

General Data Protection Regulation

Spiecker gen. Döhmann / Papakonstantinou / Hornung / de Hert

2023

ISBN 978-3-406-74386-3

C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.

beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Spiecker gen. Döhmann / Papakonstantinou / Hornung / De Hert

General Data Protection Regulation

beck-shop.de
DIE FACHBUCHHANDLUNG

General Data Protection Regulation

Article-by-Article Commentary

edited by

Indra Spiecker gen. Döhmman
Vagelis Papakonstantinou
Gerrit Hornung
Paul De Hert

2023



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 oHG, 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



beck-shop.de
DIE FACHBUCHHANDLUNG

ISBN 978 3 8487 3372 9 (NOMOS Print)

ISBN 978 3 8452 7698 4 (NOMOS ePDF)

ISBN 978 3 406 74386 3 (C.H.BECK)

ISBN 978 1 5099 3252 8 (HART)

First Edition 2023

© Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden 2023. 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.

Preface

In 2018, Europe became the worldwide leading regulator of digital goods and services as well as digital decision-making: The General Data Protection Regulation (GDPR) took effect. Conditions of consent, core principles such as lawfulness, purpose binding and data minimization, privacy by design and by default and in particular the amount of damages and fines for unlawful data processing have become parts of everyone's reality. A binding and unifying framework exists under which data processing of personal information and thus digitization work. From then on, not only European citizens but also anyone within the EU or confronted with data processing starting from establishments within the EU can trust that their human rights, their individuality, their autonomy is protected under a far-reaching and demanding legal regime.

The impact of the GDPR cannot be underestimated. Ever since it was passed two years prior to its effectuation, in 2016, a worldwide discussion on privacy and data protection has accelerated. The effects of digitization on the individual and the need for a forceful protection have left experts' secluded spaces of contemplation and research and become a far-reaching, obvious, and demanding reality. Companies and state actors alike have changed their data processing, and States as influential as Japan, Brazil and South Korea have passed similar laws to synchronize their data processing regulation with the EU legislation. Even in China and the USA data protection laws have started to regulate encroaching private companies' informational power and thus reduce – at least in the private sector – power asymmetry due to data access and data processing technology.

It might therefore be possible to state, that these rules constitute a milestone, maybe even a turning point, a “Zeitenwende”, in digitization regulation. Between the Data Protection Directive (DPD) of 1995 and the GDPR of 2016, information technology had increasingly penetrated everybody's everyday life – at the industrial internet, in the (video surveilled) public sphere, in one's (smart) home, in (virtual) worlds. Connectivity has created ubiquitous computing, social networks have changed the way of communication, online marketing has targeted in personalized ways, big data has turned individuals into statistics, artificial intelligence has competed with human cognition. All these, and also further developments in digitalization – just think of quantum computing – developed under a legal regime often compared to a toothless tiger: The Member States' authorities had little power and little competences, and the Member States' laws implementing the DPD were highly fragmented leading to a race to the bottom. With the GDPR the EU started its big offensive on digitization regulation creating a human-centered, human-rights oriented information society to counteract the imbalances and asymmetries having developed as a result. The GDPR was accompanied by the Law Enforcement Directive and soon followed by a number of highly demanding and worldwide intensely scrutinized digitalization regulatory acts concentrating on many other effects of information and communication technology such as the Digital Markets Act, the Digital Services Act, the Data Governance Act, or the Data Act und the Artificial Intelligence Act, both presently in the final stages of passing. All these more or less include provisions which leave the GDPR untouched. This may in practice and in detail cause frictions, and the exact width of such declarations is not yet fully understood, but the provisions also make clear that the GDPR remains the most comprehensive data regulation act and as such a blueprint for other regulatory efforts.

It is also the EU's most prominent step of establishing Europe as an alternative to autocratic legal regimes on the one hand and data capitalist legal regimes on the other

Preface

hand, strengthening the individual's importance and thus the backbone of the rule of law and democracy.

This commentary aims at making the leading privacy law in the world more understandable. It gives practitioners from all fields, lawyers, judges, data protection authorities, scholars, academia, regulators and all who are interested in a closer understanding of the GDPR guidance on how to interpret the relevant law. With more than twenty highly knowledgeable experts on their respective fields from practice and academia, the diversity of the EU Member States (and also of UK – this book project started, as did the GDPR, with the UK still being part of the EU), the European perspective is represented thoroughly. The basic principle of the Commentary is that of autonomous interpretation. Concepts based on a particular national legal system, rule, case-law or doctrine have no value in itself. However, problems (and their solutions) in specific countries can be a valuable source of illustration and inspiration but are connected strictly to the European perspective; sometimes, it was unavoidable to rely on non-English literature. It is the Commentary's distinctive feature to offer a sound, well-researched opinion, reflecting human rights' effects and the consequences for society.

The format of a commentary is originally a German academic format. It gives argumentative guidelines by which individual problems can be approached. In a commentary of this style, each article is extensively analyzed and discussed in the light of potential and existing legal and factual problems, presenting relevant literature and judgments (concentrating on ECJ and ECtHR case law in addition to relevant Member State of national Supreme Courts and Courts of Appeal), providing an overview over the material, enlightening about the difficult underlying structures and raising critical points. Difficult, undecided and uncertain questions are not avoided; the authors offer clear positions and give precise arguments. Wording, the historical background including the dialogue, the provision's structure, the interplay with other provisions and the recitals, the goal/telos and relevant case law, statements, decisions and opinions of important stakeholders such as the EDPB (previously, the Art.-29 Working Party), or the Member States' data protection authorities and the EDPS are presented. Sections, sentences, parts and words of each provision after another are thus commented on.

Each comment on the individual provisions is preceded by the text of the article commented on. In general, there is no universal introduction that summarizes common points before a chapter or a section. The comment of the individual provision starts with a brief overview, describing and clarifying the purpose and function of the norm in order to give general arguments how to judge concrete problems. Then, the different paragraphs and sentences are explained and analyzed one after another without paraphrasing or repeating the normtext. The general structure of the comment is from the abstract/general remarks to more specific problems.

This is done by a scientific and at the same time comprehensible style; real and hypothetical examples are presented to illustrate the meaning of a provision in the course of its thorough analysis and interpretation. The commentary focuses on the regulation itself; cross-references to further provisions are made where obvious or helpful for the analysis and understanding, e.g. the Law Enforcement Directive 2016/680, the ePrivacy Directive 2002/58, Regulation 45/2001, third-country-transfer-of-data arrangement). References to the legal status under the DPD are also made.

The most prominent – and influential – commentary on privacy in German law has been Spiros Simitis' commentary, both on the DPD and on the German Federal Data Protection Law (Bundesdatenschutzgesetz). The latter was published in eight editions until 2014 and has continued on the GDPR with the involvement of two of this commentary's editors and some of our authors who partly have been long-time

companions and students of his. Spiros Simitis, who was a law professor at Frankfurt University in Germany and later became head of the Hessian data protection agency and a highest-ranking advisor to the EU, was the “father of data protection”. He had developed the core principles of privacy regulation that still govern the GDPR today already in the 1960s culminating in the world’s first data protections law of the state Hesse in Germany in 1970: the principles of purpose binding, data minimization, transparency, legal justification for data processing, the independent data protection authorities compensating for the inadequate resources of individuals to protect their rights. We are proud that parts of the introduction have been authored by him. As Spiros Simitis sadly passed away in the final days of compiling this commentary, this edition is also commemorating his incomparable importance for the field of data protection.¹

The commentary has been a joint effort of the editors, the authors and the publisher. We thank them all for encouraging us to introduce this fairly new format to the European legal market and going this new path with us. Behind all of these directly visible contributors, numerous other researchers, assistants, staff and students have made its publication with their aid possible – not in the least our families who had to share us with the corrections, recommendations, discussions and editing in the past years. We thank them all from our hearts!

Brussels, Kassel and Frankfurt, June 2023

Vagelis Papakonstantinou

Paul de Hert

Gerrit Hornung

Indra Spiecker genannt Döhmann


beck-shop.de
DIE FACHBUCHHANDLUNG

¹ For more information see the obituaries on https://www.jura.uni-frankfurt.de/47000118/Forschungsstelle_Datenschutz.

CONTENTS

Preface	V
Authors	XIII
List of Abbreviations	XIX

Introduction	1
--------------------	---

CHAPTER I GENERAL PROVISIONS

Art. 1	Subject-Matter and Objectives	77
Art. 2	Material scope	92
Art. 3	Territorial scope	116
Art. 4(1)	Personal data	135
Art. 4(2)	Processing	148
Art. 4(3)	Restriction of processing	156
Art. 4(4)	Profiling	158
Art. 4(5)	Pseudonymisation	162
Art. 4(6)	Filing system	168
Art. 4(7)	Controller	175
Art. 4(8)	Processor	186
Art. 4(9)	Recipient	189
Art. 4(10)	Third party	192
Art. 4(11)	Consent	195
Art. 4(12)	Definitions	216
Art. 4(13)	Genetic data	219
Art. 4(14)	Biometric data	221
Art. 4(15)	Data concerning health	225
Art. 4(16)	Main establishment	229
Art. 4(17)	Representative	237
Art. 4(18)	Enterprise	239
Art. 4(19)	Group of undertakings	240
Art. 4(20)	Binding corporate rules	241
Art. 4(21)	Supervisory authority	242
Art. 4(22)	Supervisory authority concerned	244
Art. 4(23)	Cross-border processing	248
Art. 4(24)	Relevant and reasoned objection	251
Art. 4(25)	Definitions	253
Art. 4(26)	International organisation	258

CHAPTER II PRINCIPLES

Art. 5	Principles relating to processing of personal data	261
Art. 6	Lawfulness of processing	291
Art. 6(1)(f)	Content personalisation	328
Art. 6(1)(f)	Opinion and market research in the age of Big Data	340
Art. 6(1)(f)	Data processing for marketing purposes	345
Art. 6(1)(f)	Credit scoring	356
Art. 6(1)(f)	Video recording	363
Art. 7	Conditions for consent	376
Art. 8	Conditions applicable to child's consent in relation to information society services	391
Art. 9	Processing of special categories of personal data	400
Art. 10	Processing of personal data relating to criminal convictions and offences	420
Art. 11	Processing which does not require identification	426

Contents

CHAPTER III RIGHTS OF THE DATA SUBJECT

Section 1 Transparency and modalities

Art. 12	Transparent information, communication and modalities for the exercise of the rights of the data subject	434
---------	--	-----

Section 2 Information and access to personal data

Art. 13	Information to be provided where personal data are collected from the data subject	448
Art. 14	Information to be provided where personal data have not been obtained from the data subject	458
Art. 15	Right of access by the data subject	466

Section 3 Rectification and erasure

Art. 16	Right to rectification	480
Art. 17	Right to erasure ('right to be forgotten')	487
Art. 18	Right to restriction of processing	496
Art. 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	503
Art. 20	Right to data portability	508

Section 4 Right to object and automated individual decision-making

Art. 21	Right to object	518
Art. 22	Automated individual decision-making, including profiling	525

Section 5 Restrictions

Art. 23	Restrictions	543
---------	--------------------	-----

CHAPTER IV CONTROLLER AND PROCESSOR

Section 1 General obligations

Art. 24	Responsibility of the controller	564
Art. 25	Data protection by design and by default	580
Art. 26	Joint controllers	602
Art. 27	Representatives of controllers or processors not established in the Union	617
Art. 28	Processor	626
Art. 29	Processing under the authority of the controller or processor	646
Art. 30	Records of processing activities	649
Art. 31	Cooperation with the supervisory authority	656

Section 2 Security of personal data

Art. 32	Security of processing	659
Art. 33	Notification of a personal data breach to the supervisory authority	670
Art. 34	Communication of a personal data breach to the data subject	681

Section 3

Data protection impact assessment and prior consultation

Art. 35	Data protection impact assessment	687
Art. 36	Prior consultation	706

Section 4

Data protection officer

Art. 37	Designation of the data protection officer	714
Art. 38	Position of the data protection officer	725
Art. 39	Tasks of the data protection officer	730
Art. 40	Codes of conduct	736
Art. 41	Monitoring of approved codes of conduct	750
Art. 42	Certification	757
Art. 43	Certification bodies	767

CHAPTER V

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Art. 44	General principle for transfers	775
Art. 45	Transfers on the basis of an adequacy decision	785
Art. 46	Transfers subject to appropriate safeguards	803
Art. 47	Binding corporate rules	823
Art. 48	Transfers or disclosures not authorised by Union law	835
Art. 49	Derogations for specific situations	838
Art. 50	International cooperation for the protection of personal data	854

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES

Art. 51	Supervisory authority	858
Art. 52	Independence	863
Art. 53	General conditions for the members of the supervisory authority	873
Art. 54	Rules on the establishment of the supervisory authority	877
Art. 55	Competence	880
Art. 56	Competence of the lead supervisory authority	884
Art. 57	Tasks	889
Art. 58	Powers	894
Art. 59	Activity reports	901

CHAPTER VII

COOPERATION AND CONSISTENCY

Section 1

Cooperation

Art. 60	Cooperation between the lead supervisory authority and the other supervisory authorities concerned	904
Art. 61	Mutual assistance	915
Art. 62	Joint operations of supervisory authorities	922

Section 2

Consistency

Art. 63	Consistency mechanism	927
Art. 64	Opinion of the Board	938
Art. 65	Dispute resolution by the Board	959
Art. 66	Urgency procedure	975
Art. 67	Exchange of information	983

Contents

Section 3
European data protection board

Art. 68	European Data Protection Board	986
Art. 69	Independence	991
Art. 70	Tasks of the Board	993
Art. 71	Reports	999
Art. 72	Procedure	1000
Art. 73	Chair	1002
Art. 74	Tasks of the Chair	1003
Art. 75	Secretariat	1004
Art. 76	Confidentiality	1007

CHAPTER VIII
REMEDIES, LIABILITY AND PENALTIES

Art. 77	Right to lodge a complaint with a supervisory authority	1010
Art. 78	Right to an effective judicial remedy against a supervisory authority	1017
Art. 79	Right to an effective judicial remedy against a controller or processor	1023
Art. 80	Representation of data subjects	1030
Art. 81	Suspension of proceedings	1036
Art. 82	Right to compensation and liability	1041
Art. 83	General conditions for imposing administrative fines	1051
Art. 84	Penalties	1064

CHAPTER IX
PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

Art. 85	Processing and freedom of expression and information	1070
Art. 86	Processing and public access to official documents	1086
Art. 87	Processing of the national identification number	1090
Art. 88	Processing in the context of employment	1094
Art. 89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ...	1113
Art. 90	Obligations of secrecy	1122
Art. 91	Existing data protection rules of churches and religious associations	1128

CHAPTER X
DELEGATED ACTS AND IMPLEMENTING ACTS

Art. 92	Exercise of the delegation	1136
Art. 93	Committee procedure	1143

CHAPTER XI
FINAL PROVISIONS

Art. 94	Repeal of Directive 95/46/EC	1146
Art. 95	Relationship with Directive 2002/58/EC	1150
Art. 96	Relationship with previously concluded Agreements	1155
Art. 97	Commission reports	1156
Art. 98	Review of other Union legal acts on data protection	1161
Art. 99	Entry into force and application	1165

Index	1169
-------------	------