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

CONTENTS

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

Since 25 May 2018, the General Data Protection Regulation has been directly **applicable** law in every member state of the European Union.[1] This was preceded by various drafts for a Regulation by the EU Commission[2], the European Parliament[3] and **1**

[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).

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 seqq.).

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.

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 seqq.) and to the possible performance of a data protection impact assessment pursuant to Art. 35 and 36 GDPR (→ Chapter 10 mn. 35 et seqq.). 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 seqq.

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.

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 identification[10] 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]

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.

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]

14 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

[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.

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).

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).

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.

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). **20**

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. **21**

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. **22**

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. **23**

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