processing operations.[41] Since the data protection law

[37] See Art. 29(2) GDPR: "[...] may process such data only on instructions from the controller, unless they are obliged to process them under Union or Member State law".

[38] ECJ, judgment of 22 June 2023, C-579/21, para. 73.

[39] In addition to the establishment of a corresponding organisational and technical role concept, training and information for employees, for example, can be considered.

[40] Opinion of Advocate General Emiliou of 4 May 2023 in case C-683/21, para. 32.

[41] The following questions can be helpful for the assessment: "Why is the processing taking place?", "Who initiated the processing?" and "Who benefits from the processing?", European Data Protection Supervisor.

1. controller within the meaning of Art. 4 No. 7 GDPR

Since the roles are functional concepts, this examination is based primarily on an analysis of the actual facts and not on formal aspects. The decisive factor is therefore who has the legal decision-making authority or - in the absence of legal regulations - at least the de facto responsibility for the processing in question. This also applies if the decision is made unlawfully or the data processing is carried out unlawfully. Only in this way can comprehensive protection of the data subjects be guaranteed.

It should be noted here: Access to the relevant processing 24
Data alone does not grant control in the sense of responsibility. Similarly, processing personal data yourself or having access to the data[42] or access to the data are prerequisites for being categorised as a controller.[43] Although this data access will usually exist in practice, it is not necessary. It is much more sufficient if a body influences the processing of personal data out of its own interest and thus participates in the decision on the purposes and means of processing.[44]

In practice, there are various conceivable 25
fundamentals. These are related to each other in stages.

(1) The decision-making power can result from explicit legal requirements - also in the law of the Member States.

(2) The decision-making authority can result from an implied (also: implicit) responsibility.

(3) Secondarily, the controller is determined by who actually decides on the purposes and means of processing.

aa) Decision-making authority by virtue of legislation

Art. 4 no. 7 half-sentence 2 GDPR expressly regulates the responsibility arising from 26
legal provisions. If the controller is explicitly or at least indirectly named in legal provisions, this is generally decisive for determining the controller. However, the prerequisite for this is that the corresponding Member State regulations also take sufficient account of the basic concept of the term "controller" within the meaning of Art. 4 no. 7 half-sentence 1 GDPR. They must therefore adequately reflect the actual circumstances of data processing, in particular with regard to the functions and relationships of the entities involved.[45]

Data Protection Officer, EDPS Guidelines on the concepts of "controller", "processor" and "processor". "Joint controllers" according to Regulation (EU) 2018/1725, status 11/2019, p. 7 f. with further references, Internet: https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts- controller-processor-and-joint_en.

42 ECJ, judgment of 5 December 2023, C-683/21, para. 35.

43 ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 69. In this sense, also ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 38.

44 ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 68, and judgment of 29 July 2019, C-40/17 (Fashion ID), para. 68.

45 Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 4 No. 7 GDPR, para. 26.

27 Decision-making powers of this kind are regulated by law in the public sector. In the case of purpose-related decision-making powers, this is based on the level of constitutional law; reservations under organisational law enshrined therein ensure that the state and its indirect legal entities may only act in the areas of life for which they are responsible, but may not usurp the areas of life of private individuals or companies. The central instrument for the realisation of such organisational-legal reservations are statutory and sub-statutory task assignments, which in the context of data protection law generally also convey decision-making powers with regard to the purpose of processing: An authority to which a law assigns a specific task is legitimised to determine the purpose of the related processing in relation to other authorities, private individuals or companies.

28 Note: The fundamental decision-making authority referred to here within the scope of the Responsibility is not to be confused with either an authorisation to process (such as Art. 4 Para. 1 BayDSG) or an authorisation to change the purpose (such as Art. 6 Para. 2 BayDSG).

29 However, task assignments do not always guarantee that a "beneficiary" body is also authorised to make decisions regarding the means of processing. Although this may be the rule, legal (fine) control is also possible here. Of particular interest in this respect are regulations relating to the allocation of material and personnel resources, as well as specifications on the organisational structure.

30 Note: If it has been established on the basis of Art. 3 Para. 2 and Art. 1 BayDSG that a specific Bavarian public body is the controller for a specific processing operation, no further examination of decision-making powers regarding the purposes or means of this processing is generally required. Deficits existing in this respect already have an effect on the qualifica
as a public body.[46]

31 Decision-making authority by virtue of legal provisions may also exist in the non-public sector; however, this constellation will not be discussed in detail here.

bb) Decision-making authority based on implied responsibility

32 If the responsibility under data protection law is neither explicitly nor indirectly derived from legal provisions, implied (or also: implicit) responsibility may be considered. This group of cases describes the situation in which the decision-making authority can be derived from general statutory provisions or applicable legal practice in specific areas of law (e.g. civil law, commercial law or labour law).[47] In this case, the data processing authorisation for data processing

[46] Engelbrecht, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2nd ed. 2024, Section 2 BDSG marginal no. 7 (forthcoming).

[47] Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 13; Jung/Hanusch, Die Verantwortlichkeit in der DSGVO und ihre praktischen Auswirkungen, ZD 2019, pp. 143, 147. According to Radtke, Gemein- same Verantwortlichkeit unter der DSGVO, 2021, p. 112, and European Data Protection Board, Leitlinien

1. controller within the meaning of Art. 4 No. 7 GDPR

Responsible for traditional tasks/functions and professional expertise which usually imply a certain level of responsibility.

In the public sector, such implied responsibility regularly collides with the requirement of a legal (authorisation) basis (for an organisational decision) in accordance with the principle of the reservation of the law and therefore plays a minor role at best. In contrast, this construct can be used in the non-public sector in individual cases. 33
This may well justify the derivation of responsibility under data protection law.

Example: Typical case groups are the processing of personal data of employees
The data may be collected from employees by their employer, from subscribers by a publisher or from members or contributors by an association.

This means that a specific function outside of data protection allows the 34 role of the controller under data protection law. From a purely legal point of view, this applies regardless of whether the authority to decide has been transferred to the body in question and whether it is exercised by suitable persons or organisational units acting on behalf of the body in question.

cc) Subsidiary: actual influence

In the event that none of these assignments of responsibility exist, the categorisation of an actor as the controller must 35

b

e decided by assessing the actual circumstances of the processing. All relevant factual circumstances must be taken into account to determine the necessary determining i n f l u e n c e . The role
The categorisation of the controller thus results from specific activities in a specific context, whereby the categorisation must be made in each case with regard to specific data processing operations or specific series of operations and can lead to different results with regard to different parts of a processing operation.

The following can be used as reference points for the valuation: 36

– the social or (civil) legal role of the organisations involved;

– any contractual provisions between the various parties involved. A contract can formulate the contracting parties' view of the identity of the controller or at least provide corresponding indications. However, the parties to the contract cannot dispose of the allocations of responsibility contained in the General Data Protection Regulation and allocate or exclude responsibility with effect against external parties if a different allocation results from the actual circumstances;

07/2020 (fn. 22), para. 25, such traditional roles can only be taken into account when examining the actual circumstances.

- the degree of control actually exercised by a party. It should be taken into account that access to data alone does not grant control and is not an essential prerequisite for categorisation as a controller;[48]
- the impression conveyed to the persons concerned;
- the legitimate expectations of the persons concerned due to this external impact. This category is particularly important as it enables responsibility to be assigned even in cases of unlawful behaviour.[49]

37 Determining responsibility on the basis of actual influence requires a complex analysis of the facts of life in question, which may well be necessary in individual cases. At the same time, it harbours a greater risk of divergent interpretations.

Example (non-public area): SWIFT[50] (= Society for Worldwide Interbank Financial Telecommunication Organisation, which operates a particularly secure telecommunications network)

SWIFT made the decision to provide certain personal data - which had originally been processed on behalf of financial institutions for commercial purposes - also for the purposes of combating the financing of terrorist activities after being requested to do so by the US Treasury Department by administrative act. SWIFT was formally regarded as a processor of the data, but by providing the data it was actually acting as a controller.

38 If none of the described bases for responsibility are relevant, there is also no responsibility under data protection law within the meaning of Art. 4 No. 7 GDPR. In particular, a purely formal designation of a controller without the actor concerned being able to influence the purposes and means of processing personal data, at least on the basis of the actual circumstances, has no legal effect[51] - an entity that has neither legal nor factual influence on the decision as to what and how personal data is processed cannot be considered a controller. This also applies in the event that a body has expressly objected to the processing of personal data.[52]

c) Decision alone or together with others

39 Art. 4 no. 7 clause 1 GDPR provides that the decision on the purposes and means of processing may be taken "alone or jointly with others", i.e. by one or more than one actor. Different entities can therefore act as controllers for one and the same processing, whereby each of them must comply with the applicable data protection law.

[48] Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 27. On the non-requirement of data access ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 69. In this sense also ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 38.

[49] Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 15.

[50] Example according to Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 11.

[51] ECJ, judgment of 5 December 2023, C-683/21, para. 34.

[52] ECJ, judgment of 5 December 2023, C-683/21, para. 37.

is subject to protection provisions. In practice, various forms and combinations of joint participation are conceivable, see para. 77 et seq. below.

d) Decision on the purposes and means of processing

The following aspect of the definition of the controller in Art. 4 No. 7, first half-sentence of the GDPR refers 40
refers to the object of its influence, the "purposes and means" of processing. According to Art. 5 para. 1 lit. b GDPR, personal data may in particular only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes (principle of purpose limitation). Furthermore, the processing must be lawful, fair and transparent for the data subject, Art. 5 (1) (a) GDPR (principle of lawfulness, f a i r processing, transparency). Determining the purposes of the processing and the means of achieving them is therefore of particular importance.

aa) Purposes

The term "purpose" describes the objective associated with a specific processing operation 41
is to be pursued and achieved. It is sufficient if it is merely an indirect objective that is derived from an overriding interest, such as the proper fulfilment of public tasks or the pursuit of economic objectives.[53] Non-economic purposes are not to be treated differently from economic purposes, although they are less similar. This is important in the context of joint responsibility, specifically with regard to the question of whether "joint decisions are made on purposes and means".[54]

The planned measures required are based on the purpose as the expected result 42
from:

bb) Medium

The "means" refers to the way in which a result or objective is achieved. On the

o

ne hand, this43 includes the resources used for the processing in question as well as the necessary technical and organisational measures. On the other hand, it relates specifically to the personal data processed, its type and scope and the specific form of processing.

[53] ECJ, judgement of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 34, and judgement of 29 July 2019, C-40/17 (Fashion ID), para. 80. Purposes may also include the objectives and modalities of a processing operation and the associated development, Opinion of Advocate General Bot of 24 October 2017 in Case C-210/16, para. 47 et seq.

[54] para. 56 et seq.

cc) Decision on the purposes and means

44 The decision required to establish responsibility must cumulatively cover both the purposes pursued and the means used for processing; the authority to decide on only one of the two aspects is generally not sufficient. The wording of Art. 4 No. 7 half-sentence 1 GDPR is clear in this respect.[55]

45 Note: In the context of order processing, there may be a certain amount of room for manoeuvre for the processor to make independent decisions regarding the processing. In this respect, the following applies: Decisions on the purpose of processing are always reserved for the controller. When deciding on the means of processing, on the other hand, a distinction can be made between essential (closely related to the purpose and scope of processing and thus to its lawfulness, necessity and proportionality) and non-essential means (relate more to the purpose and scope of processing).[56]) and non-essential means (relate more to practical aspects of data processing[57]) can be differentiated: The decision on essential means is also reserved to the controller due to its fundamental importance;[58] However, a processor can decide on non-essential means on its own responsibility,[59] whereby the controller must continue to ensure and be able to prove that the processing in question is carried out in accordance with the General Data Protection Regulation, Art. 5 para. 2 and Art. 24 GDPR.[60]

dd) Specification of the purposes and means by Union law or the law of the Member States

46 Art. 4 no. 7 clause 2 GDPR provides that the Union legislator or the legislator of a Member State may, within the scope of their respective legislative competence, specify the purposes and means of processing. Once this has been done, the respective legislator can either directly determine who is to be regarded as the controller or specify the criteria for determining the controller. Irrespective of this, the legislator can also, in accordance with Art. 26 para. 1 sentence 2 at the end

[55] See only European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 36. Different view still Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 23, which considered the alternative existence of either a joint decision on the purpose or means of data processing to be sufficient.

[56] For example, the type of personal data processed, the duration of processing, access to the data (access control lists, user profiles, etc.), the categories of recipients and the categories of data subjects.

[57] These include individual technical and organisational issues such as the choice of specific hardware or software or the detailing of security measures.

[58] Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 17.

[59] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 80.

[60] The controller must - taking into account the type and scope of the data, the circumstances and purposes of the processing as well as the risks to the rights and freedoms of data subjects - determine and define the technical and organisational measures that are generally required for processing in individual cases and, if necessary, oblige the processor by means of corresponding provisions in the contract processing agreement, possibly by granting a certain degree of discretion.

GDPR, the respective tasks of the joint controllers are defined by legal provisions.[61]

47 Once the purposes and means of processing have been specified, the determination of the legal The decision by the controller on the basis of Art. 4 No. 7, second half-sentence GDPR also includes the decision in favour of joint responsibility.[62] This is already apparent from the wording and context of the provisions regarding controllers in the General Data Protection Regulation: Although Art. 4 no. 7, second half-sentence GDPR itself only refers to "[the] controller", numerous obligations of the General Data Protection Regulation, which also refer to the controller in the singular, also apply to joint controllers on the basis of Art. 26 para. 1 sentences 1 and 2 GDPR, for example Art. 12 ff. or Art. 33 f. GDPR. GDPR. Otherwise, joint controllership would never come into consideration if the purposes and means of data processing were specified by law. The core requirement of "joint determination of the purposes and means of processing by two or more controllers" could no longer be fulfilled, or only to a limited extent. The exclusion of this group of cases from joint controllership cannot have been the intention of the Union legislator and would also contradict the principle of the most comprehensive possible protection of the fundamental rights and freedoms of natural persons (Art. 1 (2) GDPR).

In practice, a legal definition of the purposes and means of processing is used in the public sector in particular when public bodies are assigned certain tasks. The specifications regarding the purposes and means of processing can be very far-reaching and bind the controller. This does not, however, preclude liability with regard to Art. 6 para. 1 subpara. 1 lit. c GDPR does not preclude liability.

Examples: For example, the registration law stipulates extensive requirements with regard to the processing of registration data, which leave the local authorities responsible for the registration system very little room for manoeuvre. Cf. only § 3 BMG regarding the data to be collected and Art. 3 Para. 1 of the Bavarian Law on Registration, Passport and Identity Cards regarding the restriction of the bodies to which data processing tasks can be transferred. The data protection officer and the works council[63] are also subject to strict legal limits for the purposes of processing.

It should be noted here: The legislative definition of purpose and the d efinition of purpose to be made by the res ponsible party differ significantly due to the different requirements for the concreteness of the definition of purpose. For example, the legislator does not have to expressly characterise the purpose it has defined as such, but must
The specific purpose must only be recognisable with "sufficient" certainty. For

[61] See below para. 78, 132.

[62] Radtke, Joint responsibility under the GDPR, 2021, p. 105 f.

[63] State Commissioner for Data Protection and Freedom of Information Baden-Württemberg, Activity Report Data Protection 2018, p. 37 f., Internet: https://www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht/. Other opinion Jung/Hansch, Die Verantwortlichkeit in der DSGVO und ihre praktischen Auswirkungen, ZD 2019, p. 143, 147; Kranig/Wybitul, Sind Betriebsräte für den Datenschutz selbst verantwortlich? ZD interview, ZD 2019, p. 1 f.

The purpose definition by the controller, on the other hand, is governed by Art. 5(1)(b) GDPR, which requires a "specific" purpose for the protection of the data subject affected by the data processing, which clearly focuses on and describes the task of data processing in the individual case. This requirement is flanked by provisions that are linked to this narrow purpose, such as Art. 5 para. 1 letter a GDPR (principle of transparency) and the principles of data minimisation, accuracy and storage limitation (Art. 5 para. 1 letters c to e GDPR) as well as the obligation to provide information on the purpose of processing in accordance with Art. 13 and 14 GDPR. As a result, the controller is therefore obliged to specify the purpose of processing in accordance with Art. 5 (1) (b) GDPR, despite the purpose being stated in the law.[64]

50 As seen (para. 18), the Bavarian state legislator has made use of the power to legally designate the controller in accordance with Art. 4 No. 7 half-sentence 2 at the end of the GDPR in Art. 3 para. 2 BayDSG. The purposes and means of processing to be determined as a prerequisite for the designation of the controller result from the respective (technical) legal assignment of tasks, as well as possible deviating assignments of responsibility.

e) Purposes and means of processing of personal data

51 The purposes and means defined by the controller must ultimately relate to the "processing of personal data". Art. 4 no. 2 GDPR defines the processing of personal data as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means". The term "controller" can therefore be linked either to a single processing operation or to a series of operations; accordingly, the decision-making authority and thus responsibility can extend to the entire processing in question, but can also be limited to a specific processing step.[65]

52 It is not necessary for the controller to have actual access to the processed data in order to decide on the purposes and means of such processing.[66]

53 An actor is also considered a "controller" for the processing if they process personal data unknowingly or by mistake. This ensures the most comprehensive protection possible for the data subjects.

[64] On the whole, Spies, Zweckfestlegung der Datenverarbeitung durch den Verantwortlichen, ZD 2022, p. 75 et seq. See also Schantz, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2021, Art. 5 GDPR para. 14.1; Herbst, in: Kühling/Buchner, DSGVO - BDSG, 4th ed. 2024, Art. 5 GDPR para. 35.

[65] ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 74.

[66] ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 69. In this sense, ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 38.

f) Duties of the person responsible at

Once the responsible party has been determined according to the above criteria, he or she is subject to

54

principle of accountability pursuant to Art. 5 para. 2 GDPR. The controller must ensure that

– the material provisions on the admissibility of the processing of personal data are complied with (Art. 5 para. 2 GDPR), in particular the processing principles pursuant to Art. 5 para. 1 GDPR;

– the procedural requirements of the General Data Protection Regulation are observed; this applies, for example, to

  - the maintenance of the record of processing activities in accordance with Art. 30 GDPR,
  - the reporting and notification obligations in the event of personal data breaches in accordance with Art. 33 and 34 GDPR,
  - carrying out data protection impact assessments in accordance with Art. 35 GDPR and Art. 14 BayDSG and
  - the requirements of Art. 28 GDPR when engaging a processor;

– the data protection information obligations under Art. 13 and 14 GDPR in conjunction with Art. 9 BayDSG are observed;

– the rights of the data subjects are respected, for example

  - the right to information in accordance with Art. 15 GDPR,
  - the right to erasure in accordance with Art. 17 GDPR and
  - the right to object pursuant to Art. 21 GDPR;

– appropriate technical and organisational measures are taken to protect the processed data (Art. 24 para. 1 and Art. 32 GDPR), for example in the form of data protection guidelines or other data protection instructions;

– the processing operations are documented with records (to prove compliance with the principle of accountability) (specific concretisations within the General Data Protection Regulation, for example for consent Art. 7 para. 1 GDPR).

If a public body is the controller within the meaning of Art. 4 No. 7 GDPR, it must

fu

lfil these55 various obligations. In this respect, the organisational representative of the public body is generally responsible, in the case of municipalities, for example, the first mayor in accordance with
Art. 37 of the Municipal Code for the Free State of Bavaria. The latter can make a deviating regulation and assign the fulfilment of data protection obligations to a specific office within its organisation; however, not generally to the data protection officer.[67]

[67] For example, Bavarian State Ministry of the Interior, for Sport and Integration, working aids for the practical implementation of the General Data Protection Regulation, Directive (EU) 2016/680 (Directive on the

However, this does not constitute a delegation of responsibility; the public body remains the controller in accordance with Art. 4 No. 7 GDPR due to Art. 3 para. 2 BayDSG in the sense of a guarantee responsibility and must ensure, monitor and prove the fulfilment of data protection obligations through its organisational representative, Art. 5 para. 2 GDPR.

2. Joint participation in the decision (on the purposes and means)

56 The (individual) controllers determined in accordance with these requirements must be jointly involved in the decision on the purposes and means of processing as an essential prerequisite for joint controllership.

57 The term "jointly" is to be understood as "together with" or "not alone".[68] In practice, joint participation can take various forms and combinations and must therefore be assessed on the basis of an actual, not a formal, analysis of the contributions to responsibility in each individual case.[69] For example, joint participation may take the form of a joint decision by two or more entities or result from converging decisions by two or more entities on the purposes and means of processing.[70] Coordination or co-operation is not required,[71] It is sufficient if the processing would not be possible without the involvement of both parties and the parties are aware of the "causal contributions" of the others and approve them (see para. 62 below). In contrast to commissioned processing, there is no hierarchical division of decision-making power over data processing in the case of joint controllership.

Datenschutz bei Polizei und Justiz) and the Bayerisches Datenschutzgesetz für bayerische öffentliche Stellen, status 3/2022, No. 4 Muster einer Datenschutz-Geschäftsordnung, Internet: https://www.stmi.bayern.de/sus/datenschutz/arbeitshilfen/index.php. For the role and position of the data protection officer, see Bavarian State Commissioner for Data Protection, Der behördliche Datenschutzbeauftragte, Orientierungshilfe, Stand 5/2018.

68 European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 51.

69 Strauß/Schreiner, Gemeinsame Verantwortung: Der Vertrag zur getrennten Verantwortung - Rechtsklarheit bei Unklarheit, DSB 2019, pp. 96, 97, take the view that a corresponding contractual arrangement can create the conditions for separate responsibility and avoid the impression of a joint decision on the purposes and/or means of processing from the outset. In order to ensure that separate responsibility is contractually agreed, it should be made clear that the purpose of the data processing in question is not jointly determined. For example, it could be made explicitly clear that the purpose of the data processing is determined unilaterally by the transmitting controller in such a way that the receiving controller cannot influence this decision. For reasons of comprehensive data subject protection, however, such an approach is only possible if the contractual arrangement is also reflected in the actual circumstances.

70 ECJ, judgment of 5 December 2023, C-683/21, para. 43.

71 Opinion of Advocate General Emiliou of 4 May 2023 in case C-683/21, para. 43.

2. joint decision on the purposes and means

Joint participation by way of a joint decision means

th

at58 two or more entities make a joint decision in relation to data processing and there is a joint intention to do so.

Decisions regarding the purposes and means of a data protection programme can be 59 processing if they complement each other and are necessary for the processing in such a way that they have a significant influence on the determination of the purposes and means of the processing.

Example: A religious community, together with its members acting as preachers, was to be considered in the case law as joint controllers on the basis of converging decisions, since the community participated in determining the purposes and means of data processing in the context of the door-to-door preaching activity by organising and coordinating the activities of its members, which contributed to achieving the objective of the religious community.[72]

60 Other aspects of the (business) relationship between the several players, for example of an economic nature such as the agreement of (utilisation) fees, are not included in this respect. must be taken into account. An important criterion for the determination of converging decisions is thus: Processing would not be possible without the participation of several parties in the determination of their purposes and means in the sense that the decisions of both parties are inseparable, i.e. inextricably linked.[73] It is sufficient to exert influence out of self-interest, i.e. the pursuit of one's own economic purposes, if the economic advantage pursued by one entity is "the quid pro quo" for the advantage "offered" by another entity.[74] The decisive factor is that the own purposes pursued can actually be pursued within the joint control, i.e. they must be decisive for the implementation of the processing in its concrete form.[75] These criteria result in particular from the case law of the European Court of Justice.[76]

[72] Facts of the "Jehovah's Witnesses" case, ECJ, judgment of 10 July 2018, C-25/17.

[73] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 54 f. Confirming Opinion of Advocate General Emiliou of 4 May 2023 in Case C-683/21, para. 38.

[74] ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 68, and judgment of 29 July 2019, C-40/17 (Fashion ID), paras. 68, 80. Parts of the literature consider the pursuit of economic purposes that are not congruent with each other to be critical, Kremer, Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung? CR 2019, p. 225, 227; Lee/Cross, (Joint) responsibility when using third-party content on websites, MMR 2019, p. 559, 561 f., also with reference to non-commercial organisations. However, this view is based on the - erroneous - premise that non-commercial purposes are not also worthy of recognition. But see para. 72.

[75] Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Status 5/2022, Art. 26 GDPR para. 29.

[76] ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 70 et seq. and facts of the case "Fashion ID", ECJ, judgment of 29 July 2019, C-40/17.

II Prerequisites for joint responsibility

61 Joint participation within the meaning of Art. 26 para. 1 sentence 1 GDPR does not require an equal or unanimous decision by several actors.[77] Nor is (participation in) control in rem over the processed data or the means used for data processing a mandatory requirement.[78]

62 In practical terms, this means that if one of the bodies involved provides the means for the processing of personal data by other bodies, another body that decides to use the provided means for processing is also involved in determining the means for this processing.[79] However, the prerequisites for this are at least knowledge of the overall circumstances and tacit approval of the purposes and means or the corresponding contributions of the respective other bodies involved.[80] There must be a deliberate and conscious act.[81] Any active action or causal enabling is sufficient for this[82]that indicates a corresponding will is sufficient. For example, the acceptance of conditions of use or the utilisation of the IT infrastructure provided, for example by integrating a plugin.[83] In individual cases, it may even be sufficient if one party determines the purposes and means of processing personal data in advance and the other party agrees to this afterwards;[84] "accession" for the past is not possible.[85] The exercise of a formative influence through content-related specifications is not required; a mere contributory causality for the data processing[86] However, mere joint causality for the data processing or a purely necessary actual cooperation are not sufficient; in particular, when using a joint data processing system or a joint

77 Opinion of Advocate General Bot of 24 October 2017 in Case C-210/16, para. 61 f; Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 29; Dovas, Joint Controllership - Möglichkeiten oder Risiken der Datennutzung?, ZD 2016, pp. 512, 513. This position corresponds to the opinion of the Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 23.

78 Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 40. Compare the facts of the cases Wirtschaftsakademie Schleswig-Holstein, ECJ, judgment of 5 June 2018, C-210/16, and Fashion ID, ECJ, judgment of 29 July 2019, C-40/17.

79 ECJ, judgement of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 40, and judgement of 29 July 2019, C-40/17 (Fashion ID), para. 77.

80 ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 73, and judgment of 29 July 2019, C-40/17 (Fashion ID), para. 77. The knowledge element must extend to the own enabling act, the enabled processing in its concrete form and the causal enabling context. This is sometimes referred to as the "subjective element", Lurtz/Schindler, comment on ECJ, judgment of 29 July 2019 - C-40/17 (Fashion ID), VuR 2019, p. 468, 474; Spittka/Mantz, Datenschutzrechtliche Anforderungen an den Einsatz von Social Plugins, NJW 2019, p. 2742, 2744. Being able to or having to know is also sufficient little more than a vague idea of possible processing, Hanloser, comment on ECJ, judgement of 29 July 2019, ZD 2019, p. 455, 459.

81 Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 21.

82 Hanloser, comment on ECJ, judgment of 29 July 2019, ZD 2019, p. 455, 459.

83 Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 60. For the plugin, see the facts of the "Fashion ID" case, ECJ, judgment of 29 July 2019, C-40/17.

84 DSK, Brief Paper No. 16 (fn. 27), p. 3.

85 DSK, Short Paper No. 16 (fn. 27), p. 3. Critical Kartheuser/Nabulsi, Abgrenzungsfragen bei gemeinsam Verant- wortlichen, MMR 2018, p. 717, 719. For future processing, however, other controllers may be added, provided that all parties involved jointly determine the purposes and means of processing with a view to the future.

86 Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 19.

2. joint decision on the purposes and means

The prerequisites for joint responsibility are checked on a case-by-case basis in the data processing structure.[87]

Note: In practice, it can be very difficult to prove knowledge of and authorisation for the specific processing that is possible in individual cases, but this can be decisive for data protection disputes. It is recommended that public bodies provide unambiguous documentation of the joint decisions. 63

As with sole responsibility, all parties must have access to the processed data. 64
personal data[88] or the participation of all parties in a processing[89]
not absolutely necessary.

The existence of joint controllership does not necessarily require

th

e65 same level of responsibility or degree of involvement of the different entities involved in a processing operation.[90] Rather, the European Court of Justice has clarified
The GDPR recognises that different actors may be involved in the processing of personal data at different stages and to varying degrees.[91] The responsibility of each of them must be assessed taking into account all relevant circumstances of the individual case, with the reference point being the specific process or the specific series of processes.

Beyond the individual cases that have been decided, the decisions of the European Court of Justice 66
However, the European Court of Justice does not provide any generally applicable standards for the necessary degree of influence. An overall view of the case law of the European Court of Justice shows that the requirements for the assumption of joint responsibility are rather low overall and will often be met in practice in cases of division of labour. The parties involved in a possible joint responsibility are therefore recommended to carry out a detailed examination of the individual circumstances of the case and, in case of doubt, to assume joint responsibility rather than deny it.[92]

The question of the scope of joint responsibility must be distinguished

fro

m67 the question of any gradual responsibility[93] - The General Data Protection Regulation does not provide for this. A lesser degree of cooperation within the framework of joint responsibility therefore does not lead to a reduction in responsibility in the external relationship and is at most relevant in the internal relationship, Art. 26 para. 3 and Art. 82 para. 4 GDPR.

87 European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 68.

88 ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 69, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 69, and judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 38.

89 ECJ, judgment of 5 December 2023, C-683/21, para. 35.

90 ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 66, and judgment of 29 July 2019, C-40/17 (Fashion ID), para. 70.

91 ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 66, and judgment of 29 July 2019, C-40/17 (Fashion ID), para. 70. In this sense, also ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), paras. 28, 43 and 44.

92 For the delimitation of the various roles, see para. 89 et seq. below.

93 Lang, in: Taeger/Gabel, GDPR - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 71.

II Prerequisites for joint responsibility

68 The joint decision does not have to be made in any particular form, in particular not in writing.

69 If there are several processing operations in which several bodies are involved, the examination of their responsibility under data protection law must be carried out very carefully:

Examples:

(1) Individual responsibility - Each actor determines the purpose and means for each processing operation individually: Transmission of employee data to tax authorities - A public sector organisation collects and processes personal data of its employees for the purpose of managing remuneration, business trips, health insurance, etc. The public sector organisation is legally obliged to transmit all remuneration-related data to support tax supervision. The public body is legally obliged to transmit all compensation-related data to the competent tax authorities in order to support tax supervision. In this case, although the public body and the tax authorities process the same data on remuneration, the two organisations are classified as two separate controllers due to the non-common purposes and means of data processing.

(2) Joint responsibility - delimitation of upstream and downstream processes. - Fashion ID, an online retailer of fashion items, had integrated the Facebook "Like" plugin into its website, as a result of which user data was collected and transmitted to Facebook when the website was accessed. The European Court of Justice clarified that the operator of a website is generally responsible for all processing of personal data of the users of its website, even if it is not carried out by the operator itself. Without the integration of the plugin, the processing of user data by Facebook would not be possible.[94] Consequently, the operator of the website is also responsible for the collection and transmission of the data. However, upstream and downstream processes in the processing chain for which the website operator determines neither the purposes nor the means, such as the further processing of the data exclusively by Facebook, do not fall under its responsibility.[95]

(3) Shared responsibility - At the "micro level", the various processing operations in a chain appear to be independent of each other, for example because each of them has a different purpose; at the "macro level", however, the processing operations are to be regarded as a "series of operations" with which a common purpose is pursued by jointly defined means: Financial transactions.[96] - A bank uses a transmitter of financial messages to carry out its financial transactions. The bank and the intermediary agree on the means of data processing. The processing of personal data in connection with the financial transactions is initially carried out by the bank for the purpose of executing the transactions themselves and only later by the financial messaging service for the purpose of preparing and publishing financial messages to fulfil disclosure and transparency obligations under stock exchange and capital market law. Although each of the actors pursues its own purposes at the micro level,

94 ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 85.

95 ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 74, 76.

96 Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 25.

the various phases and the purposes and means of processing are closely linked at macro level. In this case, the bank and the transmission service can be regarded as joint controllers.

3. Definition of purposes and means (in joint participation)

The point of reference for the joint participation of the multiple entities in the joint responsibility is the determination of the purposes and means of processing. In this respect, the decisions must also cumulatively[97] the purposes and means. 70

The jointly defined purposes may be the same purposes. However, according to the case law of the European Court of Justice, closely related or complementary purposes are also sufficient, provided that they are derived from the same purpose. 71

overriding interest.[98] The European Court of Justice allows a mutual benefit in the form of an economic advantage for the parties involved to suffice.[99] However, this must represent a direct benefit from the specific processing that each of the entities involved must derive and that goes beyond mere financial compensation.[100] The mere existence of a mutual benefit is not sufficient.

Insofar as non-economic purposes are pursued, these are to be treated no differently than economic purposes. Nevertheless, non-economic and economic purposes are less similar to each other, so that their linkage or complementarity should be examined in more detail. must.[101] 72

[97] This follows from the wording of Art. 26 para. 1 sentence 1 GDPR and with regard to EC 79 GDPR. See also Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 21a; Piltz, in: Gola/Heckmann, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3rd ed. 2022, Art. 26 GDPR para. 4; Petri, in: Simi- tis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 GDPR para. 12 with reference to the history o f the standard. Likewise European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 53. In contrast, the Article 29 Working Party still assumed an alternative understanding (praeter propter), Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 23.

[98] ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 34. Other opinion Moos/Rothkegel, comment on ECJ, judgment of 29 July 2019, C-40/17, MMR 2019, p. 579, 585 f., who deny the sufficient concretisation of the data processing required for the plugin provider's knowledge in the case of an autonomous decision by the website operator to integrate a plugin, as the plugin provider does not know the data to be processed with the plugin.

[99] ECJ, judgement of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 34, and judgement of 29 July 2019, C-40/17 (Fashion ID), para. 80.

[100] See ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 80. Hanloser, comment on ECJ, judgment of 29 July 2019, ZD 2019, p. 455, 459; Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 57 does not want to place too high demands on this requirement against the background of ECJ case law.

[101] Radtke, Joint responsibility under the GDPR, 2021, p. 193.

II Prerequisites for joint responsibility

73 If an entity involved in the processing does not pursue its own purpose, but merely provides services, it acts as a processor and not as a joint controller.

74 Since, as seen, different entities may be involved in different phases of a processing operation and to different degrees, not every entity involved must determine all means in every case for joint controllership to exist. Different joint controllers may determine the means of processing to different degrees, depending on who is actually in a position to do so.[102] The General Data Protection Regulation does not require participation in the material control of the processed data or the means used for processing.[103] This can go so far that one of the entities involved provides all the means for processing and makes them available for the processing of personal data by other entities; another entity that decides to use these means for processing is then also involved in determining the means for processing.[104] This scenario is particularly relevant for platforms, standardised tools and other similar infrastructures.

Joint participation …

- ▶ Joint decision
- ▶ Converging decisions

… in the decision …

… about the purposes …

- ▶ the same purposes
- ▶ closely related or complementary purposes of an economic or non-economic nature with the same overriding interest

  [no separate purpose: order processing]

… and means of processing personal data

- ▶ Each body involved determines all means
- ▶ Determination to varying degrees
- ▶ One entity provides all the resources and makes them available for processing, the other entity participates in the decision by deciding to use the resources

75 However, the use of a shared data processing system or a shared infrastructure does not necessarily mean that the actors involved are recognised as a single entity.

[102] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 63.

[103] Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 40. On the non-requirement of data access ECJ, judgement of 10 July 2018, C-25/17 (Jehovah's Witnesses), In this sense, also ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie S c h l e s w i g - H o l s t e i n), para. 38, 40, and judgment of 29 July 2019, C-40/17 (Fashion ID), para. 77, 82. See above para. 61.

[104] Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Status 5/2022, Art. 26 GDPR para. 39. See above para. 62.

are to be regarded as joint controllers. An argument against such a categorisation may be, for example, that the processing carried out in each case is separable and could be carried out by one entity without the intervention of the other, or if the provider of the processing means is a contract processor in the absence of its own pursued purpose.

Example (non-public sector):[105] If a travel agency transfers personal data of its customers to an airline and a hotel chain on a case-by-case basis in order to book a package holiday, each of the parties processes the data for its own activities and by its own means. The travel agency, airline and hotel are three different individual controllers.

The situation is different if a travel agency, hotel chain and airline decide to set up a joint internet platform for the common purpose of offering package holidays. In this case, the parties jointly determine for what purpose and by what means the personal data of their respective customers are processed and are therefore jointly responsible for processing in connection with the joint online booking platform. However, each of them retains sole control over other processing activities outside the joint online booking platform. platform.

Alternatively, if several bodies determine only the purposes or means of processing in accordance with Art. 76

joint, there is no joint responsibility. In the case of a joint decision only on non-essential means of processing, the requirements for commissioned processing must be examined (recital 92 et seq.).

[105] Example according to European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 68.

III. Examples of joint responsibility

77 The requirements of joint responsibility are often present in practice. At the same time, the forms of joint cooperation are diverse. In the following, some examples of joint responsibility with particular relevance for the public sector are presented:

1. Legally ordered Cases

78 In some cases, the joint responsibility or its design ng is regulated by special legislation (see Art. 4 no. 7 half-sentence 2 and Art. 26 para. 1 sentence 2 GDPR).[106] For example, statutory monitoring obligations with regard to data processing by subordinate bodies can lead to joint responsibility in this regard;[107] but not pure legal or technical supervision. A legal provision in the Member States on the organisation of joint responsibility within the meaning of Art. 26 para. 1 sentence 2 at the end of the GDPR can be found in Section 307 para. 5 sentences 2 and 3 of the Fifth Book of the German Social Code - Statutory Health Insurance - (SGB V). According to this, it is the task of gematik (originally Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) to set up a coordinating body that provides data subjects with general information on the telematics infrastructure and information on responsibilities within the telematics infrastructure and, in particular, on responsibility under data protection law. With regard to the provision of information by this coordinating body and the associated processing of personal data, gematik is jointly responsible under data protection law with the data controllers named in Section 307 (1) to (4) SGB V.[108]

79 As far as can be seen, however, there is no provision in German law that is compatible with both Art. 4 no. 7 half-sentence 2 GDPR with regard to the allocation of joint responsibility as well as with Art. 4 no. 7 half-sentence 1 GDPR.

[106] Neither the legal basis nor previous case law shows that joint responsibility requires the cumulative existence of both conditions. Therefore, surprisingly, CJEU, judgment of 10 January 2024, C-231/22, para. 49: "national law may establish j o i n t responsibility of several actors in a chain of processing operations involving the same personal data, provided that the various processing operations are linked by the purposes and means laid down by national law and that national law lays down the respective obligations of each joint controller" [emphasis added]. It remains to be seen how case law will develop in this respect.

[107] For the non-public sector, for example, Section 25a (1) of the German Banking Act.

[108] See SG Munich, judgement of 26 January 2023, S 38 KA 72/22, BeckRS 2023, 2607, para. 64. See also para. 132 below. gematik can also be a subsidiary independent controller under data protection law for the processing of personal data in the telematics infrastructure in accordance with Section 307 (5) sentence 1 SGB V.

also makes use of Art. 26 para. 1 sentence 2 at the end of the GDPR with regard to the specific organisation of joint responsibility.[109]

2. E- Government

A typical application of joint responsibility is the joint management of a company's 80 platforms, databases and projects[110]see also EC 92 GDPR and Art. 37 para. 1 sentences 2 and 3 of the Bavarian Digital Act. This includes e-government solutions of the public administration with portals that can be used to communicate with each other and/or with citizens,[111] such as online services of the Citizens' Registration Office regarding residence registration or vehicle deregistration. For example, Section 11 of the Act on the Promotion of Electronic Administration (E-Government Act - E GovG)[112] on the basis of Art. 26 GDPR, the requirements for so-called "common procedures", i.e. automated procedures that allow several controllers within the meaning of Art. 26 GDPR[113] enable the processing of personal data in or from a database.[114] In individual cases, electronic mailboxes may also be included.[115]

3. Official Federated files

In addition to order processing relationships,

j

o i n t

re

sponsibility81 also

of

ten plays a role in authority federated files.

Al

l participating authorities usually enter data and are authorised to access or retrieve it at the same time.
One authority is generally responsible for the technical and organisational operation, the

[109] Ingold, in: Sydow/Marsch, DSGVO - BDSG, 3rd ed. 2022, Art. 26 GDPR para. 6 claims a n e e d f o r regulation for complex constellations, in particular in connection with the use of internet communication services.

[110] For example, the commissioning of a mobile application to manage the COVID-19 pandemic through an IT tool to collect and monitor the data of persons who have been in contact with carriers of SARS-CoV-2 by a public body with purpose definition and parameterisation by the latter, s e e CJEU, judgment of 5 December 2023, C-683/21.

[111] Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 26; also DSK, Short Paper No. 16 (fn. 27), p. 4 f.; Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 3.

[112] E-Government Act of 25 July 2013 (BGBl. I p. 2749), last amended by Article 1 of the Act of 16 July 2021 (Federal Law Gazette I p. 2941) has been amended.

[113] Joint responsibility within the meaning of Art. 26 GDPR is a prerequisite. § Section 11 EGovG thus makes no use of the opening clause of Art. 4 No. 7 half-sentence 2 GDPR. For the specific allocation of tasks, Section 11 (3) EGovG also refers to the requirements of Art. 26 GDPR, namely paragraphs 1 and 2. The legislator also does not make use of the opening clause in Art. 26 (1) sentence 2 at the end of the GDPR, but leaves the organisation of the cooperation to the public bodies involved in individual cases.

[114] See the explanations in the legislative materials, Draft Act on the Promotion o f Electronic Administration and on the Amendment of Further Provisions, BR printed matter 557/12 of 21 September 2012, p. 63,

Internet: https://www.bundesrat.de/DE/dokumente/dokumente-node.html.

[115] On the electronic court and administrative mailbox VG Wiesbaden, decision of 27 January 2022, 6 K 2132/19.WI.A, BeckRS 2019, 58431.

The other participating authorities are each responsible for the permissibility of the entry and the accuracy of the data they enter. However, responsibility is often also governed by special legislation, for example for INPOL (police information system) in Section 13 in conjunction with Sections 29 and 31 (2) of the Act on the Federal Criminal Police Office and Federal and State Co-operation in Criminal Police Matters (Federal Criminal Police Office Act - BKAG)[116].

4. Cooperations between universities and research institutions

82 If universities and research institutions work together with a joint data set, a joint definition of the purposes and means indicates a joint responsibility for the processing. The situation is different if the respective project partners are independently responsible for distinct parts of the research and the associated data processing.

5. Judicial cooperation between courts, judicial authorities and service providers

83 Cooperation between courts, judicial authorities and service providers can also give rise to joint responsibility in individual cases.[117]

6. events

84 If several public bodies jointly organise an event and process personal data of the event participants in this context, for example for the registration or documentation of the event, the participating bodies act as joint controllers within the meaning of Art. 26 GDPR.

7. Use of social media and communication services

85 If a public body, as a user of social media and/or communication services, actively influences a data processing operation, for example by parameterising it[118]integration of a plugin[119] or simply by actively operating a user page

[116] Federal Criminal Police Office Act of 1 June 2017 (BGBl. I, p. 1354; 2019 I p. 400), which was last amended by Article 3 of the Act of 19 December 2022 (Federal Law Gazette I p. 2632; 2023 I No. 60).

[117] Engeler, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, Section 22 Data Protection in the Judiciary para. 31.

[118] See facts of the case "Wirtschaftsakademie Schleswig-Holstein", ECJ, judgement of 5 June 2018, C-210/16.

[119] See facts of the "Fashion ID" case, ECJ, judgment of 29 July 2019, C-40/17.

or a channel, and if it pursues common overriding purposes together with the platform operator, such as increasing reach and/or interaction, joint responsibility of the entities is to be affirmed.[120] However, the mere creation of a user account does not establish joint responsibility,[121] only the subsequent active operation of the user account.

8. Other constellations

86If a public body grants access to protected personal data in its possession in accordance with the data governance act and this data is not anonymised before access is granted, the public body and the re-user will become joint controllers within the meaning of Art. 26 GDPR with access to the data.
the common overriding interest of "further use of the data".[122]

9. Negative examples

However, not all types of partnership, cooperation or collaboration fulfil

th

e87 requirements of joint responsibility. A case-by-case analysis is decisive in each case.

There is no joint responsibility in the following cases, for example: 88

– Exchange of the same data or the same set of data between two entities without jointly specified purposes or jointly specified means of processing;

  Example: Transmission of employee data to a tax authority;

– Use of a shared database or shared infrastructure, whereby each of the utilising bodies determines its own purposes independently;

  Example: Marketing measures in a group of companies that use a shared database;

– successive processing of the same personal data by different entities in a processing chain, where each of these entities pursues an independent purpose and uses independent means in its part of the chain;

  Example: Supply of data for a statistical analysis for a task in the public interest;

[120] On design options State Commissioner for Data Protection and Freedom of Information Rhineland-Palatinate, Framework for the use of "social media" by public bodies, status 3/2020, Internet: https://www.datenschutz.rlp.de/de/themenfelder-themen/soziale-netzwerke/.

[121] ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 35.

[122] See Bayerischer Landesbeauftragter für den Datenschutz, Daten-Governance-Rechtsakt, Orientie- rungshilfe, Stand 5/2024.

III Examples of joint responsibility

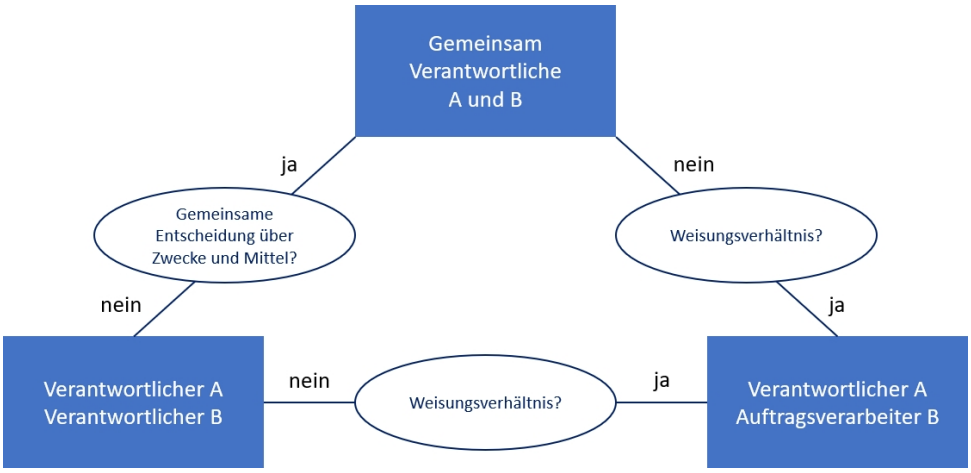
- Utilisation of a third-party professional service of a person subject to professional secrecy, e.g. doctors, tax consultants, lawyers. A joint decision-making process between a client and a professional secrecy holder is opposed by the latter's professional duties, as he acts independently, on his own responsibility and without instructions.[123]

[123] Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Status 5/2022, Art. 26 GDPR para. 76 f.

IV. Differentiation from other processor roles

The distinction between joint responsibility and other forms of responsibility is particularly i

mportant in view of the subsequent legal consequences and conceivable sanctions
89. The following explanations are intended to provide assistance in this respect.
tions.



1. Differentiation from individual responsibility and non-responsibility

Joint controllership differs from individual controllership i

n that several persons or bodies determine the purposes and means of processing. For joint controllers on the basis of Art. 26 GDPR, the following then apply
for details of requirements that go beyond the obligations of individual controllers, see para. 128 et seq. below.

If, on the other hand, there is no decision-making authority at all regarding the purposes or ess

ential means of processing, a corresponding responsibility under data protection law must also be denied (non-responsibility). Examples of this are employees or customers.

2. Differentiation from order processing in accordance with Art. 4 No. 8, 28 GDPR

"Order processing" within the meaning of data protection law refers to the processing of personal data. 92

of personal data by a natural or legal person separate from the controller.

person, public authority, agency or other body acting on behalf of the controller ("auxiliary data processing function"[124]), see Art. 4 No. 8 GDPR.[125]

– Particularly in the case of multi-level data processing processes based on the division of labour, the delimitation of joint responsibility can sometimes cause considerable difficulties.[126] However, the exact determination of the role and the subsequent classification in the data protection role model is mandatory, as the actors are each subject to a different programme of obligations. Classification as a (joint) controller or as a processor always depends on the circumstances of the individual case and must be assessed on the basis of the criterion of authority to decide on the purposes and means of processing personal data in relation to specific data records or processing operations. The European Court of Justice considers the person who influences the data processing out of their own interest to be the controller,[127] even if the processing of personal data is not the main or primary object of a process[128]. The exception for processors to independently decide on non-essential means of processing must always be taken into account, see para. 44.

– If a body is subject to the mandate and instructions of another with regard to data processing, it acts as a processor within the meaning of Art. 4 No. 8, 28 and 29 GDPR. In this case, the lawfulness of this processing in accordance with Art. 6 and, if applicable, Art. 9 GDPR is derived from the legal basis on which the controller itself bases the processing of personal data in question. As a rule, no further legal basis is required for the transfer of personal data to the processor or for the processing by the processor (privileged status of commissioned processing). The processing must be carried out on the basis of a contract or other legal instrument under Union law or the law of the Member States, Art. 28 para. 3 GDPR. The processor may only process the data in accordance with the instructions of the controller, Art. 29 GDPR, and may not carry out any processing for its own purpose(s), Art. 28 para. 10 GDPR. If the instructions of the controller are exceeded in violation of the data protection principles[129] the processor is deemed to be the controller in relation to this processing and may be subject to sanctions for exceeding the controller's instructions. Authorised processing beyond the scope of the data protection principles specified in the

[124] VG Bayreuth, decision of 8 May 2018, B 1 S 18.105, BeckRS 2018, 9586, para. 49; AG Mannheim, judgement of 11 September 2019, 5 C 1733/19 WEG, BeckRS 2019, 26873, para. 23.

[125] On the whole Bavarian State Commissioner for Data Protection, Order Processing, Guidance, status 4/2019.

[126] If an order processing agreement does not meet the minimum requirements, in particular with regard to the obligation to follow instructions, deficiencies can turn into joint responsibility in individual cases, Bergt, Wann ist eine Auftragsverarbeitung eine Auftragsverarbeitung?, DuD 2023, p. 169.

[127] ECJ, judgment of 10 July 2018, C-25/17 (Jehovah's Witnesses), para. 68, and judgment of 29 July 2019, C-40/17 (Fashion ID), para. 68.

[128] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 83.

[129] European Data Protection Supervisor, EDPS Guidelines on the concepts of "controller", "p r o c e s s o r " and "joint controller" under Regulation (EU) 2018/1725 (fn. 41), p. 18.

purposes does not, however, make the processor and the client joint controllers within the meaning of Art. 26 para. 1 sentence 1 GDPR

Order processing can also be carried ou t on behalf of joint controllers. The obligations of the joint controllers in connection with the commissioned processing are then to be included in the obligations of the joint controllers pursuant to Art. 26 para. 1 sentence 2 GDPR,
(2) GDPR to be included in the agreement. The aspects of the internal relationship between the joint controllers in relation to order processing should also be regulated, for example internal procedures and cooperation obligations.

3. Differentiation from forms of organisation under civil law for majority groups of persons

The distinction between jointly responsible parties and organisational for ms under civil law for gr oups of persons, such as partnerships under civil law within the meaning of Section 705 of the German Civil Code (BGB) or associations pursuant to Sections 21 et seq. BGB,
it is true that joint controllership in itself does not constitute such a majority of persons regulated under civil law, nor does the agreement on joint controllership required under Art. 26 para. 1 sentence 2, para. 2 sentence 1 GDPR, as they merely fulfil or shape the legal requirements of Art. 26 GDPR. If joint responsibility automatically corresponded to a specific legal figure under civil law, Art. 26 GDPR would be largely empty. Furthermore, as described in recital 77 et seq., various forms of cooperation between joint controllers are conceivable. These will very often consist of different tasks or even successive activities and less in aligned decisions.

However,97 if several controllers involved in data processing - irrespective of the requirements of Art. 26 para. 1 sentence 2, para. 2 sentence 1 GDPR - contractually undertake to pursue a specific purpose with their processing contributions or to promote a common processing purpose and determine general (civil law) rights and obligations in this context, a new assignment subject may be created (such as an association or a civil law partnership).[130] This assignment subject can then also solely assume the role of the controller within the meaning of Art. 4 No. 7 GDPR - in such a case, there is no room for joint responsibility of the members or shareholders. Whether the co-responsible parties have entered into such a contractual agreement is irrelevant for the specific case.
individual case.

[130] Hanloser/Koglin, in: Koreng/Lachenmann, Formulhandbuch Datenschutzrecht, 3rd ed. 2021, VI. Multi-party agreement between jointly responsible parties for online offers, Note 7.

4. Differentiation from the figure of the so-called "Function transfer"

98 The so-called transfer of functions was a German speciality. Under previous data protection law, a "transfer of functions" was assumed to be a transfer of personal data to third parties in the course of outsourcing a "function" or task instead of commissioned data processing, which goes beyond the outsourcing of data processing as such and in which the recipient is granted at least a certain degree of decision-making leeway with regard to the fulfilment of the task. In this case, the entity assuming the "task" was considered to be responsible in its own right; joint responsibility was usually hardly ever assumed in this context.[131]

99 Under the General Data Protection Regulation, there is no longer any room for this type of delegation of functions. The processor roles of the data protection role model are exhaustive.

100 In public law, tasks can be transferred in accordance with organisational law rules (e.g. by special purpose agreement, Art. 7 para. 2 sentence 1 of the Act on Municipal Cooperation - KommZG, or when establishing a special purpose association, Art. 17 para. 1 KommZG). However, such measures can now only be implemented in the processor roles of the General Data Protection Regulation under data protection law, just like other processing operations that were previously assessed in Germany as a so-called transfer of functions.

5. Differentiation from the employee excess

101 The terms "employee excess", "employee excess" or "excess" are used to describe constellations in which employees of those responsible use data that they are only authorised to access for official purposes for purely private purposes. In other words, they exceed their official authorisations for private reasons. Examples of this are particularly common in the police or hospital sector[132] public, as well as so-called "curiosity enquiries" using the Bavarian public authority information system (BayBIS).

102 The question now is what the legal (data protection) consequences of such a breach are.[133] The decisive factor here is who is responsible under data protection law within the meaning of Art. 4 No. 7 GDPR for the data protection breach.

103 The two Bavarian supervisory authorities - the Bavarian State Commissioner for Data Protection and the Bavarian State Office for Data Protection Supervision - represent

[131] On the whole DSK, short paper no. 16 (fn. 27), p. 2. On the old legal situation also Petri, in: Simitis, Bundesdaten- schutzgesetz, 8th ed. 2014, § 11 BDSG Rn. 22.

[132] Bavarian State Commissioner for Data Protection, 30th Activity Report 2020, No. 12.10, Internet: https://www.datenschutz-bayern.de, section "Activity Reports".

[133] Dieterle, Sanktionierung von Neugierabfragen im öffentlichen Dienst, ZD 2020, p. 135 et seq.

unanimously take the view that an employee does not become a controller within the meaning of Art. 4 No. 7 GDPR if he or she retrieves data that is available to him or her for business purposes for private purposes using business query systems:[134]

This is because the controller within the meaning of Art. 4 No. 7 GDPR is only the person who decides on the purposes and means of processing personal data. The decisive factor here is the decision on the fundamental purposes and means of the query systems. However, an employee does not decide on these even if they misuse official data for private purposes. Rather, he merely uses the query systems made available to him and these for private, non-official purposes that do not coincide with the purposes of the employing public body.[135] 104

For Bavaria, Art. 3 para. 2 BayDSG also expressly stipulates, on the basis of the specification option contained in Art. 4 no. 7 half-sentence 2 GDPR, that the controller for the processing of personal data within the meaning of the General Data Protection Regulation is the public body responsible for the processing - i.e. not an employee of this body. 105

Furthermore, a comparison with the provisions on commissioned processing in the General Data Protection Regulation also speaks in favour of this result: Art. 4 No. 8, 29 GDPR stipulate that a processor may only act on behalf of and on the instructions of a controller. It is not authorised to determine the purposes and (essential) means of data processing. In the event that a processor unlawfully exceeds its authorisations, Art. 28 para. 10 GDPR expressly stipulates that it is to be regarded as its own controller within the meaning of Art. 4 no. 7 GDPR. However, the General Data Protection Regulation, specifically Art. 29 GDPR, does not contain a corresponding provision on the personal responsibility of (public authority) employees for data processing for private purposes. It can therefore be assumed that it did not intend to stipulate such personal liability for employees acting unlawfully. 106

Finally, according to Art. 23 para. 1 no. 1 lit. c BayDSG in Bavaria, anyone who accesses personal data that is not in the public domain without authorisation or obtains it for themselves or another person from files may be subject to a fine or even a prison sentence (paragraph 2). In particular, data from registers whose access requires a legitimate interest, such as registration register and vehicle registration data, are not in the public domain. This offence of imposing a fine makes it possible to penalise inquisitive enquiries by officials without further ado. 107

The public body thus remains individually responsible within the meaning of Art. 4 No. 7 GDPR in the case of merely improper data retrieval, even for the data protection breach by its employee; joint responsibility is not established - in particular due to a lack of congruence of purpose. 108

[134] Bavarian State Office for Data Protection Supervision, 9th Activity Report 2019, p. 71 f., Internet: https://www.lda.bayern.de/de/taetigkeitsberichte.html.

[135] Due to the use of funds provided for official purposes, the budgetary exception of Art. 2 para. 2 lit. c GDPR does not apply, Ambrock, Mitarbeiterexzess im Datenschutzrecht, ZD 2020, pp. 492, 495.

IV. Differentiation from other forms of responsibility

109 The situation is different if the employee processes the retrieved data using external employer resources.[136] From this point onwards, Art. 4 No. 7 GDPR applies to the employee and the employee is individually responsible for the further processing of the data, with all the associated data protection obligations.

110 The unlawful retrieval of officially accessible data for purely private purposes constitutes a data protection offence for which a fine can generally be imposed on the controller in accordance with Art. 83 GDPR. However, Art. 22 BayDSG contains a special provision for public bodies as controllers under data protection law, according to which fines can only be imposed on them if they participate in competition as companies.[137] The employee acting unlawfully, on the other hand, can be fined in accordance with Art. 23 BayDSG. In the case of further processing of the data by the employee, the imposition of a fine against the employee pursuant to Art. 83 GDPR may even be considered as an alternative and, if the data is passed on to third parties, public officials may even be liable to prosecution.[138]

111 However, the problem of "employee excess" has not yet been conclusively clarified in legal terms. The Bavarian view on this is not shared by some other supervisory authorities: The state data protection officers in Baden-Württemberg and North Rhine-Westphalia, for example, consider the employee who uses official data for private purposes to be a data controller within the meaning of Art. 4 No. 7 GDPR.[139] In their opinion, the imposition of a fine pursuant to Art. 83 GDPR against the employee personally is therefore possible in such cases and the unauthorised access to data constitutes a breach of the protection of personal data by an - in this respect - unauthorised third party that must be reported pursuant to Art. 33 para. 1 GDPR. The Austrian Federal Administrative Court has ruled accordingly in the individual case of an unauthorised query[140] and the opinions of the European Data Protection Board and the European Data Protection[141] and the

[136] Bavarian State Office for Data Protection Supervision, 9th Activity Report 2019, p. 71 f., 10th Activity Report 2020, p. 78 f. and 13th Activity Report 2023, p. 43, Internet: https://www.lda.bayern.de/de/taetigkeitsberichte.html.

[137] For more details, see Bayerischer Landesbeauftragter für den Datenschutz, Geldbußen nach Art. 83 Datenschutz- Grundverordnung gegen bayerische öffentliche Stellen, Aktuelle Kurz-Information 17.

[138] The criminal offences of § 203 para. 2 (violation of private secrets), § 353b (violation of official secrecy and a special duty of confidentiality) and § 332 para. 1 of the Criminal Code (bribery) should be considered.

[139] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, LfDI Baden-Würt- temberg verhängt erstes Bußgeld gegen Polizeibeamten, press release dated 18 June 2019, Internet: https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten/, and 35th Activity Report 2019, p. 41, Internet: https://www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht/; Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen, 26th Activity Report for 2020, p. 143 ff., Internet: https://www.ldi.nrw.de/berichte.

[140] Federal Administrative Court (Austria), decision of 21 December 2021, W258 2238615-1/16E, BeckRS 2021, 50637. This is - as far as can be seen - the first decision on this issue by a court in German-speaking countries.

[141] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 88: "Insofar as the employee processes personal data for his own purposes which are different from those of his employer, he is then considered to be the controller and assumes all the consequences and obligations arising therefrom in relation t o the processing of personal data." The European Data Protection Board restricts this only slightly in footnote 34 above as follows: "The employer (as the original controller) could still retain some responsibility if the new processing is not authorised due to a lack of adequate safeguards.

Data protection conference[142]. The European Court of Justice has not yet ruled on the issue.

6. Differentiation from the terms "recipient" and "third party"

In the role model of the General Data Protection Regulation, in addition to the processor roles, there are 112

In addition to the roles of "controller", "joint controller" and "processor", there are also the roles of "recipient" and "third party". However, unlike controllers, joint controllers and processors, the General Data Protection Regulation does not stipulate any specific obligations for these roles. Rather, these terms serve to describe a data protection relationship with a (joint) controller or processor from a specific perspective.

Art. 4 no. 9 sentence 1 GDPR defines "recipient" as a natural or legal person, public authority, agency or other body to whom personal data are disclosed, whether or not it is a third party. The definition of recipient therefore includes anyone who receives personal data. If a controller transfers personal data to another entity, be it a joint controller[143]a processor or a third party, this entity is the recipient. Employees of an organisation are generally not recipients.[144] An entity that receives data is in turn considered a controller for any processing that it carries out for its own purposes after it has received the data. 113

A more differentiated approach must be taken for public authorities: Public authorities can also be recipients of data in accordance with Art. 4 No. 9 sentence 1 GDPR. However, with regard to Art. 4 no. 9 sentence 2 GDPR, this does not apply in the event that they receive personal data as part of a specific investigation mandate under Union law or the law of the Member States. 114

safety measures are taken." Critical in this respect Dieterle, comment on Federal Administrative Court (A u s t r i a), decision of 21 December 2021, W258 2238615-1/16E, ZD 2022, p. 439, 440, due to the lack of binding effect of the guidelines.

142 DSK, Companies are liable for data protection violations by their employees! - Resolution of the 97th Conference of the Independent Federal and State Data Protection Supervisory Authorities on 3 April 2019, p. 1, Internet: https://www.datenschutzkonferenz-online.de/entschliessungen.html with reference to the functional concept of a company under European primary law and the resulting principle of functional responsibility, whereby attribution in the sense of corporate liability should be excluded in the event of an excess. Such an excess is deemed to exist if the action of an employee cannot be attributed to the scope of the respective (entrepreneurial) activity upon reasonable judgement. Thus, if an employee "only" exceeds his internal powers, he is not acting in excess if this is objectively done to promote the economic interests of the company, Ambrock, Mitarbeiterexzess im Datenschutzrecht, ZD 2020, p. 492, 493. Only in exceptional cases can excesses be attributed to the company, for example if the management approves the behaviour, Ambrock/Karg: in Bussche v. d./Voigt, Konzern- datenschutz, 2nd ed. 2019, Part 8 para. 102. Depending on the case constellation, there is then joint r e s p o n s i b i l i t y in accordance with Art. 26 GDPR.

143 See para. 124 et seq.

144 ECJ, judgment of 22 June 2023, C-579/21, para. 73, see also para. 22.

Member States (e.g. tax and customs authorities, financial investigation offices, etc.), see also EC 31 GDPR.

115 The term "third party" is primarily used to differentiate from other actors. According to Art. 4 No. 10 GDPR, a third party is a natural or legal person, public authority, agency or other body outside the controller's or data subject's sphere of responsibility. According to the negative definition of Art. 4 No. 10 GDPR, a third party is not the data subject, the controller, the processor or persons who are authorised to process personal data under the direct responsibility of the controller or the processor. The designation
In this context, "controller" also includes joint controllers with regard to Art. 4 No. 7 half-sentence 1 GDPR.

116 However, the General Data Protection Regulation does not explain the definition of "persons who are authorised to process personal data under the direct responsibility of the controller or processor". The European Data Protection Board understands this to mean persons "who are part of the legal entity of the controller or processor (i.e. who are employees or have a role that is highly comparable to that of employees, for example temporary workers), but only to the extent that they are authorised to process personal data."[145] According to this view, employees who are given access to data to which they should not actually have access and use it for purposes other than those of the employer are therefore not covered; rather, they should be regarded as third parties.[146] The same must apply to employees who do not work for an organisation but for themselves, for example as a publicly appointed expert.

117 In summary, the term "third party" in the data protection role model therefore describes the actor who has no specific legitimisation or authorisation to process personal data, i.e. the typical "outsider". A third party who - lawfully or unlawfully - receives personal data is generally a new controller, provided that the other requirements of Art. 4 No. 7 GDPR are met.

Example: Employees of a cleaning company. - A public authority concludes a contract with a cleaning company for the cleaning of its offices. The cleaning staff are contractually prohibited from accessing personal data in connection with this activity. However, when cleaning the offices, the cleaning staff may come across such data in individual cases. If they become aware of this, they are "third parties" within the meaning of Art. 4 No. 10 GDPR.

118 The General Data Protection Regulation primarily refers to the concept of third parties when it comes to including their interests in a consideration, for example in Art. 6 para. 1 subpara. 1 letter f GDPR and in Art. 14 para. 2 letter b GDPR. However, the term has no meaning in the definition of transfer. A transfer is always based on

[145] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 88.
[146] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 88.

to a recipient. Whether this is also a third party or not is irrelevant in accordance with Art. 4 No. 9 GDPR.

Joint controllers, on the other hand, are recipients within the meaning of Art. 4 No. 9 GDPR in relation to each other, not third parties. Data transfers from one joint controller to another are to be regarded as data transfers that require a legal basis (para. 124 et seq.). 119

7. Differentiation of the various roles[147]

The following questions, among others, can be helpful in differentiating between the various roles: 120

– Decision-making authority

  - Who decides on the purposes and means of processing? Para. 23 ff.
  - Is there an (expressly) regulated legal responsibility for the processing? Margin no. 26 ff.
  - Is the purpose of the processing the fulfilment of a legal obligation? Para. 26 ff.
  - Is the processing the result of an implied responsibility arising from general statutory provisions, current legal practice or traditional roles? Para. 32 ff.
  - Is there a de facto influence on the purposes and essential means of processing? Recital 35 et seq.

– concerning the purposes and means of processing

  - Why does the processing take place? No. 41
  - Do the parties pursue the same purpose or do the parties pursue their own purposes, but which are complementary to the purpose of the other parties or are mutually dependent? Para. 70 f.

If, in exceptional cases, it is not possible to draw a clear-cut distinction despite a thorough examination taking into account all aspects of the facts of the case, the more "data protection-friendly" assignment of responsibility for the data subjects must be assumed. In the case of processing of personal data based on the division of labour, this will generally be a joint responsibility that places the several parties involved under the same obligation as the data subjects. 121

[147] The flow charts in European Data Protection Board, Guidelines 07/2020 (fn. 22), Annex I, and European Data Protection Supervisor, EDPS Guidelines on the terms "Controller", "processor" and "joint controller" according to Regulation (EU) 2018/1725 (footnote 41), p. 36 (Annex 1).

V. Legal consequences of joint responsibility

1. No legal basis within the meaning of Art. 6 para. 1 GDPR

122 The fulfilment of the criteria of Art. 26 GDPR and thus the establishment of joint controllership does not constitute a legal basis for the processing operations carried out under joint controllership. Rather, the permissibility of the processing in question must result from other provisions. Insofar as a joint controller processes personal data within the scope of joint controllership, it therefore requires a legal basis for this processing in accordance with Art. 6 para. 1 GDPR, and additionally in accordance with Art. 9 para. 2 GDPR when processing special categories of personal data.[148]

123 If one of several joint controllers cannot base its processing (steps) on a (sufficient) legal basis, this will - for reasons of legal certainty[149] - However, for reasons of legal certainty, this does not generally result in the unlawfulness of the entire data processing; rather, a separate assessment is required for each of the joint controllers.[150]

2. No processing privilege

124 Joint responsibility is a separate legal concept. However, joint controllership does not create a separate subject for the assignment of rights and obligations (no separate legal personality of the joint controllers). This means that the joint controllers are not third parties within the meaning of Art. 4 No. 10 GDPR in relation to each other. Rather, they are recipients within the meaning of Art. 4 No. 9 GDPR, insofar as the joint responsibility extends.[151] An exception applies in the event that one of the joint controllers is based in a third country and therefore the joint controllership involves the transfer of data to a third country: In this case, the special provisions of Art. 44 et seq. GDPR apply and the joint controllers are treated as third parties.[152]

[148] ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 96 f.

[149] Lurtz/Schindler, comment on ECJ, judgment of 29 July 2019, Case C-40/17 - Fashion ID, VuR 2019, p. 468, 475.

[150] Moos/Rothkegel, comment on ECJ, judgment of 29 July 2019, C-40/17, MMR 2019, p. 579, 586 f.

[151] Lang, in: Taeger/Gabel, GDPR - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 112 f.

[152] Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 3b¸ Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 114. For cross-border processing by groups of companies, see in particular Art. 47 GDPR.

2. no processing privilege

In the absence of a separate legal personality of the joint controllers, they also do not enjoy a processing privilege if they exchange data with each other.[153] This means that the transfer of data between them requires - in addition to the justification of their own processing activities - a separate legal basis within the meaning of Art. 6 GDPR or, if applicable, Art. 9 GDPR. This requirement is already apparent from the wording of Art. 26 para. 1 GDPR, which does not contain any exception to the justification requirement or any corresponding privileged treatment of data exchange between joint controllers, but also from the legal materials.[154] In this respect, joint controllership differs significantly from commissioned processing with its processing privilege (para. 94). 125

However, the independent authorisation required for the transfer between joint controllers is likely to often result for public bodies from the fulfilment of a legal obligation (Art. 6 para. 1 subpara. 1 lit. c, para. 3 GDPR in conjunction with an obligation under national law)[155] or the performance of a task carried out in the public interest (Art. 6 para. 1 subpara. 1 letter e, para. 3 GDPR in conjunction with a processing authorisation under national law). Art. 5 para. 1 sentence 1 no. 1 BayDSG applies to the transfer of data between public bodies (fulfilment of a task incumbent on the transferring or receiving public body). For joint controllers in the non-public sector, the lawfulness of the transfer based on a legitimate interest in the division of labour (Art. 6 para. 1 subpara. 1 letter f, subpara. 2 GDPR) also comes into consideration.[156] If processing by several joint controllers is to be based on consent in accordance with 126

[153] ECJ, judgment of 29 July 2019, C-40/17 (Fashion ID), para. 96 f.; Bertermann, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2nd ed. 2018, Art. 26 GDPR para. 11; Hartung, in: Kühling/Buchner, DSGVO - BDSG, 4th ed. 2024, Art. 26 GDPR para. 62; Piltz, in: Gola/Heckmann, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3rd ed. 2022, Art. 26 GDPR para. 17; Dovas, Joint Controllership - Möglichkeiten oder Risiken der Datennutzung? ZD 2016, p. 512, 515; DSK, short paper no. 16 (fn. 27), p. 1. Other view Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 DSGVO para. 3a; Plath, in: Plath, DSGVO/BDSG, 4th ed. 2023, Art. 26 GDPR para. 29. Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, status 5/2022, Art. 26 GDPR para. 43, 46 differentiates between initial and subsequent joint responsibility. 43, 46 differentiates between initial and subsequent joint responsibility depending on the time at which it is established - in the case of initial joint responsibility, the transfer or granting of access "within the scope of control of joint responsibility" is legitimised by the original collection and its justification, whereas the subsequent establishment of joint control is accompanied by a data transfer or provision, which must be examined against the standard o f Art. 6 GDPR.

[154] An addition proposed by the European Parliament, according to which the term "processing of personal data" should also include the possibility that the controller "transfers the data to joint controllers or a processor for the purpose of processing on their behalf", did not find its way into the version adopted by the legislator (EC 79 GDPR), EC 62 sentence 2 Position of the European Parliament (fn. 12).

[155] In the case of data processing on the basis of Art. 6 para. 1 subpara. 1 lit. c GDPR in conjunction with an obligation under national law, however, individual responsibilities are often also taken into account, see para. 69.

[156] Schall, in: Katko, Checklisten zur Datenschutz-Grundverordnung (DSGVO), 2nd ed. 2023, Chapter 11 para. 115. As a rule, this legitimate interest of the joint controllers should also outweigh any c o n f l i c t i n g interests, fundamental rights and freedoms of the data subjects - at least insofar as the processing vis-à-vis the data subjects can be based on a legal basis per se and the requirements of Art. 26 GDPR are met in the internal relationship.

If the consent is based on Article 6(1)(1)(a) GDPR, the consent must unambiguously include the processing by all joint controllers and therefore also the corresponding transfer to the other joint controller(s).

127 Practical note: With regard to Art. 7 GDPR, a prerequisite for the informed consent of data subjects to the processing of their personal data by joint controllers is that they have a reasonable opportunity to obtain information in advance about all features characterising the data processing in question. In the case of data processing carried out under joint responsibility, this includes the identities of all parties involved, their processing purpose(s), the processed data and, if applicable, the intention of an exclusively automated decision or a data transfer to third countries. The data subjects must also be informed to whom and in what form they can give their consent. Finally, according to Art. 7 para. 3 sentences 3 and 4 GDPR, the data subjects are
of the possibility of cancellation and its modalities.

3. Applicability of special regulations

128 If there is joint responsibility, the scope of application of some special provisions of the General Data Protection Regulation opens up:

- Art. 30 para. 1 sentence 2 letter a GDPR regarding the record of processing activities: The name and contact details of the joint co-controller shall be included in the record of processing activities;[157]
- Art. 36(3)(a) GDPR regarding prior consultation for data protection impact assessments: The respective responsibilities of the joint controllers shall be made available to the supervisory authority;
- Art. 82 (2), (4) and (5) GDPR regarding liability and the right to compensation: The construction of joint responsibility and the liability of the joint controllers in the external relationship as well as the compensation in the internal relationship are most comparable to a joint and several debt within the meaning of Section 421 BGB.
- Possible fines on the basis of Art. 83(4)(a) GDPR have a special status in this respect: The joint controllers are liable for them separately and according to their individual responsibilities.

[157] It is also possible to keep a separate register only for the processing operations under joint responsibility. This may facilitate supervision, Martini, in: Paal/Pauly, GDPR - BDSG,
3rd ed. 2021, Art. 30 GDPR para. 5a.

4. Obligation to conclude an agreement

As we have seen, the meaning and purpose of Art. 26 GDPR is particularly evident against the background of EC 79 GDPR, according to which a clear allocation of data protection responsibilities is required to protect the rights and freedoms of data subjects and with regard to the responsibility and liability of controllers and also with regard to the monitoring and other measures of supervisory authorities.[158] a clear allocation of responsibilities under data protection law is required. Data subjects should not suffer any disadvantages as a result of several controllers working together on a processing operation.[159] 129

If the conditions for joint responsibility are met, Art. 26 para. 1 sentence 2 GDPR therefore stipulates the obligation to conclude a joint controllership agreement in which the parties involved must specify in a transparent manner which of them fulfils which obligation under the General Data Protection Regulation. 130

The agreement is therefore not a prerequisite for joint responsibility, but its legal consequence.[160] The existence of joint liability is not at the discretion of the persons or bodies involved - joint liability cannot be established or excluded by an agreement. 131

According to Art. 26 para. 1 sentence 2 at the end of the GDPR, the conclusion of an agreement is only not required if and insofar as Union law or national law regulates the question of the allocation of responsibility. In this respect, no other agreements on responsibility between the joint controllers are possible. However, it is advisable to include the EU or national regulations in an agreement for declaratory purposes.[161] However, this does not mean that a statutory allocation of responsibilities is mandatory for public bodies and that the conclusion of an agreement between public bodies is inadmissible in this respect.[162] The opening clause also applies in this respect. Jointly responsible public bodies may and 132

[158] However, the supervisory authorities are not bound by the provisions in the joint controllers' agreement, see para. 197 below.

[159] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 16.

[160] ECJ, judgment of 5 December 2023, C-683/21, para. 44 f.; Martini, in: Paal/Pauly, GDPR - BDSG, 3. 2021, Art. 26 GDPR para. 22; Piltz, in: Gola/Heckmann, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3rd ed. 2022, Art. 26 GDPR para. 20; Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 49; Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 4th ed. 2019, Art. 26 GDPR para. 10; Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 72.

[161] Knoblauch, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 11/2018, Art. 26 GDPR para. 16; European Data Protection Board, Guidelines 07/2020 (fn. 22), fn. 72: "In any case, the joint controllers' agreement should comprehensively address all responsibilities of the joint c o n t r o l l e r s , including those that may already be laid down in relevant EU or Member State law, and without prejudice to the obligation of the joint controllers to make a v a i l a b l e t h e essence of the agreement between the joint controllers pursuant to Article 26(2) GDPR."

[162] Radtke, Joint Liability under the GDPR, 2021, p. 247. See also footnote 106 in this context.

must conclude an agreement in the absence of corresponding legal provisions.

Examples of statutory allocation of tasks in accordance with Art. 26 para. 1 sentence 2 at the end of the GDPR:

- § Section 307 (5) sentences 2 and 3 of the Fifth Book of the German Social Code - Statutory Health Insurance - (SGB V) regarding gematik's task of setting up a coordinating body in connection with the telematics infrastructure (see para. 78 above);[163]
- § Section 204 (7) of the Seventh Book of the German Social Code - Statutory Accident Insurance - (SGB VII), which assigns responsibility for the duty to inform in accordance with Art. 13 GDPR to the accident insurance institution responsible for the insured person if a file system is set up for several accident insurance institutions.

In contrast, the designation of the public body as the controller under data protection law pursuant to Art. 3 para. 2 BayDSG does not constitute a concretisation of the responsibilities within the meaning of Art. 26 para. 1 sentence 2 at the end of the GDPR with regard to the respective joint processing. In this respect, the Bavarian legislator has only made use of the opening clause
of Art. 4 No. 7 half-sentence 2 GDPR.

133 The Union legislator has left the content of the agreement open: The joint controllers must regulate the fulfilment of all obligations of the General Data Protection Regulation, whereby Art. 26 para. 1 sentence 2 GDPR emphasises the protection of the rights of the data subject and the information obligations pursuant to Art. 13 and 14 GDPR. Art. 26 GDPR leaves the specific allocation of responsibilities (and thus indirectly of liability) to the bodies involved ("regulated self-regulation").[164]

134 The agreement between the joint controllers is therefore a consequence of the principle of accountability in Art. 5 para. 2 GDPR. A breach of the obligations provided for in Art. 26 GDPR does not constitute "unlawful processing". This is because the standard for the lawfulness of processing is Art. 5 para. 1 letter a, 6 para. 1 GDPR, concretised in Art. 7 to 11 GDPR. Compliance with the obligation to conclude an agreement in accordance with Art. 26 GDPR is not one of the grounds for the lawfulness of processing specified in Art. 6 para. 1 subpara. 1 GDPR; the aim of Art. 26 GDPR is also not to limit the scope of the requirements in Art. 5 para. 1 lit. 1 and Art. 6 para. 1 GDPR.[165]

135 If the agreement is missing or inadequately drafted[166] there is at least a violation of Art. 26 GDPR. The joint controllers must subsequently conclude the agreement or formulate it in accordance with the requirements. The data protection

[163] See SG Munich, judgement of 26 January 2023, S 38 KA 72/22, BeckRS 2023, 2607, para. 64.

[164] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 4.

[165] ECJ, judgment of 4 May 2023, C-60/22, para. 54 et seq. The absence of an agreement establishing joint responsibility pursuant to Art. 26 GDPR is not in itself sufficient to prove that there has been a violation of the fundamental right to the protection of personal data (ibid., para. 65). Misleadingly speaking generally of an unlawfulness of the processing DSK, Beschluss der DSK zu Face- book Fanpages, 5 September 2018, p. 2, Internet: https://www.datenschutzkonferenz-online.de/beschlu- e s s e - d s k .html.

[166] Lang, in: Taeger/Gabel, GDPR - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 119.

The supervisory authority can work towards this with the means permitted in the individual case (in particular also measures pursuant to Art. 58 para. 2 GDPR). According to Art. 83 para. 4 letter a GDPR, all joint controllers can be prosecuted for non-compliance with the requirements set out in Art. 26 GDPR;[167] However, fines may only be imposed on public bodies under Art. 83 GDPR if they participate in the competition as companies, Art. 22 BayDSG.

How detailed the description of the responsibilities of the bodies involved must be is determined in each case by the scope and complexity of the processing, the number of persons involved in the processing and the risks that arise for the data subjects. This does not necessarily require a schematic presentation, but rather documentation appropriate to the processing, which must also correspond to the facts and specifically describe the data processing in question.[168] and specifically describe the data processing in question.[169] 136

The joint controllers have a certain degree of flexibility in the distribution and allocation of obligations among themselves. They only need to ensure full compliance with the General Data Protection Regulation in relation to the processing they carry out jointly - each entity involved in the processing is subject to the applicable data protection provisions. In particular, the parties may consider who is competent and able to effectively guarantee the rights of data subjects and fulfil the relevant obligations under the GDPR.[170] The obligations do not have to be evenly distributed among the joint controllers.[171] The European Data Protection Board recommends recording the relevant facts and the internal assessment regarding the allocation as part of the documentation in accordance with the principle of accountability.[172] 137

However, some obligations, for example regarding the principle of purpose limitation (Art. 5(1)(b) GDPR) or certain security measures for IT systems used (Art. 5(1)(f), Art. 24, Art. 32 GDPR), cannot be divided up and must be fulfilled equally by all joint controllers. 138

Independent of this are the data protection requirements that apply to the parties involved not in connection with the joint processing, but in their function as data controllers, such as the maintenance of a register of processing activities (Art. 30 para. 1 sentence 1 GDPR in compliance with Art. 30 para. 1 sentence 1 GDPR). 139

[167] Note the exception regarding the imposition of fines on public bodies under Art. 23 para. 3 BayDSG. Incidentally, this has no effect on the effective application of the General Data Protection Regulation, ECJ, judgment of 4 May 2023, C-60/22, para. 68.

[168] Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 4; Hartung, in: Kühling/Buchner, DSGVO - BDSG, 4th ed. 2024, Art. 26 GDPR para. 55; Specht-Riemenschneider/Schneider, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, p. 503, 506.

[169] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 16.

[170] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 168.

[171] ECJ, judgment of 5 June 2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein), para. 43.

[172] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 168.

para. 1 sentence 2 letter a GDPR) and the appointment of a data protection officer (Art. 37 para. 1 GDPR).

140 Art. 26 para. 1 sentence 2 GDPR presupposes the cooperation of all jointly responsible parties involved and, in conjunction with EC 79 and Art. 83 GDPR, grants them a claim against each other.[173] This is the only way to effectively realise the objective of the clear allocation of responsibilities set out in EC 79 GDPR. If one party could refuse to participate in the agreement, this objective would regularly be thwarted. In addition, the obligation to conclude an agreement under Art. 83 (4) (a) GDPR is subject to sanctions (however, an exception applies to public bodies under Art. 22 BayDSG).

a) Mandatory content of the agreement pursuant to Art. 26 para. 1 sentence 2, para. 2 sentence 1 GDPR

141 Art. 26 para. 1 sentence 2 GDPR specifies the mandatory content of the agreement. According to this, the joint controllers must determine which of them fulfils which obligation under the General Data Protection Regulation, in particular with regard to the exercise of the rights of data subjects, and who complies with which information obligations under Art. 13 and 14 GDPR, taking into account Art. 9 BayDSG. The agreement must duly reflect the respective actual functions and relationships of the joint controllers vis-à-vis data subjects, Art. 26 para. 2 sentence 1 GDPR.[174] However, information on the economic conditions of joint responsibility, such as the distribution of costs, is not required.

142 Practical note: Although the mention of other jointly responsible parties in the informa- or information pursuant to Art. 13 to 15 GDPR is not mandatory, but such an obligation will nevertheless exist due to the requirements in Art. 26 para. 2 sentence 2 GDPR.

b) Specifications in the agreement

143 Joint controllers must ensure that all joint processing is fully compliant with the General Data Protection Regulation. This requires that all essential obligations of the General Data Protection Regulation are regulated and responsibilities are determined in each case.[175] The parties involved can use the

[173] Specht-Riemenschneider/Schneider, The joint responsibility in data protection law, MMR 2019, Different view Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 74. Weichert, Die DSGVO, ein - ganz guter - Anfang, DuD 2020, pp. 293, 295, sees legal uncertainty and the need for clarification by the legislator here.

[174] For more details on this requirement, see para. 175 et seq.

[175] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 162 et seq.

content of agreements on order processing in accordance with Art. 28 para. 3 GDPR and Annex B of the standard contractual clauses[176] should be taken into account.[177]

The parties should therefore make provisions on the following aspects in particular (in the agreement or, if applicable, in its annexes): 144

– clear designation of the bodies involved in the agreement; 145

– Preamble: 146

in the sense of a preliminary presentation of the meaning and purpose of the cooperation for a better understanding of the following regulations;

– Description of the processing carried out under joint responsibility: 147

Precise, clear and consistent description, in particular of the subject matter and duration, nature and purpose of the processing, type of personal data processed, categories of data subjects, means, scope and differentiation of the areas of influence and impact of the parties involved;[178] also recording the actual logical infrastructure, i.e. the application programmes, their interfaces and the physical infrastructures on which they are based;[179] The parties have considerable room for manoeuvre in this respect;

– Legal basis (Art. 6 para. 1 GDPR, if applicable Art. 9 para. 2 GDPR): 148

Joint controllers may base the processing operations they carry out on different legal bases; the European Data Protection Board recommends, however, "using the same legal basis for a specific purpose wherever possible";[180]

– Regulations including the responsibilities for handling consents and revocations, 149

to ensure immediate and uniform implementation and documentation;

– Allocation of responsibilities of the parties for ensuring compliance with the General Data Protection Regulation, in particular 150

[176] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses (SCCs) 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, 7 June 2021, p. 31 et seq.).

[177] Knoblauch, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 11/2018, Art. 26 GDPR para. 11. Suggestions on the content of the agreement in Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 76 f., 84 ff.

[178] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 175.

[179] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 16.

[180] European Data Protection Board, Guidelines 07/2020 (fn. 22), fn. 73: "Although the GDPR does not prevent joint controllers from using different legal bases for different processing operations they carry out, it is recommended that the same legal basis be used for a given purpose wherever possible."

V. Legal consequences of joint responsibility

151 ● General obligation of the parties involved to comply with all data protection regulations;

152 • Duty to provide information to data subjects (in addition to Art. 13 and 14 GDPR as mandatory content, also 26 para. 2 sentence 2 GDPR);

153 ● Enquiries and rights of the data subject (Art. 12 to 23 GDPR), designation of a contact point if necessary (Art. 26 para. 1 sentence 3 GDPR);

Note: Joint controllers who carry out processing within the scope of Art. 28 para. 1 BayDSG must agree and provide a contact point in accordance with Art. 26 para. 1 sentence 3 GDPR (Art. 30 sentence 1 BayDSG). Outside the scope of application of Art. 28 para. 1 BayDSG, the establishment and designation of a contact point is not mandatory. A contact point is intended to ensure functioning communication between controllers on the one hand and data protection supervisory authorities and data subjects on the other. Whether it makes sense to set one up depends on the number of joint controllers involved and the complexity of the processing operations. The contact point cannot be decoupled from the joint controllers,[181] This means that it must be one of the joint controllers or a specific person or body assigned to their organisational unit, such as the data protection officer or, if available, a processor. Delegating this task of the controller to a third party would run counter to the core idea of Art. 26 GDPR to spare data subjects from climbing a "carousel of responsibilities".[182] The scope of the power of representation of a contact point is not expressly regulated - since its establishment as such is basically at the discretion of the parties to the agreement, they have freedom of design in this respect.[183] However, unlike the structurally comparable representative within the meaning of Art. 27 GDPR, the contact point is not a representative of the controller in the legal sense.[184] Irrespective of the establishment of a contact point, each joint controller remains authorised to act as a representative of the controller on the basis of the provision in Art. 26 para. 3

[181] An independent third party is out of the question: European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 185; Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 29; Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. According to the wording of the provision, a different interpretation would also be possible, but the drafting history of the standard speaks in favour of a narrow understanding: The general approach of the European Council still spoke (in more detail) of the indication, "which the joint controller shall act as a single point of contact for data subjects when exercising their rights" (Art. 24 para. 1 sentence 3 in the version of the Council of the European Union, document 9565/15 [footnote 14]). According to the dissenting opinion of Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 81, the controller should also be able to use an external party to fulfil this task.

[182] Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 29.

[183] Petri, in: Simitis/Hornung/Spiecker gen. Lang, in: *Taeger/Gabel/Lang*, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 82, who sees the contact point reduced to the function of a "receiving and explaining agent".

[184] Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 29a.

GDPR; an exemption from responsibility and liability is not possible.

- Enquiries from data protection supervisory authorities or third parties; 154
- Regulations on the use of processors (Art. 28 GDPR); 155

Joint controllers may engage processors for the processing of personal data. They may stipulate internally that one or all of the parties involved - after prior information and consent of the others - are authorised to commission contractors as (sub)processors in accordance with Art. 28 GDPR. The party or parties concluding the data processing agreement are obliged to select the (sub)processor with due care and to draft the contractual agreements in accordance with the provisions of Art. 28 para. 3 GDPR. If several jointly responsible parties utilise a processor at the same time, it must be made clear
The data controller must indicate in whose area of activity the respective data processing is carried out on behalf of the data subject.

- List of processing activities (Art. 30 GDPR) with specifics of Art. 30 para. 1 sentence 2 letter a GDPR; 156

An exception to the documentation obligation applies if a body is jointly responsible within the meaning of Art. 26 GDPR without processing personal data itself.[185] If there is no own data processing, no documentation is required in the record of processing activities.

In cases of (co-)controllers who are not yet known by name but who later become concretely known or constantly changing (co-)controllers, at least the fact of joint responsibility must be documented with regard to Art. 30 para. 1 sentence 2 letter a GDPR and the circle of potential (co-)controllers must be described. The traceability of the
The time of (co-)responsibility must be ensured.

- technical and organisational measures (Art. 32, Art. 24, Art. 25 GDPR) 157

The regulations regarding technical and organisational measures must be differentiated on a case-by-case basis: For example, if there is joint responsibility only for the collection and transfer of data and one party is solely responsible for further processing steps, technical and organisational measures must only be jointly defined for the jointly responsible processing part. Each party is independently responsible for the other areas.

The technical and organisational measures are determined on a case-by-case basis.
depending on the risk of the processing and must take into account the principles of privacy by default and privacy by de- sign in accordance with Art. 25 GDPR.

[185] For example, the religious community in the Jehovah's Witnesses case, ECJ, judgement of 10 July 2018, C-25/17.

158 • Regulations regarding data security breaches (Art. 33 and 34 GDPR);[186]

159 Data protection impact assessment (Art. 35 and 36 GDPR) with specific feature of Art. 36 para. 3 letter a GDPR;[187]

The following applies: The mere fact that different parties work as joint controllers does not necessarily increase the risk of violating data protection obligations and therefore does not necessarily require a data protection impact assessment. A case-by-case assessment must be carried out.[188] EC 92 GDPR provides for a simplification in this respect with the possibility of carrying out a thematic data protection impact assessment instead of a project-related data protection impact assessment if this is
is "reasonable and expedient from an economic point of view".[189]

160 • Regulations on data transfer to third countries (Art. 44 to 50 GDPR),

in particular defining the mechanisms and responsibilities used;

161 - special regulations in the internal relationship,

disputes, the allocation of liability pursuant to Art. 82 (4) GDPR, agreements on the
The following are examples of such agreements: the definition of emergency and escalation mechanisms, relationship to other contracts and agreements, arbitration agreements and confidentiality agreements;

162 - mutual support and information obligations of the parties,

including the fulfilment of the necessary documentation in general, in each case limited to what is necessary for the fulfilment of duties;[190]

163 - Entry into force, term and termination of the agreement and its legal consequences;

i.e. processing, deletion, etc., if necessary extraordinary right of cancellation, in particular in the event of serious data protection violations by the other party;

164 - Attachments;

165 - Final provisions.

[186] See only European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, Status 3/2023, para. 42, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en.

[187] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and answering the question of whether processing is "likely to result i n a high risk" within the meaning of Regulation 2016/679, status 10/2017, WP 248 Rev. 01, p. 8, Internet: https://www.datenschutzkonferenz-online.de/wp29- leitlinien.html.

[188] Lang, in: Taeger/Gabel, GDPR - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 10; DSK, short paper No. 16 (fn. 27), p. 4: "Cases of joint responsibility can often lead to an increase in the risks to the rights and freedoms of data subjects."

[189] As an example of these aspects, the legislator mentions cases in which "authorities or public bodies wish to create a joint application [...]" or "several responsible parties wish to introduce a joint application [...]".

[190] Specht-Riemenschneider/Schneider, The joint responsibility in data protection law, MMR 2019, S. 503, 506.

d) Agreements for mixed contractual relationships

In practice, complex processing operations involving several entities occasionally exhibit both the characteristics of joint controllership and elements of commissioned processing. 166

Example: Processing of registration data and civil status data by the Institute for Municipal Data Processing - AKDB:[191]

For example, the AKDB can be commissioned by registration authorities to process personal data as a processor in accordance with Art. 3 Para. 1 of the Bavarian Law on Registration, Passport and Identity Cards (BayGMPP). In this respect, the provisions of Art. 28 GDPR apply.

In addition, the AKDB is expressly assigned responsibility under data protection law for certain case constellations in Art. 7 para. 2 sentence 2 BayGMPP, Art. 24 para. 2 sentence 2 Ordinance on the Transmission of Registration Data and Art. 7 para. 3 Act on the Implementation of the Personal Data Act, which it generally shares with the data transmitter.
the body responsible for processing. In this context, Art. 26 GDPR must be taken into account.

167

In these cases, not all parties involved decide equally and with equal rights on all purposes and (essential) means of processing. In such cases, the responsibilities of the parties involved must be contractually defined both in accordance with Art. 26 GDPR as joint controllers and in accordance with Art. 28 (3) and (4) GDPR as principals or contractors, unless a statutory provision already exists.

e) Form of the agreement

The General Data Protection Regulation does not prescribe a specific form for the agreement. However, the documentation and accountability obligations of data controllers pursuant to Art. 5 para. 2 GDPR generally require a written or electronic form, in any case at least text form in accordance with Section 126b BGB. In the interests of legal certainty and transparency, the European Data Protection Board therefore recommends concluding the agreement in the form of a binding document such as a contract or other binding legal instrument.[192] This view is supported by a look at Art. 26 para. 2 sentence 2 GDPR, according to which "the [essential[193] of the agreement [...] shall be made available to the data subject". With regard to this information obligation, it is also advisable to regulate the parts of the agreement to be disclosed separately as an annex.[194] In this way, the essential contents of the agreement for the persons concerned can be communicated without having to make confidential contents unrecognisable. 168

[191] Knoblauch, in: Wilde/Ehmann/Niese/Knoblauch, Data Protection in Bavaria, status 11/2018, Art. 26 GDPR para. 14.

[192] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 173.

[193] In this respect, the standard text uses an unusual spelling ("the essential"). The terminology is used in corrected form below.

[194] Plath, in: Plath, DSGVO/BDSG, 4th ed. 2023, Art. 26 GDPR para. 38.

169 Practical note: In the case of agreements between public bodies, the conclusion of a contract is unusual and an agreement in the form of an "other binding legal instrument" (see Art. 28 para. 3 sentence 1 GDPR), such as a public law cooperation agreement or a special purpose agreement, is more likely to be considered. Also the arrangement of joint responsibility by means of a regulation,
Directive or formal law are "other binding legal instruments".

170 If the parties choose the civil law form of contract for the agreement, the contractual provisions of the German Civil Code apply; in the case of public law contracts, Art. 54 et seq. BayVwVfG, whereby the General Data Protection Regulation contains special legal requirements for the design of the joint controllership agreement.

f) Transparency

171 According to Art. 26 para. 1 sentence 2 GDPR, the agreement must be in a transparent form. This requirement primarily addresses the content of the agreement. The agreement on joint responsibility can also be combined with other agreements, provided that this does not impair the transparency and quality of the information.[195]

172 However, the agreement itself does not have to fulfil the specific transparency requirements of EC 58 GDPR.[196] This stipulates that information intended for the public or the data subject must be precise, easily accessible and comprehensible and written in clear and plain language. However, the contents of the agreement pursuant to Art. 26 para. 1 sentence 2, para. 2 sentence 1 GDPR are not intended "for the public or the data subject" and only to a limited extent for the data protection supervisory authorities, to whom the contents of the agreement, in particular the internal assignments of responsibility, are not binding.[197] Nothing else arises from the requirements of EC 79 GDPR. Therefore, the "simple transparency requirement" of Art. 26 para. 1 sentence 2 GDPR applies to the agreement itself and the agreement can therefore be drafted in standard contractual language - even if this may not be directly accessible to everyone affected by the processing covered by the agreement[198]. However, something different applies with regard to the "essence of the agreement", which must be made available to the data subject in accordance with Art. 26 para. 2 sentence 2 GDPR - in this respect, the requirements of EC 58 GDPR must be observed. The differentiation within Art. 26 GDPR is therefore reflected in different transparency requirements.

[195] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 21.

[196] See also Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 87, 101; Plath, in: Plath, DSGVO/BDSG, 4th ed. 2023, Art. 26 GDPR para. 34. Other view Piltz, in: Gola/Heckmann, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3rd ed. 2022, Art. 26 GDPR para. 24.

[197] See para. 197 below.

[198] Schreiber, Joint responsibility towards data subjects and supervisory authorities, ZD 2019, p. 55, 56.

g) Timing

The agreement between the joint controllers is neither a prerequisite for the existence of joint controllership nor can it establish it. Regardless of this, the agreement must be concluded prior to the processing in question. This follows from the purpose of Art. 26 GDPR in conjunction with EC 79 GDPR to protect the rights and freedoms of data subjects through a transparent assignment of the obligations incumbent on the joint controllers. Effective protection requires that this assignment has already taken place before the start of processing.[199] 173

5. Relationship between the joint controllers and the data subjects

The General Data Protection Regulation contains specific regulations regarding the relationship between the joint controllers and the data subjects. 174

a) Requirement of the agreement to adequately reflect the respective actual functions and relationships with data subjects, Art. 26 para. 2 sentence 1 GDPR

The agreement between the joint controllers pursuant to Art. 26 para. 2 sentence 1 GDPR must duly reflect the respective actual functions and relationships of the joint controllers vis-à-vis the data subjects. This means that the data protection role of the joint controllers involved must be correct in terms of content,[200] This means that the data protection role of the joint controllers involved must be presented correctly, comprehensibly and in accordance with the facts. This requirement relates solely to the actual functions and relationships with the data subjects, but not to the relationships between the joint controllers.[201] 175

Compliance with this condition is a prerequisite for the agreement to be effective. Only in this way can it be ruled out that, in the event of a serious imbalance between the jointly responsible parties, an improper internal "indemnification" of a controller is agreed, which contradicts or conceals the actual shares of responsibility. However, the aspect of avoiding a misconception about the responsibilities of the data subjects is not of decisive importance, as they are not the primary addressees of the agreement. Furthermore, the obligation under Art. 26 para. 2 sentence 2 GDPR also realises indirect traffic protection.[202] 176

[199] Lang, in: Taeger/Gabel, GDPR - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 94.

[200] On the truthfulness requirement of the agreement Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 30.

[201] Piltz, in: Gola/Heckmann, General Data Protection Regulation - Federal Data Protection Act, 3rd ed. 2022, Art. 26 GDPR para. 29.

[202] On the whole Ingold, in: Sydow/Marsch, GDPR – BDSG, 3rd ed. 2022, Art. 26 GDPR para. 9.

177 It is not clear from the General Data Protection Regulation which standard must be used to determine the appropriate reflection. According to the meaning and purpose of the provision, a distinction must again be made according to the recipient's horizon[203] - As far as the essential content of the agreement within the meaning of Art. 26 para. 2 sentence 2 GDPR is concerned, the perspective of the data subject must therefore be taken into account.

b) Duty to inform

178 In addition, the joint controllers are obliged to provide information to the data subjects. In principle, each of the joint controllers must fulfil the obligations, whereby the parties involved can divide the performance of the obligations among themselves:

179 On the one hand, in accordance with Art. 26 para. 1 sentence 2 GDPR, data controllers must stipulate the fulfilment of the general data protection information obligations under Art. 13 and 14 GDPR.[204]

180 On the other hand, Art. 26 para. 2 sentence 2 GDPR stipulates the requirement to provide the data subject with the essentials of the agreement. However, the General Data Protection Regulation does not specify the concrete content and formal requirements for this information obligation.

181 According to the meaning and purpose of the provision of Art. 26 para. 2 sentence 2 GDPR, the "essence of the agreement" meaningfully covers the minimum content of the agreement pursuant to Art. 26 para. 1 sentence 2 GDPR (see para. 141 et seq. above).[205] However, it does not include information on the economic conditions of the cooperation.[206] If the joint controllers provide information on liability, this must not mislead the data subjects with regard to liability claims.[207]

182 The addressee of the information pursuant to Art. 26 para. 2 sentence 2 GDPR is the data subject, therefore the principle of transparency applies to the presentation according to EC 58 GDPR. EC 58 sentence 1 GDPR specifies this requirement to the effect that the information must be precise, easily accessible and comprehensible and written in clear and plain language.

[203] See para. 172 above.

[204] For comprehensive information on this, see Bavarian State Commissioner for Data Protection, Information Obligations of the C o n t r o l l e r , Orientation Guide, status 11/2018.

[205] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 GDPR para. 26; Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 57; E u r o p e a n Data Protection Board, Guidelines 07/2020 (fn. 22), para. 180: The European Data Protection Board recommends that at least all elements of the information referred to in Articles 13 and 14 that should already be accessible to the data subject are included.

[206] Bertermann, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2nd ed. 2018, Art. 26 GDPR para. 15; Knob- lauch, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 11/2018, Art. 26 GDPR para. 18.

[207] Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 33. In the opinion of Spoerr, in Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 58, information on claims for damages should not be included as these are not part of the "rights of the data subject" within the meaning of Art. 26 GDPR. 58, information on claims for damages should not be included, as these are not part of the "rights of the data s u b j e c t " within the meaning of Art. 26 GDPR, as they are regulated in Art. 82

5. relationship between the joint controllers and the data subjects

GDPR and not in Chapter III of the GDPR.

must. In this respect, it is a matter of addressee justice in the sense of lay and everyday comprehensibility.[208] Therefore, for example, a (shortened) presentation in table form or using comprehensible symbols is also conceivable.[209] For information and notices aimed at children, EC 58 sentence 4 GDPR contains a specification to the effect that, due to their special need for protection, "information and notices [should] be provided in such clear and simple language that a child can understand them".

The manner in which this information is to be made available to the data subject is not regulated. In particular, unlike other provisions of the General Data Protection Regulation, Art. 26 para. 2 sentence 2 GDPR does not contain any indication that the information should only be available on request or published in an appropriate manner. The decision on this is therefore generally the responsibility of the joint controllers. However, the following applies: 183

– The information must be provided in a consistent manner.[210]

– The information can be provided in writing, but also in electronic form (see EC 58 sentence 2 GDPR). When choosing the form, however, the verifiability as a result of the accountability obligation should be kept in mind.[211] Therefore, information that is only provided verbally should be viewed critically.[212]

– It is sufficient to provide access to the information (cf. English language version: "shall be made available"), for example by making it freely available. It is therefore conceivable to provide the "essence of the agreement" together with the information in accordance with Art. 13 and 14 GDPR, in the privacy policy, on request from the data protection officer (if available) or from the contact point named, if applicable, or on a website.[213] or on a website[214] (see EC 58 sentence 2 GDPR).

Art. 26 para. 2 sentence 2 GDPR also contains no requirements regarding the timing of the information. However, it makes sense to make the "essence of the agreement" available to the data subjects at the same time as the information pursuant to Art. 13 and 14 GDPR. This follows from the purpose of Art. 26 GDPR in conjunction with EC 79 GDPR to protect the rights and freedoms of data subjects by transparently allocating the obligations incumbent on the joint controllers. Effective protection requires early access to this information, which in any case cannot be provided after 184

[208] Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Status 5/2022, Art. 26 GDPR para. 57.

[209] See EC 58 sentence 1 GDPR at the end: "... and, where appropriate, additional visual elements".

[210] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 181.

[211] See only Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 35 with further references.

[212] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2019, Art. 26 GDPR para. 27.

[213] European Data Protection Board, Guidelines 07/2020 (fn. 22), para. 181.

[214] Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 35; Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 GDPR para. 27; DSK, Short Paper No. 16 (fn. 27), p. 4; agreeing Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 51. Different view Plath, in: Plath, DSGVO/BDSG, 4th ed. 2023, Art. 26 GDPR para. 40, who does not consider unsolicited disclosure to be necessary.

the time for the general information obligation pursuant to Art. 13 and 14 GDPR. The information must therefore be provided (at the latest) at the same time as Art. 13 and 14 GDPR.[215]

185 If there are significant changes with regard to the subject matter of the information, for example if additional joint controllers are added, the obligations under Art. 26 GDPR arise anew at the respective time. This arises in particular from the requirement of Art. 26 para. 2 sentence 1 GDPR that the agreement must adequately reflect the actual functions and relationships of the joint controllers vis-à-vis data subjects.

c) Art. 26 para. 3 GDPR

186 Art. 26 para. 3 GDPR contains a clarification to the effect that the data subject can assert their rights under the General Data Protection Regulation[216] with and against each of the joint controllers - regardless of any other provisions in the agreement and/or the designation of a contact point. Art. 26 para. 3 GDPR not only provides guidance for the assertion of claims by data subjects, but also for possible claims for compensation between the joint controllers.[217]

6. Legal effects of the agreement

187 The agreement to be concluded in accordance with Art. 26 para. 1 sentence 2 GDPR is binding on the joint controllers: they must adhere to the content of their agreement both with each other and with the data subjects and supervisory authorities.

[215] Lang, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4th ed. 2022, Art. 26 GDPR para. 100; probably also DSK, short paper no. 16 (fn. 27), p. 3f. Other view Piltz, in: Gola/Heckmann, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3rd ed. 2022, Art. 26 GDPR para. 33, according to which the essence of the agreement can also be made available after collection and also after further processing.

[216] DSK, short paper no. 16 (fn. 27), p. 2: "The enforcement of civil law claims is facilitated for the data subject with joint and s e v e r a l liability in accordance with Art. 26 para. 3 GDPR." This includes all rights of the data subject under the General Data Protection Regulation and is not limited to the rights under C h a p t e r III GDPR. In contrast, Spoerr, in Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, status 5/2022, Art. 26 GDPR para. 59.

[217] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 GDPR para. 29. The joint controllers are j o i n t l y liable even without an agreement pursuant to Art. 26 para. 1 sentence 2 GDPR; however, this helps with the internal equalisation of liability pursuant to Art. 82 para. 5 GDPR, DSK, Kurzpapier No. 16 (fn. 27), p. 4.

a) Mutual obligation and liability

The agreement between the jointly responsible parties has the effect of concluding a contract between the parties; its content is binding for each of the parties involved (principle of "pacta sunt servanda", Section 241 (1) BGB). 188

Like any contract, the agreement ideally avoids legal ambiguities and the resulting liability disputes if it is properly drafted. This i s of particular importance if the parties involved are not in equal negotiating positions. In such a case, the transparency requirement helps to protect the contractual symmetry of the parties to the agreement and to uncover their imbalance as far as possible.[218] In addition, the agreement fulfils an important function of preserving evidence and attribution, taking into account the requirements of Art. 82 GDPR in particular. This applies not only, but also especially in connection with a possible compensation of damages between the parties to the agreement. 189

For actions within the relationship between the joint controllers, jurisdiction arises from Art. 79 para. 2 GDPR: This is because the legal relationship between joint controllers exists by law - only its formulation taking into account the requirements of Art. 26 GDPR is carried out individually by agreement - and establishes a joint and several debt in the external relationship. In accordance with the general principles of civil and administrative law, the courts that would also have jurisdiction for an action brought by a data subject against one of the joint and several debtors are responsible for the internal settlement between joint and several debtors.[219] 190

b) Binding effect vis-à-vis third parties

aa) Binding effect vis-à-vis data subjects, in particular Art. 26 (3) GDPR

Joint controllers must adhere to the content of their agreement vis-à-vis data subjects, Art. 26 (2) GDPR (para. 175).

191

However, the provisions of the agreement are not binding on data subjects insofar as they can assert their rights with and against each of the joint controllers in accordance with Art. 26 (3) GDPR - regardless of any explicit assignment of responsibility and/or the designation of a contact point.[220] If necessary, the indicated 192

[218] Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 10.

[219] ECJ, judgment of 15 June 2017, C-249/16 (Kareda), para. 31 f.

[220] There is also no teleological reduction in the event that it is objectively recognisable to the data subjects that one of the joint controllers "has no decision-making power and therefore cannot fulfil the obligation alone". This would contradict the regulatory purpose of Art. 26 GDPR. See, however, Hacker, Mehrstufige Informationsanbieterverhältnisse zwischen Datenschutz und Störerhaftung, MMR 2018, p. 779, 780, 783 f.

The data controller shall forward the data subject's enquiry to the internally responsible body in accordance with the agreement.[221]

193 Art. 26 para. 3 GDPR thus supplements the allocation of obligations under liability law in Art. 82 para. 4 GDPR at the primary claim level: Art. 82 para. 4 in conjunction with para. 2 sentence 1 GDPR also stipulates joint and several liability, but only applies to the settlement of claims. An obligation can therefore also be implicitly derived from Art. 26 para. 3 GDPR for each party to the agreement to influence the other controllers within the scope of the "primary obligations" under data protection law (insofar as it cannot or does not have to fulfil these obligations itself).[222]

194 Art. 26 para. 3 GDPR also establishes a basis for attribution for the joint controllers that goes beyond the mere "liability regulation": For example, a controller who wishes to base their data processing on the consent of the data subject must allow themselves to be held responsible for the actions of the joint controllers that call into question the voluntary nature of the consent, insofar as these are based on a division of labour. As a result, the consent given to the data subject may prove to be invalid.

195 The international jurisdiction for the assertion of claims by a data subject against one of the joint controllers arises from Art. 79 para. 2 GDPR as a lex specialis[223] to the international jurisdiction standards. Art. 79 para. 2 sentence 1 GDPR stipulates that the courts of the Member State in which the controller has an establishment (see EC 22 sentences 2 and 3 GDPR) have jurisdiction for all actions against a controller. According to Art. 79 para. 2 sentence 2 half-sentence 1 GDPR, the data subject also has the option of bringing an action before the courts of the Member State in which the data subject is habitually resident.[224] has their habitual residence. This does not apply if the controller is an authority of a Member State which has acted in the exercise of its public powers, Art. 79 para. 2 sentence 2 clause 2 GDPR. The local jurisdiction is then determined by the national provisions, namely in accordance with the provisions of the Administrative Court Code for the public sector and Section 44 BDSG as a special regulation for the non-public sector.

[221] Knoblauch, in: Wilde/Ehmann/Niese/Knoblauch, Data Protection in Bavaria, status 11/2018, Art. 26 GDPR para. 19.

[222] Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 36.

[223] EG 147 GDPR.

[224] The concept of "habitual residence" is associated with a certain degree of permanence and the existence of subjective components, although the details are still unclear. The European Court of Justice d e f i n e s "habitual residence" in a different context as the place "which the person concerned has chosen as the permanent or habitual centre of his interests with a view to m a k i n g it permanent", whereby "account must be taken of all the relevant factual elements", ECJ, judgment of 15 September 1994, C-452/93 P, para. 22.

bb) Binding effect vis-à-vis supervisory authorities

The jointly responsible parties must also adhere to the content of their agreement vis-à-vis the supervisory authorities. 196

However, the supervisory authorities are not bound by the provisions of the agreement either with regard to the question of the categorisation of the parties as joint controllers or with regard to a contact point that may be named .[225] 197

The authorities can therefore contact any of the joint controllers in order to exercise their powers pursuant to Art. 58 GDPR; in this respect, they are equipped with extensive powers of investigation to clarify the facts. The supervisory authorities only have to assess the defined allocation of duties as part of their judgement o n the measures to be taken and the addressees of the measures.[226] This is also in line with the principle of proportionality in accordance with EC 129 sentence 5 GDPR. When exercising discretion, the central purpose of the GDPR, i.e. ensuring the effective protection of data subjects (Art. 1 para. 2 GDPR), must always be taken into account. In this respect, irrespective of the particular situation of joint responsibility, the effectiveness of the elimination of a data protection breach - in terms of time and other qualitative aspects - can be used as a guiding criterion.[227] 198

However, supervisory authorities cannot invoke Art. 26 para. 3 GDPR, as it only expressly refers to "the data subject" as the authorised party. This is relevant, for example, if the joint controllers do not regulate who is subject to the obligation to notify the supervisory authority of personal data breaches under Art. 33 GDPR. In the absence of the relevance of Art. 26 para. 3 GDPR, the general principles of Art. 26 GDPR with the guiding rule of para. 1 sentence 1 GDPR must be applied in such a case: Several controllers are jointly responsible.[228] 199

However, the question of determining the lead supervisory authority in the event of joint responsibility remains unresolved in this context. The lead supervisory authority - and the exercise of its powers - cannot be determined by the (joint) controllers themselves (prohibition of so-called "forum shopping")[229] 200

[225] European Data Protection Board, Guidelines 8/2022 on the determination of the lead supervisory authority of a controller or processor, Version 2.0, as of 3/2023, para. 32, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82022-identifying-controller- or-processors-lead_en. Different view Ingold, in: Sydow/Marsch, GDPR - BDSG, 3rd ed. 2022, Art. 26 GDPR para. 10.

[226] In addition, the statutory discretionary limits including the principles of expediency and proportionality, see also EC 129 sentence 5 GDPR, as well as the general principles of fault selection must be taken into account, Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2022, Art. 26 GDPR para. 61. According to Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021,
Art. 26 GDPR para. 37a, the selection of interferers under data protection law is not based on the provisions of the administrative procedure laws; only the General Data Protection Regulation is decisive.

[227] BVerwG, judgement of 11 September 2019, 6 C 15/18, para. 30 f.

[228] Martini, in: Paal/Pauly, GDPR - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 22.

[229] European Data Protection Board, Guidelines 8/2022 (fn. 225), para. 33 f.

and the General Data Protection Regulation does not contain any regulation for the case of joint responsibility: In principle, Art. 55 et seq. GDPR stipulate requirements for the supervisory authorities.[230] According to Art. 55 para. 1 GDPR, the principle applies that each supervisory authority is responsible in the territory of its own member state. However, several joint controllers may be located in different Member States or areas of responsibility (in Germany, different responsibilities for each federal state, cf. Art. 51 para. 1 GDPR in conjunction with Section 40 BDSG, Art. 18 BayDSG for the non-public sector, Art. 15 BayDSG for the public sector). The General Data Protection Regulation makes no provision for this constellation or for joint responsibility in general. In particular, Art. 56 GDPR, which determines the lead supervisory authority in the case of several branches of a controller or processor ("one-stop shop principle"), does not apply to the determination of the lead supervisory authority for joint controllers, as this provision explicitly only deals with a single controller.[231]

201 The European Data Protection Board therefore advises the following procedure in its "Guidelines 8/2022 on identi- fying a controller or a processor's lead authority":[232] If the joint controllers are based in the European Union or the European Economic Area, the main establishment or sole establishment must be determined separately for each of the joint controllers. The lead supervisory authority pursuant to Art. 55 para. 1 or Art. 56 para. 1 GDPR is the competent supervisory authority for the respective joint controller.[233] However, a single lead supervisory authority is not designated for the joint controllers. If differences arise in practice between the competent supervisory authorities, it is recommended to organise the cooperation in accordance with the principles of Art. 60 et seq. GDPR and work together to reach a consensus;

[230] §§ However, Sections 27 (5) and 40a of the draft of a first law to amend the Federal Data Protection Act (BT-Drs. 20/10859) currently provide for "forum shopping" to a certain extent for joint controllers in the non-public sector.

[231] However, each of the joint controllers may of course have a main or sole establishment within the meaning of Art. 56 (1) GDPR.

[232] European Data Protection Board, Guidelines 8/2022 (fn. 225), Annex No. 2 d, p. 13 f. Schneider, Kollision von Joint Controllership und One-Stop-Shop, ZD 2020, p. 179, 181 et seq. on the other hand, proposes solutions for determining a single lead supervisory authority, but also points out the associated problems: (1) broad interpretation of the term "main establishment" within the meaning of Art. 56 para. 1 GDPR (main establishment at the centre of gravity of the respective data processing) - problematic in t h e case of equal distribution of data processing and generally regarding the criteria for determining the c e n t r e of gravity; (2) autonomous determination by the joint controllers (see also Article 29 Working Party, Guidelines for the determination of the lead supervisory authority of a controller or processor, status 4/2017, WP 244 rev. 01, p. 8 f., Internet: https://ec.europa.eu/newsroom/ar- ticle29/items/611235/en) - in contradiction to EC 36 sentence 2 GDPR and risk of abuse, moreover, agreements on jurisdiction are alien to public law; (3) introduction of a priority principle (the supervisory authority that acts first) - lacks flexibility; (4) decision by a (p o s s i b l y higher) authority, cf. section 39 of the Administrative Offences Act, Art. 65 para. 1 letter b GDPR combined with priority principle.

[233] European Data Protection Board, Guidelines 8/2022 (fn. 225), p. 14.

If necessary, a dispute resolution must be carried out by the European Data Protection Board, Art. 65 GDPR.

VI. Excursus: Directive (EU) 2016/680 (combating criminal offences)

202 In the case of joint controllership for the processing of personal data for the purposes of combating criminal offences, Art. 26 GDPR applies in national implementation of Art. 21 Directive (EU) 2016/680[234] pursuant to Art. 2 sentence 1 and Art. 28 para. 2 sentence 2 BayDSG in accordance with Art. 30 BayDSG.

203 According to Art. 26 para. 1 sentence 3 GDPR, the indication of the contact point is mandatory for the data subjects, Art. 30 sentence 1 BayDSG. However, the provision of Art. 26 para. 2 GDPR does not apply, Art. 30 sentence 2 BayDSG.

204 Art. 21 para. 2 Directive (EU) 2016/680 also allows the member states to create a provision comparable to Art. 26 para. 3 GDPR, but does not oblige them to do so. Germany has made use of this option, for example, in Section 63 sentence 4 BDSG.

[234] See footnote 2.

VII. Conclusion

When examining the existence of joint controllership, it always depends on the individual case, in which the criteria developed above must be measured against the actual processes and structures of the specific data processing, taking into account the protection objectives of Art. 26 GDPR and the General Data Protection Regulation as a whole, with a "pragmatic approach" that "places greater emphasis on the freedom of discretion in deciding on the purposes and on the scope for decision-making".[235] Despite the case law of the European Court of Justice, the distinction between joint controllership and order processing and parallel controllership harbours considerable difficulties. In particular, the correct categorisation of participation in processing is made more difficult by the fact that the Court of Justice sets low requirements for the actual contribution to a decision on the means and purposes of processing. The background to this broad interpretation is clearly the interest in ensuring that there are no gaps in protection for the data subjects.[236] 205

The requirements established by the case law of the European Court of Justice for the assumption of joint responsibility are rather low overall. In legal reality - especially due to increasing digital cooperation - there will be far more applications for joint responsibility than currently appears to be the case, for example due to the existence of corresponding agreements.[237] In most cases, the joint controllers will not even be aware in practice that they have (become) joint controllers in the legal sense. 206

Jointly responsible processing can certainly improve the legal position of data subjects due to joint and several liability in accordance with Art. 26 para. 3, Art. 82 para. 4 in conjunction with para. 2 sentence 1 GDPR. For providers of complex and integrated processing, however, the liability risk increases considerably, albeit with the regulation limiting liability to the phases of actual participation. In this respect, the effects on practice are probably considerable, but the details are still open and the legal uncertainty is great. Against this background, (joint) controllers and processors should systematically and clearly define, delimit and document their respective roles and responsibilities before the start of a processing activity in order to be able to fulfil their respective data protection obligations on this basis. 207

[235] This was already the case at the time and is still the case today Article 29 Working Party, Opinion 1/2010 (fn. 7), p. 16.

[236] On the possible risks for the persons concerned, but also in relation to unreasonable or unfair liability, Opinion of Advocate General Bobek of 19 December 2018 in Case C-40/17 (Fashion ID), paragraphs 91, 93.

[237] Hanloser/Koglin, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 3rd ed. 2021, VI. Mehrparteien-Vereinbarung zwischen gemeinsam Verantwortlichen bei Online-Angeboten, Note 1 even speak of a "mass phenomenon", and Martini, in: Paal/Pauly, DSGVO - BDSG, 3rd ed. 2021, Art. 26 GDPR para. 42 fears that Art. 26 GDPR itself contributes to a "diffusion of responsibility" in data protection law.