

Laue / Nink / Kremer

European Data Protection Law in Practice

A Practitioner's Guide



Laue / Nink / Kremer
European Data Protection Law in Practice

European Data Protection Law in Practice

A Practitioner's Guide

by

Philip Laue
Judith Nink
Sascha Kremer

2025



Published by

Nomos Verlagsgesellschaft mbH & Co. KG, Waldseestraße 3-5, 76530 Baden-Baden, Germany,
email: vertrieb@nomos.de

Co-published by

Verlag C.H.Beck GmbH & Co. KG, Wilhelmstraße 9, 80801 München, Germany,
email: bestellung@beck.de

and

Hart Publishing, Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, United Kingdom,
online at: www.hartpub.co.uk

Published in North America by Hart Publishing,
An Imprint of Bloomsbury Publishing 1385 Broadway, New York, NY 10018, USA
email: mail@hartpub.co.uk

ISBN 978 3 7560 1744 7 (NOMOS Print)

ISBN 978 3 7489 4406 5 (NOMOS ePDF)

ISBN 978 3 406 82592 7 (C.H.BECK)

ISBN 978 1 5099 8188 5 (HART)

First Edition 2025

© Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden 2025. Overall responsibility for manufacturing (printing and production) lies with Nomos Verlagsgesellschaft mbH & Co. KG.

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use a fee is payable to »Verwertungsgesellschaft Wort«, Munich, Germany.

CONTENTS

Authors	VII
Literature	IX
Abbreviations	XV
Chapter 1 Introduction	1
Chapter 2 Lawfulness of the processing	38
Chapter 3 Obligation to inform	83
Chapter 4 Rights of the data subject	99
Chapter 5 Roles and responsibilities in the processing of data	131
Chapter 6 International processing of data	161
Chapter 7 Right to erasure and data protection-compliant erasure	181
Chapter 8 Data protection officer	200
Chapter 9 Technical data protection	218
Chapter 10 Organisational data protection	235
Chapter 11 Employee data protection	276
Chapter 12 Supervisory authorities	285
Chapter 13 Liability, Penalties and remedies	300
Chapter 14 Data protection and Artificial Intelligence	321
Index	331

Authors

Philip Laue has been working in the field of data protection law since 2005, first as a research assistant at the University of Kassel, Germany, and later as a lawyer and in-house lawyer at different DAX-listed companies. As a lecturer at the FernUniversität Hagen, Germany, and as a speaker at events and conferences, he regularly speaks on data protection topics. He is also the author of numerous articles on data protection.

Judith Nink has been dealing with data protection, data security and IT law for about 20 years. Her day-to-day work focuses on advising clients (from start-ups to DAX-listed companies) on international data transfers and the entry of non-European companies into the EU market. Previously, she headed the legal departments of technology companies and built interdisciplinary data protection and security teams. She is the author of numerous publications, a lecturer at the FernUniversität in Hagen in the field of employee data protection, and a speaker on data protection and security topics at professional and interdisciplinary conferences and events.

Sascha Kremer is a specialist in IT law and has been dealing with data protection law since 2009. He provides his clients with highly specialized advice at the interface between technology and law. In addition to data protection law, his main areas of expertise include the regulation of artificial intelligence as well as IT- and Data-related collective labor law. As a lecturer at two universities and a speaker at professional and interdisciplinary conferences and events, he trains and educates lawyers, data protection officers, works councils, managers and HR professionals. He is co-editor and author of numerous publications.

Chapter 1 Introduction

A. General	1
B. Scope of the General Data Protection Regulation	3
I. Material scope of the General Data Protection Regulation	5
1. Processing of data	6
2. Storage in a filing system for non-automated processing	8
3. Personal reference of the data	9
a) <i>Identifiability</i>	10
aa) <i>Anonymous data</i>	16
bb) <i>Pseudonymised data</i>	20
cc) <i>Encrypted data</i>	27
b) <i>Natural person</i>	30
II. Personal scope	33
III. Territorial scope	35
1. Scope of the General Data Protection Regulation	36
a) <i>Principle of establishment under Art. 3 para. 1</i>	37
aa) <i>Effective and actual exercise of an activity</i>	38
bb) <i>Processing in the context of the establishment's activities</i>	40
cc) <i>Place of processing</i>	44
b) <i>Market place principle according to Art. 3 para. 2</i>	45
aa) <i>Offer of goods and services</i>	46
bb) <i>Behavioural observation</i>	50
c) <i>Processing outside the scope of Art. 3 para. 2 GDPR</i>	52
2. Territorial scope within the EU	53
a) <i>Domicile principle</i>	55
b) <i>Territoriality principle</i>	58
c) <i>Special case of consent</i>	59
aa) <i>Art. 8 para. 1</i>	61
bb) <i>Art. 9 para. 2 letter a</i>	62
d) <i>Choice of law clauses</i>	65
IV. Opening clauses and special processing situations	68
1. Opening clauses in individual regulations	69
2. Processing in the employment context	73
3. Processing for scientific research and statistical purposes	74
a) <i>Data minimisation and right to object</i>	76
b) <i>Privileges</i>	78
4. Delegated acts and implementing acts of the EU Commission	80
5. General Data Protection Regulation and ePrivacy Directive	82
V. Processing principles and accountability obligation	85

A. General

Since 25 May 2018, the General Data Protection Regulation has been directly **ap- 1**
licable law in every member state of the European Union.¹ This was preceded by
various drafts for a Regulation by the EU Commission², the European Parliament³ and

¹ The member states of the European Economic Area (EEA), i.e. Iceland, Liechtenstein and Norway, are not directly covered by the scope of the General Data Protection Regulation, as it is only aimed at EU member states. However, under the EEA Treaty, they are obliged to implement the requirements of the European Single Market in the same way as EU Member States. This includes the General Data Protection Regulation as a text of relevance to the EEA.

² European Commission proposal of 25 January 2012 (COM(2012) 11 final; 2012/0011 (COD)).

³ Decision of the European Parliament of 12 March 2014 at first reading on the above-mentioned proposal of the European Commission (Interinstitutional Dossier of the Council of the European Union of 27 March 2014, 2012/0011 (COD); 7427/1/14, REV 1).

Chapter 1 Introduction

the Council of the European Union.⁴ Today's General Data Protection Regulation is therefore an overall compromise that those stakeholders involved agreed on after a total of ten negotiation meetings ("trilogue").

- 2 More than five years after its applicability, the General Data Protection Regulation continues to present enterprises with a wide range of legal and factual **challenges** across all areas of the Regulation. However, a reform and adaptation of the regulations in the sense of a "GDPR 2.0" is not to be expected in the foreseeable future. The political differences and objectives at both national and supranational level within the European Union are currently too great to successfully conclude renewed trilogue negotiations on the General Data Protection Regulation. It seems more likely that attempts at European level will be made to use data-specific legislative projects – for example in the form of an AI Act and the Data Act – to indirectly "reform" the General Data Protection Regulation in individual matters. It remains to be seen to what extent this will lead to simplification and greater legal certainty in day-to-day business or raise new legal questions – for example, on issues relating to the data protection regulatory system in Europe.

B. Scope of the General Data Protection Regulation

- 3 Whether and to what extent the General Data Protection Regulation applies cannot be answered in practice in an abstract and general manner. The decisive factor is the specific context of the processing. The following questions arise, for example: Does the specific processing, the specific data protection incident ("Incident"), the intended introduction of an IT system or a specific request for information from a data subject fall within the scope of the General Data Protection Regulation?
- 4 In order to answer these questions, the General Data Protection Regulation distinguishes between the material, the personal and the territorial scope. In relation to the specific event, this means
 - Is the data concerned personal data (**material scope**)?
 - Is the enterprise the addressee of the General Data Protection Regulation in connection with the respective processing (**personal scope**)?
 - Does the respective processing take place at a location that is covered by the General Data Protection Regulation (**territorial scope**)?

The provisions of the General Data Protection Regulation must only be observed in operational practice if all questions are answered in the affirmative. Furthermore, from a territorial perspective, enterprises may be faced with the question of the extent to which any **special national provisions** must be additionally considered due to flexibility clauses (→ mn. 53 et seq.).

I. Material scope of the General Data Protection Regulation

- 5 According to Art. 2 para. 1 GDPR, the General Data Protection Regulation applies "*to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*". Whether processing falls within the material

⁴ Interinstitutional dossier of the Council of the European Union of 11 June 2015, 2012/0011 (COD); 9565/15.

B. Scope of the General Data Protection Regulation

scope of the General Data Protection Regulation must therefore be assessed according to,

- whether processing is taking place,
- whether the subject of the processing is personal data,
- whether the processing is fully or partially automated **or** whether the data is intended for storage in a filing system.

Note: Forward displacement of the scope for certain obligations

The controller must comply with certain obligations under the General Data Protection Regulation even before a specific processing takes place. This applies both to his obligations under Art. 25 para. 1 and 2 GDPR (→ Chapter 9 mn. 5 et seq.) and to the possible performance of a data protection impact assessment pursuant to Art. 35 and 36 GDPR (→ Chapter 10 mn. 35 et seq.). In order to ensure that he has fulfilled these obligations at the time of initial processing.

1. Processing of data

The term “**processing**” is defined in Art. 4 no. 2 GDPR. It refers to “*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*”. The definition is broad. It covers not only typical data usage such as storage, transmission or modification of data, but in principle **all** forms of handling personal data from collection to final destruction. It is irrelevant whether the processing is manual, i.e. subject to additional requirements (→ mn. 8) or automated, i.e. in IT systems. 6

Furthermore, with regard to the question of whether a processing takes place, the General Data Protection Regulation does not differentiate between the intensity or duration of the respective processing or the technology used in connection with the processing.⁵ Therefore, even the **short-term** use of a small amount of seemingly insignificant personal data falls in principle within the scope of the General Data Protection Regulation. 7

Example:

Even if personal data is only temporarily stored on an IT system, for example in the cache of a browser, this constitutes processing in the same way as the mere display of a file on a screen or the transfer of a mobile storage medium.

Note: Processing of test data

If data contains information that relates to an identified or identifiable natural person, the use of this data to test IT systems also constitutes processing that is relevant under data protection law.⁶ In order to avoid this fictitious (synthetic), anonymous or anonymised data (→ mn. 16) should be used as test data, provided that tests can still be carried out reasonably.

2. Storage in a filing system for non-automated processing

Despite the conceivably broad definition of processing, not all non-automated processing of personal data is covered by the material scope of the General Data Protection 8

⁵ “technology-neutral” see recital 15.

⁶ CJEU 5 December 2023 – C-683/21, BeckRS 2023, 34702 mn. 53 et seq.

Chapter 1 Introduction

Regulation, but only if the data is intended for storage in a “**filing system**” in accordance with Art. 2 para. 1 GDPR. Art. 4 no. 6 GDPR defines what this means. It refers to “*any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis*”. Again, a very broad understanding of the term must be assumed. Correspondingly, according to recital 15, only unstructured (non-electronic) files or collections of files and their cover pages are excluded from the scope of the Regulation, regardless of how much or which personal data they contain. However, this exception is likely to play only a very minor role in business practice. On the one hand, only in the rarest of cases would a collection of paper be randomly filed and not organised according to any criteria in a file folder. Secondly, a filing system is generally assumed from the moment an initially unstructured paper-based collection of data is scanned and thus made available electronically and can therefore generally be searched and analysed according to various criteria.⁷

Note: Data handling = processing in a filing system

Due to the broad definition of the term “processing” and the term “filing system”, enterprises should in principle carefully check any handling of personal data, even outside of automated processing, to ensure that it does not qualify as a structured data collection and therefore is subject to the General Data Protection Regulation.

3. Personal reference of the data

- 9 The General Data Protection Regulation regulates the processing of **personal data**. According to Art. 4 no. 1 GDPR, this is “*any information relating to an identified or identifiable natural person (hereinafter “data subject”)*”. A personal reference is therefore not only given when a person is directly identified by the information, but already when the information is suitable for identifying the person.

a) Identifiability

- 10 According to Art. 4 no. 1 GDPR, a natural person is **identifiable** if it can be identified “*directly or indirectly*”. As examples, Art. 4 no. 1 GDPR mentions in particular the possibility of assigning a person
- to an identifier such as a name,
 - to an identification number,
 - to location data,
 - to an online identifier or
 - one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 11 This is not an exhaustive list of possible links, but merely a list of frequently encountered assignments of persons to certain data in practice. In doing so, the legislator takes into account the progressive development of technology with location data and online identifiers as examples of possible assignment objects. As examples of **online identifiers**, the European legislator mentions IP addresses and cookie identifiers provided by the data subject’s device or software applications and tools or protocols, as well as other identifiers such as radio frequency identification tags.⁸
- 12 However, the exemplary list in Art. 4 no. 1 GDPR does not mean that such an identifier is always personal data, regardless of the circumstances of the individual case, just

⁷ Ehmann/Selmayr/Klabunde GDPR Art. 4 mn. 35; Gola/Heckmann/Gola GDPR Art. 4 mn. 60.

⁸ Recital 30.

B. Scope of the General Data Protection Regulation

because such an identifier is associated with a natural person. Rather, the European legislator clarifies that it depends in principle on the means available for this purpose whether data can be traced back to a person and thus whether a personal reference is given. All **means** “likely to be used by the controller or another person to identify the person directly or indirectly” must be considered.⁹ All “objective factors, such as the costs of and the amount of time required for identification” must be taken into account when examining which means are reasonably likely to be used for identification¹⁰ In this context “the available technology at the time of the processing and technological developments” must be considered.¹¹

Note: Personal reference and joint control

It is not necessary for all identifiers to be in the hands of a single person.¹² If, in the case of joint control (→ Chapter 5 mn. 15 seq.), not every controller has the information required for the identification of the person concerned, this does not prevent the personal reference of the data processed under joint control.¹³

By including cost factors and time expenditure as criteria for identifiability, which can vary from person to person, the European legislator makes it clear that the reference to a person must always be determined **in relative terms** and not the abstract potential of the entire world to attribute the data to an individual person.¹⁴ The relativity of the reference to a person has been confirmed in several decisions by both the CJEU and the EGC.¹⁵ According to the CJEU, the means “likely reasonably to be used either by the controller [...] or by any other person, to identify that person, without, however, requiring that all the information enabling that person to be identified should be in the hands of a single entity” must be taken into account.¹⁶ Correspondingly, according to the CJEU, data is only personal data for the person that “reasonably has means enabling that datum to be associated with a specific person”.¹⁷ It is irrelevant whether identification is intended or not. The only decisive factor is whether an identifiability can be assumed according to objective standards. 13

Note: Relativity of the personal reference and pseudonymous data

The EGC has clarified that pseudonymous data is only personal data for the recipient if (i) he has the right to access the additional information available to a third party for identification purposes and if (ii) this access is also practically feasible (→ mn. 20 seq.).¹⁸

The relativity of the personal reference also applies to **IP addresses**. Accordingly, recital 30 states that online identifiers can leave traces that can be used “combined” with unique identifiers and other information to identify a person. In addition, the CJEU expressly stated that, in any event, a **dynamic** IP address does not in itself constitute information relating to a “specific natural person”, since it does not directly reveal the 14

⁹ Recital 26.

¹⁰ Recital 26.

¹¹ Recital 26.

¹² CJEU 19 October 2016 – C-582/14, NJW 2016, 3579 mn. 43; 7 March 2024 – C-604/22, BeckRS 2024, 3638 mn. 40.

¹³ CJEU 7 March 2024 – C-604/22, BeckRS 2024, 3638 mn. 45 et seq.

¹⁴ Roßnagel/Kroschwald ZD 2014, 495 (496 et seq.).

¹⁵ CJEU 19 October 2016 – C-582/14, NJW 2016, 3579 mn. 38 (still on the old legal situation); 9 November 2023 – C-319/22, BeckRS 2023, 30962 mn. 45 et seq.; CJEU 26 April 2023 – T-557/20, ZD 2023, 399 mn. 105.

¹⁶ CJEU 9 November 2023 – C-319/22, BeckRS 2023, 30962 mn. 45.

¹⁷ CJEU 9 November 2023 – C-319/22, BeckRS 2023, 30962 mn. 46.

¹⁸ CFI 26 April 2023 – T-557/20, ZD 2023, 399 mn. 105.

Chapter 1 Introduction

identity of the owner of the computer to which the address is assigned, nor the identity of any other person who might use that computer.¹⁹ In the specific case to be decided, the CJEU ultimately assumed a personal reference solely because website operators generally have **legal means** under German law to obtain the additional information required for identification from the internet access provider in the event of cyberattacks, for example.²⁰

Note: IP addresses and time component

With regard to (dynamic) IP addresses, it is of decisive importance whether the controller has an at least abstract legal possibility of obtaining the necessary identification features of a natural person behind the address and whether this legal possibility is (still) realisable in practice. The answer to the question of personal reference therefore also has an important temporal component. Even if an IP address was originally personal data, a reference to a person ceases to exist at any rate at the point in time at which the controller no longer has an originally existing legal possibility of identification. However, the same must also apply if the storage period of the IP address is so short that a theoretically existing legal possibility of access is not practically enabled in terms of time.

- 15 Finally, the European legislator clarifies that it is not important which means are specifically used in the individual case, but which “*means are reasonably likely to be used*” according to general judgment.²¹ For the question of whether identifiability exists, all means that are reasonably available to the processing body for identification must therefore be taken into account, regardless of whether or not it makes use of these possibilities in the specific individual case. The European legislator mentions the following objective factors:²²

- Cost of identification;
- time required for identification;
- available technologies;
- technological developments.

Example:

An enterprise stores data in different databases without merging them. However, merging and thus identification would generally be possible with a reasonable amount of time and cost, taking into account the analysis tools typically available on the market.

In this case, it is personal data regardless of whether the data is actually merged.

aa) *Anonymous data*

- 16 The term anonymous or anonymised data is not defined in the General Data Protection Regulation. However, the European legislator presupposes the existence of anonymous data (“*anonymous information*”) in recital 26. In general, **anonymous data** refers to individual details about a person that cannot be attributed to them by anyone.²³ Personal data is anonymised if it has been altered in such a way that the individual details about personal or factual circumstances can no longer be attributed to a specific or determinable natural person, or only with a disproportionate amount of time, cost and labour. Data can be anonymised by filtering out information without personal reference from a pool of personal data and using it for planning or statistical purposes,

¹⁹ CJEU 19 October 2016 – C-582/14, NJW 2016, 3579 mn. 38.

²⁰ CJEU 19 October 2016 – C-582/14, NJW 2016, 3579 mn. 47, 49.

²¹ Recital 26.

²² Recital 26.

²³ Roßnagel/Scholz MMR 2000, 721 (723).

B. Scope of the General Data Protection Regulation

for example. Another possibility for anonymisation is the irreversible erasure of the identification features in the database, which removes the personal reference (for the legal ground for anonymisation → Chapter 7 mn. 14).²⁴

Note: Aggregated data and anonymisation

In principle, anonymisation through aggregation of personal data is also conceivable. This involves summarising a number of individual pieces of data into a single value, which as such no longer has any personal reference. A typical use case here is statistical analyses of employee surveys in the enterprise, in which the answers of individual employees are summarised and, e.g., only output as the average value of a team or department. If anonymisation is to be achieved through data aggregation, particular attention must be paid to the correct minimum group size, a necessary minimum number of cases, if applicable, and the level of aggregation (i.e. which data is aggregated at what granularity). In addition, it must be ensured that a personal reference is not revived by combining different aggregated data sets with each other and thus – for example through an exclusion procedure – making it possible to draw conclusions about a specific person.

Anonymous data should not be covered by the **scope** of the General Data Protection Regulation, meaning that their processing is not subject to any restrictions under data protection law.²⁵ If the identifiability of individuals is not necessary to achieve the purpose of the respective data use, the use of anonymous data is recommended. This not only ensures data-saving processing that protects the data subject, but also avoids the restrictions of processing personal data and the associated technical and organisational effort. 17

Example 1:

Telematics data such as location data and driving speed without identifiable features such as vehicle identification number or licence plate number can play an important role in traffic monitoring and control, e.g. to determine the traffic flow for dynamic traffic control.

Example 2:

The system tracks who and when has bought which products. The buyer's identification data is later deleted.

In practice, it can be difficult to distinguish between anonymous and personal data. Given the information technologies available today, it is rarely possible to completely rule out re-identification. Rather, “**de facto**” **anonymity** is the standard when it comes to anonymous data. Although re-identification is theoretically possible, it is so disproportionate in view of the effort required that identification is not to be expected according to general life experience or the state of the art in science and technology.²⁶ Whether the data is anonymous in a specific individual case therefore depends on the risk of re-identification (so-called de-anonymisation). The available or obtainable additional knowledge of the controller, current and future technical possibilities of processing as well as potential effort and the available resources and time must be taken into account.²⁷ The additional knowledge of a third party may also be relevant here. On the one hand, it must be examined whether a personal reference still exists despite the 18

²⁴ Roßnagel ZD 2021, 188 (189). For possible anonymisation techniques, see also Article 29 Working Party WP 216 sentence. 32 et seqq.; Schwartmann/Jaspers/Lepperhoff/Weiß/Meier Practice Guide p. 30 et seqq.

²⁵ Recital 26; CJEU 5 December 2023 – C-683/21, BeckRS 2023, 34702 mn. 57.

²⁶ Roßnagel/Scholz MMR 2000, 721 (724); Härting NJW 2013, 2065 (2066).

²⁷ Roßnagel/Scholz MMR 2000, 721 (724).

Chapter 1 Introduction

controller's own anonymisation measures because the controller can reasonably use the additional knowledge available to third parties to identify the data subject (→ mn. 13).²⁸ Secondly, it must be assessed to what extent it is objectively likely that third parties will come into possession of the data processed by the controller with the aim of de-anonymisation and that there is a **risk of re-identification** due to the additional knowledge they have or can acquire. Depending on the criticality of the data and the specific application scenario, the possibility of third parties gaining unauthorised access to the data (e.g. through a hacker attack) may also play a role. Unlike the controller (→ mn. 13), an attacker – who is often unknown to the controller – can generally be expected not to be deterred by any prohibitions.²⁹

Note: “Attacker model”

In order to determine the risk of re-identification by third parties, a so-called “attacker model” should be used as a basis. This involves determining, based on the respective context of use of the data, whether the controller is likely to have to reckon with potential attackers from an objective point of view. If this is the case, the controller should examine what reasonably conceivable knowledge and skills the attacker has and, considering the technical and organisational measures taken by the controller, assess how likely, simple and promising the use of such knowledge and skills is.³⁰ In addition to targeted attacks, this objective assessment should also take into account situations in which third parties come into possession of the data rather by chance, but due to objectively recognisable risks already present in the controller.³¹

- 19 Because the risk of re-identification is a decisive differentiator between anonymous and personally identifiable data, an enterprise must not stop at a **one-off risk analysis** when considering the anonymity of data. Especially when anonymous data is used for data analysis (for example in connection with “AI” and “big data applications” or “web tracking tools”), it must be regularly checked whether additional knowledge acquired over time now makes it possible to identify the originally anonymous data, for example through additional data (if applicable also in other databases) or through improved analysis and linking options. From this point onwards, they are subject to the scope of the General Data Protection Regulation as personal data. If the enterprise has not taken sufficient precautions for data protection-compliant processing in this case, there is a considerable risk that the processing will be unlawful from this point onwards.

Note: Preliminary consultation with supervisory authorities for the processing of anonymous data

If the use of anonymous data is a significant part of an enterprise's business model and there is uncertainty as to whether it is really anonymous data, the enterprise should contact the competent supervisory authority before processing in order to minimise data protection risks. It should not only be clarified whether, in the opinion of the supervisory authority, the data is anonymous data, but also which technical and organisational measures, if applicable, (permanently) eliminate the risk of a (subsequently arising) personal reference.

²⁸ CJEU 19 October 2016 – C-582/14, NJW 2016, 3579 mn. 45.

²⁹ Schwartmann/Jaspers/Lepperhoff/Weiß/Meier Practice Guide p. 18.

³⁰ Schwartmann/Jaspers/Lepperhoff/Weiß/Meier Practice Guide p. 18.

³¹ Schwartmann/Jaspers/Lepperhoff/Weiß/Meier Practice Guide p. 5 et seq.

B. Scope of the General Data Protection Regulation

bb) Pseudonymised data

Pseudonymous data constitutes a special case of personal data. According to Art. 4 no. 5 GDPR, “**pseudonymisation**” means the processing of personal data in such a way that *“the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.”* Pseudonymous data is usually created by replacing the identifier of a data subject (such as their name) in a database with an identifier (“pseudonym”) that does not itself allow any conclusions to be drawn about the identity of the data subject. However, pseudonymisation can also be assumed, for example, if a data collection only makes a personal reference recognisable for those who have the necessary algorithm (e.g. through coding).³² In addition, it must always be ensured that the identifiers are stored separately from the pseudonymised data and are protected against access by unauthorised persons or third parties by means of suitable protective measures. There must therefore be two data collections in order for personal data to be pseudonymised: On the one hand, the data collection without identifiers (but with the pseudonym), and on the other hand, the data collection with the identifiers (and also the pseudonym to ensure that they are associated with each other).

Example: Pseudonyms

Personnel number, identification number, invented name when using online services, user ID, vehicle identification number (VIN). However, if the personnel number is known to every employee in the enterprise or if it is used together with identifying information as an identifier for a data subject, it is not a pseudonym in the absence of suitable technical and organisational measures to protect the identity.

In contrast to anonymous data, pseudonymous data is **personal data** according to recital 26 and therefore falls within the scope of the General Data Protection Regulation. However, they are privileged compared to other personal data because they cannot be assigned to a specific person without knowledge of additional, separately stored information. In practice, it is therefore important to clearly distinguish them from both anonymous data and other personal data.

There are various provisions in the General Data Protection Regulation in which pseudonymisation is **legally privileged**. For example, it can legitimise a change of purpose (→ Chapter 2 mn. 49), contribute to data protection through technology as a technical and organisational measure (→ Chapter 9 mn. 12), contribute to general data security (→ Chapter 9 mn. 24) and represent an appropriate protective measure for data minimization in connection with the processing of data for scientific, statistical or historical purposes (→ Chapter 2 mn. 74). However, the processing of pseudonymous data can also be useful regardless of these explicitly named scenarios. Depending on the quality of the technical and organisational measures enabling and safeguarding the pseudonymisation, pseudonymous data can play an important role for the controller, for example if the interests of the controller in the processing and possible conflicting interests of the data subjects must be weighed up in the context of Art. 6 para. 1 sentence 1 et seq. of the GDPR.

Pseudonymous data and anonymous data are similar in that a dataset cannot be easily assigned to an identified person without knowing additional information. In contrast to “absolutely anonymous” data, however, pseudonymous data contains additional information. This is also referred to as the “**assignment rule**”. Anyone who has access to the assignment rule is able to assign the data to a natural person.

³² See different pseudonymisation techniques also Article 29 Working Party 216 p. 24 et seq.; Schwartmann/Weiß Pseudonymisierungslösungen p. 26 et seq.

Chapter 1 Introduction

- 24 In contrast to “de facto anonymous” data (→ mn. 18), there is a higher **risk of re-identification** with pseudonymous data. This is because a re-identification risk is not excluded simply because the assignment rule is stored separately and is subject to technical and organisational measures that prevent it from being linked to the corresponding data. Such measures are already a necessary component of any “pseudonymisation” (→ mn. 20). In terms of the general distinction between anonymous and personal data, it is necessary to ask how high the risk is, according to general experience or the state of the art in science and technology, that re-identification will occur despite appropriate protective measures (→ mn. 18). Only if, despite existing or obtainable additional knowledge of the controller, current and future technical possibilities of processing and taking into account the possible effort and time available, it is factually impossible for the data user to become aware of the assignment rule or to assign the data by other means, is it anonymous data for the controller, otherwise it is pseudonymous data.

Note: Pseudonymous data within a group of undertakings

If a separation of assignment rule and data only takes place within a group of undertakings or through technical and organisational measures by the controller itself, the data is pseudonymous data in the context of internal processing. Although the risk of misuse is minimised, it cannot be completely ruled out based on general experience.

- 25 If making a link between the data and the assignment rule is de facto impossible for all internal parties involved in the processing, the data is anonymous for the controller even if a third party has such a link, but is not allowed to make the assignment rule accessible to the controller.³³ In this case, the anonymising effect of the pseudonymisation means that further processing by the controller of the data anonymised in this way does not fall within the scope of the General Data Protection Regulation.³⁴

Examples: Pseudonymous and anonymous data

Pseudonymous data: Department A offers information services to customers. The personal data generated about the customers’ usage behaviour is stored in a data warehouse. This is operated by Department B. Before the processing in the data warehouse, the data is replaced by pseudonyms. It is therefore in principle not possible for the employees of Department B to assign the data contained in the data warehouse to specific persons. The assignment rule is deposited with the data protection officer of the enterprise and he is prohibited by a corresponding organisational instruction from issuing the assignment rule to employees of Department B. For employees of Department B, this is pseudonymous and therefore personal data, as such an organisational instruction is generally not suitable for minimising the risk of misuse in such a way that re-identification is excluded according to general experience.

Anonymous data: In the result of a research project, possible identifiers are replaced by pseudonyms and the assignment rule is handed over to an independent third party (e.g. notary), who must not make it available to researchers either directly or indirectly. For researchers who continue to use the research result adapted in this way, it is anonymous data, as there is no objective way for them to obtain the assignment rule.³⁵

The provider of an information portal on the internet logs the time, date, browser used and the last website visited as technical data. The provider does not collect any other data. In this case, the log file data is anonymous data for the provider. This is because, according to general experience and the state of the art in science and technology, it is impossible for the provider to identify a specific visitor without additional information.³⁶

- 26 In order to distinguish pseudonymised data from other personal data, the technical and organisational measures do not have to generally exclude the linking of the data with the assignment rule. In this sense, the definition of “pseudonymisation” does not

³³ Roßnagel ZD 2018, 243 (245); in that sense also ECJ 26 April 2023 – T-557/20, ZD 2023, 399 mn. 105.

³⁴ Roßnagel ZD 2018, 243 (245).

³⁵ Roßnagel ZD 2018, 243 (245).

³⁶ Regional Court of Berlin 31 January 2013 – 57 S 87/08, ZD 2013, 618.

Index

Bold numbers refer to chapters, normal ones to margin numbers.

- Abuse of rights 12 10, 12
- Access
 - Misuse 4 24
- Accountability obligation 1 90 et seqq.
- Action
 - Decisions of the committee 13 56 et seq.
 - Suspension of the proceeding 13 55
- Address data trading
 - Consent 2 51
- Adequacy decision 6 8 et seqq.
 - Area 6 9
 - Level of data protection 6 7 et seqq.
 - Monitoring 6 10
 - Sector 6 9
 - Third countries 6 10
- Adequate level of data protection
 - Catch-all provision 6 47 et seqq.
 - Consent 6 42
 - Exceptions 6 41 et seqq.
 - Fulfilment of contractual obligations 6 44 et seq.
 - Other contracts 6 31
 - Transfer Impact Assessment 6 32 et seqq.
- Age group
 - Double opt-in 2 64
- AI Act
 - Artificial intelligence 14 6
- Anonymisation 1 16 et seqq.
 - Artificial intelligence 7 14
 - Big Data 7 14
 - Erasure 7 29
- Anonymous data 1 16 et seqq.
 - Differentiation from personal data 1 18 et seq.
 - Differentiation from pseudonymisation 1 23 et seqq.
 - General Data Protection Regulation 1 17
- Archive systems 7 12
- Article 29 Working Party 12 4
- Artificial intelligence 14 1, 13, 19 et seqq., 22 et seqq., 25
 - Accuracy of the data 14 21
 - AI Act 14 6
 - AI system 14 4
 - Anonymisation of data 7 14
 - Anonymous data 14 21
 - Autonomy 14 4 et seq.
 - Big Data 14 21
 - Black Box 14 27
 - Co-determination 14 12
 - Collective labour law 14 12
 - Consent 14 14
 - Contract 14 9, 15
 - Data minimisation 14 20
 - Data processing agreement 14 10
 - Data protection by technology 14 22 et seqq.
 - Data protection impact assessment 14 26
 - Data protection principles 14 22
 - Data transfer 14 8
 - Definition 14 2 et seqq.
 - Distribution of roles 14 9 et seq.
 - Employment relationship 14 11
 - Erasure 14 27
 - GDPR 14 7 et seq.
 - Information 14 18
 - Inspection obligation 14 24
 - Joint control 14 10
 - Large language models 14 20
 - Law 14 16
 - Lawfulness 14 14
 - Laws 14 6
 - Legal basis 14 15 et seqq.
 - Legal obligation 14 16
 - Legitimate interest 14 17
 - Machine learning 14 4
 - Mass processing 14 14
 - Metadata 14 24
 - Necessity 14 17
 - Non-contractual liability 14 6
 - Personal reference of processed data 14 7
 - Pre-contractual measures 14 15
 - Profiling 14 18
 - Purpose limitation 14 19
 - Recruitment procedure 14 11
 - Risk-based approach 14 25
 - Security 14 25
 - Self-learning 14 5
 - Target group 14 9
 - TOM 14 23
 - Training data 14 27
 - Transparency 14 18
 - User group 14 8
 - Work processes 14 11
 - works council 14 12
- Associations and organisations
 - Right to lodge a complaint 13 53 et seqq.
- Associations and other bodies
 - Appointment of a data protection officer 8 3 et seq.
- Audit 5 63 et seqq.
 - Inspections 5 63 et seq.
- Authorisations
 - Criminal judgements 2 77 et seqq.
 - Criminal offences 2 77 et seqq.
 - Criminal record 2 77
- Automated decision making 2 83 et seqq.
 - Binding Corporate Rules 2 93
 - Children 2 89
 - Consent 2 89
 - Data protection impact assessment 2 93

Index

- Fraud 2 91
- Lawfulness 2 88 et seqq.
- Legitimate interest 2 89
- Loss of context 2 84
- Obligation to inform 2 92
- Online payment 2 91
- Prerequisites 2 85 et seqq.
- Profiling 2 94 et seqq.
- Special categories of personal data 2 90
- Tax evasion 2 91
- Technical and organizational measures 2 90
- Timing 2 87
- Automated process
 - Exercising the right of objection 4 71
- Backup copies 7 12 et seq.
- Backups 7 12 et seq.
- Balancing of interests 2 41 et seqq.
 - Children 2 54 et seqq.
 - Expectations of the data subject 2 46
 - Fraud 2 43
 - Group privilege 5 6 et seqq.
 - Legitimate interests 2 41 et seqq.
 - Objection 4 68 et seq.
 - Protected interests of data subjects 2 45
 - Right of objection 2 48
 - Security 2 43
 - Third-party interest 2 41
 - Three-stage examination 2 42
- Ban with permit reservation 2 1, 7
- Big Data
 - Anonymisation of data 7 14
- Binding Corporate Rules 6 18 et seqq.
 - Authorisation, authorisation procedure 6 18
 - Authorisation process 6 22
 - Automated decision-making 2 93
 - Binding corporate rules 6 18 et seqq.
 - Consistency mechanism 6 22
 - Contents 6 21
 - Enforceability 6 21
 - Legally binding 6 21
- Biometric data 2 70
- Burden of demonstration
 - Processor 5 63 et seqq.
- Burden of proof
 - Right of access 4 36
 - Right of objection 4 74
 - Right to erasure and right to be forgotten 7 23
 - Right to rectification 4 46
 - Right to restriction 4 53
- Certification body
 - Accreditation criteria 9 43 et seqq.
 - Supervisory authority 9 43
- Certification procedure
 - Adequate level of data protection 6 27 et seqq.
- Change of purpose 2 49 et seqq.
 - Artificial intelligence 14 19
 - Opening clause 2 49 et seqq.
- Children 2 53 et seqq.
 - Age 2 54 et seqq.
 - Age group 2 56, 64
 - Age limits 2 61
 - Automated decision-making 2 89
 - Balancing of interests 2 54 et seqq.
 - Conditions for consent 2 60 et seqq.
 - Consent 2 57 et seqq.
 - Contract 2 65
 - Cross-border services 2 63
 - Data-free entry into the age of majority 7 10
 - Data minimisation 2 64
 - E-Commerce 2 56
 - Games 2 56
 - Illustration suitable for children 2 59
 - Information society services 2 58, 7 10
 - Insightfulness 2 55
 - Legal guardian 2 60 et seqq.
 - Offer 2 59
 - Parents 2 60 et seqq.
 - Personal development 2 53
- Codes of conduct 10 99 et seqq.
 - Accreditation of monitoring bodies 10 108 et seqq.
 - Adequate level of data protection 6 27 et seqq.
 - Audit standard of the supervisory authorities 10 102
 - Authorisation procedure 10 104 et seq.
 - Binding effect for supervisory authorities 10 110
 - Compliance 10 112
 - Data protection impact assessment 10 60 et seqq.
 - Entities authorised to submit documents 10 100
 - Facilitation of demonstration 10 111 et seqq.
 - Infringements 10 113 et seqq.
 - Infringements of competition law 10 114 et seqq.
 - Legal consequences 10 109 et seqq.
 - Micro, small and medium-sized enterprises 10 101
 - Monitoring 10 106 et seqq.
 - Monitoring bodies 10 107 et seqq.
 - Preparation 10 104
 - Purpose 10 101 et seqq.
 - Rule example 10 103
 - See Codes of conduct 10 99
 - Subject 10 103
- Collective agreements
 - Co-determination 11 19
 - Data protection principles 11 22
 - Full harmonisation 11 23
 - Level of data protection 11 21
 - Limits 11 11 et seqq.
 - Permission 11 24
 - Personal rights 11 20
 - Regulation limits 11 23 et seqq.

Index

- Transparency requirement 11 20 et seq.
- Communication of personal data breach to data subjects 10 22 et seqq.
- Communication period 10 28 et seqq.
- Content of communication 10 30
- Events 10 23 et seqq.
- Exceptions 10 32 et seq.
- High risk of a personal data breach 10 23 et seqq.
- Likelihood of potential damage 10 27
- Overview 10 34
- Potential damage 10 24 et seqq.
- Responsible Disclosure 10 29
- Company agreement 2 37
- Complaint 13 38, 42, 51
 - Discretion 13 41
- Confidentiality
 - Data protection officer 8 36 et seqq.
 - Data secrecy 5 57
 - Professional secrecy 5 57
- Consent 2 7 et seqq.
 - Artificial intelligence 14 14
 - Burden of demonstration 2 9
 - Burden of proof 2 9 et seq., 11
 - Children 2 30 et seqq., 57, 60 et seqq., 66
 - Cookie Consent Banner 2 107
 - Cookies and similar technologies 2 100 et seqq.
 - Dependency relationship 2 23
 - Documentation children 2 62 et seqq.
 - Double opt-in 2 10
 - Electronic 2 8 et seqq.
 - Emphasis 2 14
 - Employees 2 23
 - Employment relationship 2 23
 - Exceptions for cookies and similar technologies 2 103
 - Explicit grant 2 73
 - Form 2 8 et seqq.
 - GTC 2 14
 - Imbalance 2 23
 - Implied consent 2 15 et seqq.
 - International processing of data 6 42 et seq.
 - Legal guardian 2 60 et seqq.
 - Logging 2 10 et seq.
 - Minimum content 2 18
 - Opt-in 2 15 et seqq.
 - Opt-Out 2 15 et seqq.
 - Parents 2 60 et seqq.
 - Period of validity 2 31
 - Personalised marketing 2 31
 - Phone call 2 8
 - Preformulated 2 14
 - Process documentation 2 11
 - Profiling 2 31
 - Prohibition of coupling 2 26 et seqq.
 - Relationship to other legal grounds 7 7
 - Right to withdraw 3 14
 - Separation rule 2 25
 - Special categories of personal data 2 73
 - territorial scope 1 59 et seqq.
- Tracking on websites and in apps 2 100 et seqq.
- Transparency 2 17 et seq.
- Voluntariness 2 22 et seqq.
- Withdrawal 2 19 et seqq.
- Withdrawal and right to erasure 7 7
- Written 2 8, 13
- Consent Management Platform 2 105 et seq.
- Consent of children
 - Rome I Regulation 1 60 et seq.
- Consistency mechanism 12 41 et seqq.
 - Lawfulness requirement for decisions of the supervisory authorities 12 41
 - Urgency procedure 12 39
- Consultation of the supervisory authority on data protection impact assessment 10 63 et seqq.
- Contact details
 - Term 8 19
- Contract
 - Children 2 65
- Contract initiation
 - Necessity 2 34
- Contracts for digital products 2 108 et seqq.
- Controller 5 4 et seqq.
 - Cooperation with supervisory authority 12 11 et seqq.
 - Definition 5 4 et seq.
 - Determination of means 5 23
 - Due to actual influence 5 12 et seqq.
 - Due to legal attribution 5 11
 - Excess 5 5
 - Group privilege 5 6 et seqq.
 - Internal administrative purposes 5 7 et seqq.
 - Joint controllers 5 15 et seqq.
 - Obligation to provide support to the data protection officer 8 26 et seqq.
 - Purposes and means of processing 5 10 et seqq.
 - Works council 5 5
- Cookie Consent Banner 2 105 et seq.
- Cookies and similar technologies 2 100 et seqq.
 - Exceptions to consent 2 103
- Cooperation between supervisory authorities 12 20 et seqq., 32
 - Complaints from other Member States 12 21
 - Cooperation procedure 12 33 et seq.
 - Joint operations 12 38
 - Mutual assistance 12 37
 - One-stop shop 12 30 et seq.
 - Responsibility 12 21 et seqq.
 - Supervisory authorities concerned 12 22
 - Urgency procedure 12 39 et seqq.
- Copy
 - Protocol data 4 29
- Copy claim
 - Contents 4 30

Index

- Copy of personal data
 - Right of access 4 29 et seq.
- Corrective powers of the supervisory authority 12 18
- Covert monitoring
 - Proportionality 11 17
 - Transparency 11 17
- Criminal judgements 2 77 et seq.
- Criminal offences 2 77 et seq.
- Criminal record 2 77
- Damage
 - Compensation for damages 13 9 et seq.
 - Materiality 13 8
- Damage amount 13 9 et seq.
 - Assessment criteria 13 10
- Dark Patterns 2 107
- Data made public
 - Right to be forgotten 7 15 et seq.
- Data minimisation
 - Children 2 64
- Data mobility 4 55
- Data Privacy Framework 6 11 et seq.
 - Certification 6 12 et seq.
- Data processing 2 5 et seq.
 - Ban with permit reservation 2 1
 - consent 2 7 et seq.
 - Lawfulness 2 3
 - Permission 2 1 et seq.
- Data processing agreement
 - Authorisation 6 31
 - Other contracts 6 31
- Data protection by default
 - Discretion 9 18
 - Facilitation of evidence 9 34
 - Manufacturer 9 16
 - Necessity 9 16
 - Penalties 9 5
 - Principle of necessity 9 15
 - Processor 9 8
 - Requirements 9 15 et seq.
 - Selection discretion 9 16
 - Self-data protection 9 5 et seq.
 - Social networks, online newspapers, information portals, blogs 9 17
- Data protection by design
 - Addressees of the provision 9 6 et seq.
 - Balancing 9 13
 - Controller 9 7
 - Control mechanisms 9 10
 - Data protection impact assessment 9 13
 - Facilitation of evidence 9 34
 - Necessary measures 9 11 et seq.
 - Processor 9 8
 - Proportionality 9 13
 - Pseudonymisation 9 12
 - Requirements 9 10 et seq.
 - Selection decision 9 7
 - System data protection 9 5 et seq.
 - Timing 9 10
- Data protection by design & by default 9 9
- Data protection certification 9 35 et seq.
 - Certification criteria 9 40
 - Competitive advantage 9 44
 - Data protection seals and certification marks 9 35, 48
 - Easier facilitation of proof 9 45 et seq.
 - Incentives 9 44
 - Infringements of competition law 9 48 et seq.
 - Legal consequences 9 44 et seq.
 - Manufacturer certification 9 38
 - Micro, small and medium-sized enterprises 9 36
 - Obligation to co-operate 9 41
 - Obligation to inform towards supervisory authority 9 42
 - Penalties 9 47 et seq.
 - Period of validity of the certificate 9 42
 - Procedure 9 40 et seq.
 - Product certification 9 38
 - Regulatory framework 9 35
 - Scale 9 39
 - Subject 9 37
 - Supervisory authority 9 40
 - Veto right of the supervisory authority 9 42
- Data protection-friendly default settings
 - Addressees of the provision 9 6 et seq.
 - Manufacturer 9 6
- Data protection impact assessment
 - Special categories of personal data 2 67
- Data protection impact assessment 10 35
 - Advice period of the supervisory authority 10 67 et seq.
 - Artificial intelligence 14 26
 - Assessment of the specific risk 10 49 et seq.
 - Assessment phase 10 53 et seq.
 - Automated decision-making 2 93
 - Codes of conduct 10 60 et seq.
 - Conflicting commercial interests 10 76 et seq.
 - Data protection officer 10 62
 - Documentation 10 58 et seq.
 - Exceptions to the involvement of data subjects 10 75 et seq.
 - Involvement of data subjects 10 71 et seq.
 - Likelihood of a high risk 10 39 et seq.
 - Lists of supervisory authorities 10 45 et seq.
 - Measure phase 10 55 et seq.
 - Necessity 10 38 et seq.
 - Necessity test 10 51 et seq.
 - Negative list 10 47
 - New technologies 10 38
 - Obligations of the processor 10 37
 - Overview 10 79
 - Performance 10 49 et seq.
 - Positive list 10 45
 - Preparation phase 10 51 et seq.
 - Prior control 10 35 et seq.

Index

- Profiling 2 99, 10 44
- Regulatory addressees 10 37 et seqq.
- Representative of the data subject 10 73 et seq.
- Reservation of authorisation 10 65 et seqq.
- Review 10 78 et seq.
- Risk classification 10 54
- Risk management system 10 50
- Security interests 10 76 et seq.
- Similar processing operations 10 57
- Special data categories 10 44
- Statutory rule examples 10 44
- Supervisory authority 10 63 et seqq.
- Threshold analysis 10 51
- Works council 10 73
- Data protection impact assessment
 - Fines 10 36
- Data protection officer 8 1 et seqq.
 - Aids 8 27 et seq.
 - Associations and other bodies 8 3 et seq.
 - Breaches of obligation 8 48
 - Breach of obligation 8 32
 - Conflict of interest 8 23
 - Contact details Publication and notification 8 18 et seq.
 - Contact person for data subjects 8 37
 - Cooperation with supervisory authorities 8 44 et seqq.
 - Core activity of the controller or processor 8 8 et seq.
 - Data protection impact assessment 10 62
 - Designation 8 3 et seqq., 20 et seqq.
 - Designation obligation 8 6 et seqq.
 - Discrimination 8 34
 - Dismissal 8 33
 - Dismissal by supervisory authority 12 18
 - Expert knowledge 8 21
 - External data protection officer 8 16
 - Form of designation 8 5
 - Freedom from instructions 8 30
 - Impact assessment 8 40
 - In-company damage compensation 8 50
 - Independence 8 29 et seqq.
 - Joint data protection officer 8 11
 - Legal person 8 17
 - Liability 8 49 et seqq.
 - Micro, small and medium-sized enterprises 5 68
 - Monitoring function 8 41 et seqq.
 - Monitoring guarantor 8 51
 - Obligation of confidentiality 8 36
 - Obligation of secrecy 8 36 et seqq.
 - Obligation of the controller or processor to provide support 8 26 et seqq.
 - Obligation to inform 3 7
 - Position 8 24 et seqq.
 - Prior check 8 40
 - Prohibition of discrimination 8 31 et seqq.
 - Proper and early involvement 8 24 et seqq.
 - Recall 8 31 et seqq.
 - Reliability 8 22 et seqq.
 - Reporting obligation 8 35
 - Risk appropriateness of the activity 8 47 et seqq.
 - Role 8 1 et seqq.
 - Role conflict 8 46
 - Tasks 8 38 et seqq.
 - Teaching and counselling function 8 39 et seqq.
 - Training and awareness-raising 8 42 et seqq.
 - Voluntary designation 8 3
- Data protection regulations, binding internal
 - see Binding Corporate Rules 6 18
- Data security 9 24, 10 1 et seqq.
 - Backups 9 25
 - Botnet 9 25
 - Concretisations 9 24 et seqq.
 - Contractor 9 20
 - Controller 9 20
 - Cyberattacks 9 2
 - Emergency plans 9 25
 - Facilitation of evidence 9 34
 - Fines 9 19
 - Implementation costs 9 22
 - Indemnifiability 9 27
 - ISO 27001 9 33
 - Lowering the level of protection 9 27
 - Necessary measures 9 21 et seqq.
 - Probability of loss occurrence 9 23
 - Processor 9 7
 - Proportionality 9 26
 - Regulation GDPR 9 4
 - Regulatory addressees 9 20
 - Risk assessment 9 21 et seqq.
 - Risk-based approach 9 26
 - State of the art 9 21 et seqq.
 - technical and organizational measures 9 1 et seqq.
 - Technical measures 9 22
 - TOM 9 3
- Data security concept
 - DPMS 9 29
 - ISMS 9 29 et seqq.
- Data separation 4 37
- Data subject 1 9 et seqq.
 - Communication of personal data breach to data subjects 10 22 et seqq.
 - Data protection officer as a contact person 8 37
- Deadlines
 - Rights of the data subject 4 19 et seqq.
- Decision 2 86
- Delegated acts 1 80
- Delete
 - Big Data 7 14
- Deletion
 - See Erasure 7 1
- Designation of the data protection officer 8 3 et seqq.
 - Core activity of the controller or processor 8 8 et seqq.

Index

- Opening clause for the Union or Member States 8 10
- Destruct 7 4
- Digital content 2 108 et seqq.
- Digital products 2 108 et seqq.
- Digital services 2 108 et seqq.
- DIN 66398
 - Erasure concept 7 28
- Direct collection 3 3 et seqq.
- Direct marketing 2 51
 - Profiling 2 94
- Double opt-in 2 10
- E-Discovery
 - See International processing of data 6 40
- EDPB 12 4 et seqq.
 - Composition 12 5
 - Tasks 12 6
- Employee data protection 1 73, 11 1 et seqq.
 - Collective agreements 11 2, 19, 23 et seq.
 - Compliance assessments 11 16 et seqq.
 - Covert measures 11 18
 - Covert monitoring 11 17
 - GPS monitoring 11 18
 - Level of protection 11 7
 - Matrix structures 11 4 et seqq.
 - Opening clause 11 8 et seqq., 19
 - Protective purpose 11 8 et seqq.
 - Scope of national regulations 11 5 et seqq.
 - Secret monitoring 11 18 et seq.
- Employees
 - personal data 1 32
- Encryption 1 27 et seqq.
 - Definition of 1 27
 - privilege 1 27
 - pseudonymisation 1 28 et seq.
 - Technical and organisational measures 5 49
- End devices, reading and saving information 2 100 et seqq.
- ePrivacy Directive 1 82 et seqq.
 - Implementation 1 83
 - Precedence 1 83 et seq.
- Erase
 - Anonymisation 7 14
 - Artificial intelligence 7 14
- Erasure 7 1 et seqq., 4
 - Anonymisation 7 29
 - Artificial intelligence 7 17
 - Control 7 41
 - Documentation 7 40
 - Information for recipients 7 18
 - Privacy by design 7 17
 - Realisation in practice 7 25 et seqq.
 - Technical and organisational measures 7 29
- Erasure concept 7 1, 25 et seqq.
 - Contents 7 26
 - DIN 66398 7 28
 - Erasure rules 7 39
 - ISO/IEC 27555:2021 7 28
- Joint controllers 7 27
- Procedure 7 32
- Realisation 7 33
- Responsibility 7 30
- Responsibility for implementing 7 34
- Retention period 7 36 et seqq.
- Standard erasure period 7 39
- Time of creation 7 31
- Update 7 35
- Erasure deadline 7 36 et seqq.
- Erasure of data
 - Archive systems 7 12
 - backup copies 7 12
 - Backups 7 12
- Establishment 1 38 et seqq.
 - Main establishment 12 26 et seqq.
 - processing 1 40 et seqq.
- Establishment principle 1 37 et seqq.
- European Privacy Seal 9 37
- Exceptions to the obligation to erasure
 - Information 7 20
 - Preview images in search engines 7 20
 - Weighing up fundamental rights 7 20
- External collection 3 3 et seqq., 18
- Fines 13 27 et seqq.
 - Categories 13 30 et seqq.
 - Discretion 13 28 et seqq.
 - Group of undertakings 13 33 et seqq.
- Formal requirements 2 7 et seqq.
 - Designation of the data protection officer 8 5
 - Electronic format for the provision of information 4 32 et seq.
 - Electronic format for the right to data portability 4 63 et seq.
 - Exercising the rights of the data subject 4 16
 - Interoperability of electronic formats 4 64
 - Resolutions by supervisory authorities 12 14
- Freedom from instructions
 - Data protection officer 8 30
- Function transfer 5 45
- General Data Protection Regulation
 - History 1 1
 - Scope 1 3 et seqq.
 - Trilogue 1 1
- Genetic data 2 70
- German Federal Commissioner for Data Protection (BfDI) 12 13
- Group data protection office
 - Accessibility 8 13 et seqq.
- Group data protection officer 8 11 et seqq.
 - Designation 8 12
- Group of undertakings 13 33
 - One-stop shop 12 31
 - Penalties 13 33 et seqq.
- Group privilege 2 47
 - Balancing of interests 5 8

Index

- Joint controllers 5 16
- Health data 2 70
- Heatmaps 2 69
- Identification 4 7 et seqq.
 - Demonstration of identity 4 7 et seq.
 - Desire for identification 4 14
 - Features 2 82
 - Identity verification 4 12
 - Information 2 81
 - Multi-factor 4 12
 - Negative information 4 13
 - Official identity cards 4 13
 - Online identifiers 4 11
 - Post 4 10
 - Processing of data 2 80 et seqq.
 - Protection of personal data 2 81
 - Reasonable doubts 4 8 et seqq.
 - Security questions 4 11 et seq.
- Identity card
 - Identification 4 13
- Impact assessment
 - Liberation 10 48 et seq.
 - Obligation to provide information towards the supervisory authority 10 64
- Implementing acts 1 81 et seq.
- Information
 - Identification 2 81
- Information obligation
 - Performance of a contract 2 32
- Information society services
 - Children 2 58
 - Data collected from children 7 10
- Infringement
 - Materiality 13 5
- Inspections
 - On-site audit 5 63
- Instruction 5 55 et seqq.
 - Decision-making authority 5 56
 - Documentation 5 55 et seq.
- International processing of data
 - Adequacy decision 6 7 et seqq.
 - Binding Corporate Rules 6 18 et seqq.
 - BPO 6 1
 - Catch-all provision 6 47
 - Certification procedure 6 27 et seqq.
 - Codes of conduct 6 27 et seqq.
 - Consent 6 42 et seq.
 - Data Privacy Framework 6 11 et seqq.
 - E-Discovery 6 46
 - Employment relationship 6 43
 - Examination first stage 6 3
 - Fulfilment of contractual obligations 6 44 et seq.
 - Mutual legal assistance agreement 6 40
 - Onward transmission 6 6
 - Other contracts 6 31
 - Outsourcing 6 1
 - Pre Trial Discovery 6 46
 - Safeguards, appropriate 6 16 et seqq.
 - Second stage examination 6 4
 - Secret services 6 40
 - Self-commitment 6 11 et seqq.
 - standard data protection clauses 6 23 et seqq.
 - Third countries 6 1 et seqq.
 - Transfer Impact Assessment 6 32 et seqq.
 - Two-stage inspection 6 1
- Investigative powers of the supervisory authority
 - Scope and limits 12 16 et seq.
- ISO/IEC 27555:2021
 - Erasure concept 7 28
- IT and security concept 9 31 et seq.
- IT Security Act 9 3
- Joint controllers 5 15 et seqq.
 - Agreement 5 28 et seqq.
 - Conditions 5 18 et seqq.
 - Corporation 5 21
 - Differentiation from processors 5 17
 - Erasure concept 7 27
 - Group privilege 5 16
 - "If" of the processing 5 24
 - Indications 5 25
 - Legal consequences 5 26 et seqq.
 - Obligation to inform vis-à-vis data subjects 5 33
 - Privilege of data exchange 5 26
 - Rights of the data subject 4 1, 5 31
 - Sense of responsibility 5 27
- Joint data protection officer 8 11
- Justification 2 7 et seqq.
 - Legitimate interests 2 41 et seqq.
- Lawfulness
 - Pre-contractual measures 2 32
- Lawfulness 2 32 et seqq.
 - Address data trading 2 51
 - Artificial intelligence 14 14
 - Automated decision-making 2 88 et seqq.
 - Balancing of interests 2 45 et seqq.
 - Case-by-case assessment 2 45 et seqq.
 - Change of purpose 2 49 et seqq.
 - Children 2 53 et seqq.
 - Collective agreements 2 37
 - Collective labour agreements 2 37
 - Company agreement 2 37
 - Contract initiation 2 32
 - Exercise of sovereign authority 2 40
 - Freedom of expression 2 79
 - Legal obligation 2 35
 - Legitimate interest 5 7 et seq.
 - List data 2 51
 - marketing 2 51
 - opening clause 2 3
 - Paying with data 2 111
 - Processing principles 2 1
 - Profiling 2 98
 - Public interest 2 40
 - Purpose limitation 2 49

Index

- Lawsuit
 - From associations 13 51 et seqq.
- Lead supervisory authority 12 23 et seqq.
 - Affectedness of controllers and processors 12 28
 - Decline jurisdiction 12 29
 - Main establishment 12 26
 - Several controllers or processors 12 25
 - Several establishments of a controller 12 26 et seq.
 - Several establishments of a processor 12 28
- Legitimate interests 2 41 et seqq.
 - Economic interest 2 43
 - Idealistic interest 2 43
- Liability
 - Burden of proof and evidence 13 4
 - Claimant 13 11
 - Claims under the law of obligations 13 20
 - Compensation for damages 13 9 et seq.
 - Damage 13 6 et seqq.
 - Data protection officer 8 49 et seqq.
 - Exculpation 13 14 et seqq.
 - Fault 13 14 et seqq.
 - Infringement 13 2 et seqq.
 - Injunctive relief 13 21 et seqq.
 - Joint and several liability 13 17 et seqq.
 - Legal persons 13 11, 20
 - Material damage 13 6
 - Non-material damage 13 7
 - Offence 13 20
 - Processor 13 12 et seqq.
 - Recourse 13 19
 - Removal 13 21 et seqq.
 - Third party 13 11
- List data 2 51
- Lock-in effect 4 54
- Main establishment 12 26
- Marketing
 - Consent 2 51
 - Right of objection 4 70
- Market place principle 1 45 et seqq.
 - Behavioural observation 1 50 et seqq.
 - Criteria for offer 1 46 et seqq.
 - social networks 1 50
- Material damage
 - Liability 13 6
- Materiality
 - Damage 13 8
 - Infringement 13 5
- Material scope
 - filing system 1 8
- Media privilege
 - Freedom of information 2 79
 - Online archives 2 79
- Medical records 4 41
- Memory limitation
 - Identification 2 80
- Micro, small and medium-sized enterprises 5 67 et seqq.
 - Codes of conduct 10 101
 - Data protection certification 9 36
 - Data protection officer 5 68
 - Definition 5 69
 - Privileges 5 68
 - Recording of processing activities 10 83
- Misuse
 - Abuse of rights 4 25
 - Good faith 4 24
- Monitoring bodies
 - See Codes of conduct 10 107
- Mutual assistance 12 37
- Necessity
 - Contract initiation 2 34
 - Performance of a contract 2 34
- Negative information 4 13, 28
- Negative list for impact assessments 10 47
- Non-automated processing 1 8
- Non-direct collection 3 3 et seqq.
 - Deadlines 3 22
- Non-material damage
 - Liability 13 7
- Notification obligation to supervisory authorities
 - Documentation 10 17
 - Notifiable events 10 7 et seqq.
 - Notification period 10 10 et seqq.
 - Overview 10 21
 - Start of notification period 10 11 et seqq.
 - Support obligation of the processor 10 18 et seqq.
- Nudging 2 107
- Objection 4 66 et seqq.
 - Automated processes 4 71
 - Balancing of interests 2 48, 4 68 et seqq., 7 8
 - Burden of proof 4 74
 - Consequences of the exercise 4 72 et seqq.
 - Direct marketing 4 70, 7 8
 - General objection 4 68 et seqq.
 - Marketing 4 70
 - Obligation to inform 2 92, 3 13
 - Prerequisites 4 69
 - Profiling 2 99
 - Reference to right of objection 4 66
 - Scientific research 1 77
 - Statistical purposes 1 77
- Obligation of secrecy
 - Data protection officer 8 36 et seqq.
 - Observance of the rights of the data subjects 4 34 et seqq.
- Obligation to erase
 - Erasure concept 7 25 et seqq.
 - Realisation in practice 7 25 et seqq.
- Obligation to erasure 7 1
 - Consequences of erasure 7 11 et seqq.
 - Exceptions 7 19
 - Exceptions in national law 7 22

Index

- Omission of the processing purpose 7 6
- Processor 7 42
- Reasons for erasure 7 5
- Withdrawal of consent 7 7
- Obligation to inform 3 26 et seq.
 - Address, deliverable 3 6
 - Assumption of costs 3 31
 - Automated decision making 2 92
 - Automated decision-making, individual case decision 3 15 et seq.
 - Balancing of interests 3 8
 - Change of purpose 3 17
 - Consent 3 14
 - Contact details 3 6
 - Cookies 3 21
 - Data protection officer 3 7
 - Demonstration, proof 3 25
 - Direct collection 3 4 et seq.
 - Electronic form 3 24
 - Exceptions 3 19 et seq.
 - Fair processing 3 12
 - Fines 3 33
 - Form 3 23 et seq., 26
 - Historical purposes 3 19
 - Horizon of understanding 3 29 et seq.
 - Legitimate interests 3 8
 - Lingua franca 3 29 et seq.
 - Local Storage 3 21
 - Logic 3 16
 - Logic, access 3 15
 - Marketing 3 2
 - Market place principle 3 29 et seq.
 - Market research 3 2, 19
 - National language 3 29 et seq.
 - Non-direct collection 3 18, 22
 - Objection 2 92
 - Obligation of secrecy 3 20
 - Obligation to inform 3 2
 - Obligation to notify 3 2
 - Opinion research 3 2, 19
 - Overview 3 4 et seq., 12, 32
 - Own processing purposes 3 19
 - Perspective of recipient 3 29
 - Perspective of the recipient 3 26
 - Pictograms 3 28
 - Presentation 3 23 et seq.
 - Privacy policy 3 24
 - Profiling 3 15 et seq.
 - Public sources 3 18
 - Recipient 3 9
 - Recipient horizon 3 30
 - Regulatory offense 3 33
 - Representative 3 7
 - Right of appeal 3 12
 - Right to object 3 13
 - Right to withdraw 3 14
 - Scope 3 27
 - Scoring 3 16
 - Statistical purposes 3 19
 - Style 3 26
 - Timing 3 4 et seq., 21
 - Transparency 3 1 et seq., 12
 - Verbal form 3 25
 - Written form 3 24
- Obligation to inform in the event of data breaches
 - Content and form of the communication 10 30 et seq.
- Obligation to inspect
 - Adequate level of data protection 6 27 et seq.
- Official identification documents
 - Identification 4 13
- One-stop shop 12 30 et seq.
- On-site audit 5 63
- Opening clause
 - Lawfulness 2 3
 - Special categories of personal data 2 76
- Opening clauses 1 68 et seq.
 - Individual regulations 1 69 et seq.
 - Overview 1 71
 - Requirements 1 72
- Paying with data 2 108 et seq.
- Penalties 13 24 et seq.
 - Corrective powers 13 24
 - Discretion 13 28 et seq.
 - Fault 13 25 et seq.
 - Fines 13 27 et seq.
 - Group of undertakings 13 33 et seq.
 - Investigative powers 13 24
 - Member states 13 35 et seq.
 - Supervision fault 13 26
- Performance of a Contract
 - External business purposes 2 32
 - Information obligation 2 32
 - Necessity 2 34
- Personal data 1 9 et seq.
 - Differentiation from anonymous data 1 18 et seq.
 - Employee data 1 32
 - Identifiability 1 10 et seq.
 - IP addresses 1 13 et seq.
 - legal persons 1 30 et seq.
 - natural person 1 30 et seq.
 - Online identifiers 1 11 et seq.
 - Relativity 1 12 et seq.
- Personal data breach 10 2 et seq.
 - Definition 10 2
 - Fines 10 3
 - Form of notification 10 16
 - Minimum content of the notification 10 14
 - Nemo-tenetur principle 10 4 et seq.
 - Notification towards supervisory authorities 10 6 et seq.
 - Regulatory addressees 10 6
 - Self-incrimination 10 4 et seq.
- Personal scope 1 33 et seq.
 - Deceased 1 33
 - recipient 1 34
 - Third party 1 34
 - Unborn 1 33

Index

- Phone call
 - Consent 2 8
- Photos 2 69 et seq.
- Pictograms
 - Delegated acts 3 28
 - Symbols 3 28
- Positive list for data protection impact assessments 10 45 et seqq.
- Prior control 10 35
- Privilege
 - Processing 5 46 et seq.
- Proceedings
 - Against controllers or processors 13 45 et seqq.
 - Against supervisory authorities 13 43 et seq.
 - Representative 13 48
- Processing
 - Agreement content 5 53 et seqq.
 - Bearing of costs 5 54
 - Case groups 5 39 et seqq.
 - Certification procedure 5 49
 - Codes of conduct 5 49
 - Confidentiality 5 57
 - Definition 5 36 et seqq.
 - Demonstrability 5 51
 - Destruct 7 4
 - Electronic form 5 50
 - Electronic format 5 50 et seq.
 - Erasure 7 4
 - Fines 5 64
 - Function transfer 5 45
 - Guarantees 5 48
 - Instruction 5 55 et seqq.
 - Legitimate interest 5 46
 - Liability 5 64 et seqq.
 - Obligations of the controller 5 48 et seqq.
 - Other processors (subcontractors) 5 58 et seqq.
 - Outsourcing 5 58 et seqq.
 - Penalties 5 64
 - Permission, justification 5 46
 - Professional secrecy holder 5 44
 - Retention periods 5 62
 - Special data categories 5 46
 - Standard contractual clauses 5 52
 - Subcontractor 5 58 et seqq.
 - Termination 5 62
 - Written form 5 50
- Processing principles 1 85 et seqq.
 - Concretisation 1 88
 - Fines 1 85
 - Lawfulness 2 1
 - Requirement of certainty 1 89
- Processing purpose
 - Omission 7 6
- Processing term 1 6 et seqq.
 - Test data 1 7
- Processor
 - Burden of demonstration 5 63 et seqq.
 - Cooperation with supervisory authority 12 11 et seq.
 - Definition 5 35 et seq.
 - Fault 5 66
 - Liability 13 12
 - Obligations, overview 5 65
 - Obligation to provide support to the data protection officer 8 26 et seqq.
- Professional secrecy 2 75
- Professional secrecy holder
 - Processing 5 44
- Profiling 2 83 et seqq., 94 et seqq.
 - Automated decision-making 3 15
 - Big Data 2 95
 - Data protection impact assessment 2 99, 10 44
 - Direct marketing 2 94
 - Internet offer 2 94
 - Lawfulness 2 98
 - Location Based Services 2 94
 - Right of objection 2 99
 - Scoring 2 84, 97
 - Term 2 95
 - Usage profiles 2 96
- Prohibition of coupling
 - Monopoly 2 26
 - Penalties 2 27
 - Performance of a contract 2 28
- Protected interests of data subjects 2 45
- Protection of minors 2 64
- Pseudonymisation 1 20 et seqq.
 - Data minimisation 9 12
 - Data protection by design 9 12
 - Definition of 1 20
 - Differentiation from anonymous data 1 23 et seqq.
 - Personal reference 1 21
 - privilege 1 22
 - Special categories of personal data 2 74
 - Technical and organisational measures 5 49
- Pseudonymous data 1 20 et seqq.
- Purpose limitation 2 49
- Recipient
 - Obligation to inform 3 9
 - Right to vote 3 9
- Records of processing activities
 - Fines 10 82
 - Form 10 85
 - Micro, small and medium-sized enterprises 10 83
 - Processing activity 10 87
 - Processor 10 81
 - Provision 10 84
 - Public record 10 84
 - Recording obligations 10 80 et seqq.
 - Records of the controller 10 87 et seqq.
 - Records of the processor 10 95 et seqq.
 - Update 10 86

Index

- Re-identification risk
 - artificial intelligence 1 19
 - Big Data 1 19
 - pseudonymous data 1 24
 - Web tracking tools 1 19
- Relationship between Art. 6 and Art. 9, 10 GDPR 2 2
- Remedies 13 36 et seqq.
 - Complaint 13 38 et seqq.
 - Controller or processor 13 49
 - From associations 13 50
 - Of data subjects 13 38
- Representative 5 70 et seqq.
 - Agreement 5 73
 - Commissioning 5 79
 - Cooperation with supervisory authority 12 11 et seq.
 - Designation 5 78
 - Designation obligation 5 70 et seqq.
 - Establishment 5 72
 - Exceptions to the designation obligation 5 71
 - Liability 5 77
 - List of procedural activities 5 73
 - Obligations 5 73 et seqq.
 - Obligation to inform 3 7
 - Penalties 5 75 et seq., 80
- Responsibility
 - Erasure concept 7 30
- Responsibility of the supervisory authority 12 21 et seqq.
- Retention period 7 36 et seqq.
- Retention processing of identification data 4 14
- Right of access 4 26 et seqq.
 - Blackening 4 30 et seqq.
 - Content of the access 4 39
 - Copy of the personal data 4 29 et seqq.
 - Data Act 4 27
 - Exceptions 4 38
 - First copy 4 40
 - Free of charge 4 40
 - Highly personal right 4 26
 - Medical records 4 41
 - Negative information 4 28
 - Object 4 28
 - Opening clauses 4 38
 - Provision in common electronic format 4 32 et seq.
 - Recipients of data 4 44, 51, 7 18
 - Refusal by controller 4 26
 - Specification of the request for access 4 31
 - Whistleblowing Directive 4 30
- Right of completion
 - Data minimisation 4 45
- Right of copy
 - Contents 4 29
- Rights and freedoms of third parties
 - Copy 4 35
 - Security 4 34
- Rights of the data subject
 - Communication of personal data breach to data subjects 10 22 et seqq.
 - Compliance with the rights of third parties 4 61
 - Deadlines 4 19 et seqq.
 - Defendant 4 1
 - Electronic application and processing 4 18
 - Erasure 7 1 et seqq.
 - Exercise of rights 4 6 et seqq.
 - Exercise procedure 4 15 et seqq.
 - Form of the messages 4 16 et seq.
 - Identification 4 7 et seq.
 - Misuse fee 4 22 et seq.
 - Non-remuneration 4 22
 - Observance of third party rights 4 34 et seq.
 - Paying with data 2 112
 - Purposes 4 2 et seq.
 - Refusal of erasure 7 21
 - Rejection by controller 4 21
 - Restrictions by the Union or Member States 4 4 et seq.
 - Right of access 4 26 et seqq.
 - Right of completion 4 45
 - Right to rectification 4 42 et seq.
- Right to be forgotten 7 1
 - Appropriateness of the measures 7 17
 - Technical and organisational measures 7 16
 - Search engine operator 7 16
- Right to be forgotten for data made public 7 15 et seqq.
- Right to data portability 4 54 et seqq.
 - Data Act 4 55
 - Data mobility 4 55
 - Data provided 4 58
 - Direct transfer to new controller 4 61 et seq.
 - Exceptions 4 65
 - Exclusion 4 59
 - Lock-in effect 4 54
 - Relationship to the right to erasure and the right to be forgotten 4 60
 - Scope 4 57 et seqq.
 - Technical requirements 4 63 et seq.
- Right to erasure 7 1
 - burden of proof 7 23
 - Consequences of erasure 7 11
 - Data collected from children 7 10
 - Exceptions 7 19
 - Objection to processing 7 8
 - Omission of the processing purpose 7 6
 - Processing in practice 7 24
 - Reasons for erasure 7 5
 - Right to be forgotten in the narrower sense 7 15 et seqq.
 - Search engine results 7 5
 - Unlawful processing 7 9
 - Withdrawal of consent 7 7
- Right to erasure and right to be forgotten
 - Relationship to the right to data portability 4 60
 - Search engine results 4 46

Index

- Right to rectification 4 42 et seqq.
 - Completion of accurate data 4 45
 - Correction of inaccurate data 4 44
 - Facts 4 44
 - Relationship to other standards 4 43 et seqq.
 - Saving additional data 4 45
 - Self-data protection 4 42
- Right to restriction of processing 4 47 et seqq.
 - Burden of proof 4 53
 - Consequences of the restriction 4 50 et seq.
 - Exceptions 4 52 et seq.
 - Informing the data subject about repeal 4 51
 - Reasons for restriction 4 48 et seq.
 - Technical implementation of the restriction 4 50
- Right to withdraw 3 14
- Risk analysis 9 31 et seq.
- Risk management system
 - Data protection impact assessment 10 50
 - Data security 9 29 et seqq.
- Roles 5 1 et seqq.
- Rome I Regulation
 - Sensitive data 1 62 et seqq.
- Safeguards, appropriate
 - Remedies 6 16
 - Rights of the data subject 6 16
- Scientific research 1 74 et seqq.
 - Data minimisation 1 76
 - Objection 1 77
 - Privileges 1 78
 - Special categories of personal data 2 74
- Scope
 - Artificial intelligence 14 7 et seq.
 - material 1 5 et seqq.
 - Professional secrecy holder 12 17
- Scoring 2 84, 97
 - Obligation to inform 3 16
- Search engine operator
 - Right to be forgotten 7 16
- Search engines
 - Erasure of results 4 46, 7 5
- Secrecy 2 75
 - Investigative powers of the supervisory authority 12 17
- Sensitive data 2 67 et seqq.
- Social networks
 - Data Protection by default 9 17
- Special categories of Data
 - Data protection impact assessment 10 44
- Special categories of personal data 2 67 et seqq., 90
 - Archives 2 74
 - Ban with permit reservation 2 67
 - Consent 2 73
 - Data protection impact assessment 2 67
 - Exceptions to the processing ban 2 71 et seqq.
 - Historical purposes 2 74
 - Opening clause 2 76
 - Professional secrecy 2 75
 - Pseudonymisation 2 74
 - Scientific research 2 74
 - Secrecy 2 75
 - Statistical purposes 2 74
 - Term 2 68 et seqq.
- Special data categories
 - Guarantees 2 72
- Specialised erasure concept 7 32
- Special processing situations 1 73 et seqq.
- Standard contractual clauses
 - Processing 5 52
 - third country transfer 6 23 et seqq.
- Standard data protection clauses
 - Adequate level of data protection 6 26
 - Changes 6 26
 - Guarantees, suitable 6 23 et seqq.
 - Modules 6 25
 - Safeguards, appropriate 6 17
 - standard contractual clauses 6 23 et seqq.
- Standard erasure period 7 39
- Statistical purposes 1 75 et seqq.
 - Data minimisation 1 76
 - Objection 1 77
 - Obligation to inform 3 19
 - Privileges 1 78 et seq.
 - Special categories of personal data 2 74
- Storage deadline
 - Determination 7 37 et seq.
 - Start 7 38
 - Storage duration 7 37
- Structured, common and machine-readable format 4 63 et seq.
- Subcontractor 5 58 et seqq.
 - Authorisation 5 58 et seqq.
 - Guarantees 5 61
 - Objection 5 59 et seq.
- Supervisory authority 12 1 et seqq.
 - Advisory powers 12 19
 - Authorisation powers 12 19
 - Cooperation between supervisory authorities 12 32
 - Cooperation with controllers, processors and representatives 12 11 et seq.
 - Cooperation with data protection officers 8 44 et seqq.
 - Discretionary decisions 12 15
 - Dismissal of the data protection officer 12 18
 - Form of resolutions 12 14
 - Joint operations 12 38
 - Mutual assistance 12 37
 - Non-remuneration of the fulfilment of the task 12 9 et seq.
 - One-stop shop 12 30 et seq.
 - orrective powers 12 18
 - Powers 12 13 et seqq.
 - Professional secrecy 12 17
 - Responsibility 12 21 et seqq.

Index

- Supervisory authority concerned 12 3, 22
- Tasks 12 7 et seqq.
- Urgency procedure 12 39 et seqq.
- Supervisory authority concerned 12 3, 22
- Tax consultants
 - Processing 5 44
- Technical and organisational measures
 - Erasure 7 29
 - Right to be forgotten 7 16
- Technical and organizational measures
 - Special categories of personal data 2 90
- Technical erasure concept 7 32
- Technical standards
 - ISO 27001 9 33
- Territorial scope 1 35 et seqq.
 - Choice of law clauses 1 65 et seqq.
 - Domestic processing 1 52 et seq.
 - Domicile principle 1 55 et seq.
 - Establishment principle 1 37 et seqq.
 - Rome I Regulation 1 60 et seqq.
 - Territoriality principle 1 57 et seq.
 - within the EU 1 53 et seqq.
- Third country transfer
 - International processing of data 6 1
- Third party collection 3 3 et seqq., 18
- TIA
 - see Transfer Impact Assessment 6 32
- Tracking on websites and in apps 2 100 et seqq.
- Transfer Impact Assessment
 - Measures 6 37 et seqq.
 - Necessity 6 36
 - Performance 6 35
 - Risk assessments 6 38 et seq.
- Transfer Impact Assessments 6 32 et seqq.
- Transparency
 - Identification 2 81
 - Purposes 2 17
- Usage profiles 2 96
- Video surveillance
 - Publicly accessible rooms 2 52
- Vital interests 2 39
- Withdrawal 2 19 et seqq., 21