General Data Protection Regulation

Article-by-Article Commentary
Spiecker gen. Döhmann / Papakonstantinou / Hornung / De Hert

General Data Protection Regulation
General Data Protection Regulation

Article-by-Article Commentary

edited by

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

2023
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 and 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 triologue, 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

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 ................................................................................................. 172
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

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
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
## Contents

<table>
<thead>
<tr>
<th>Section 3</th>
<th>European data protection board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 68</td>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>Art. 69</td>
<td>Independence</td>
</tr>
<tr>
<td>Art. 70</td>
<td>Tasks of the Board</td>
</tr>
<tr>
<td>Art. 71</td>
<td>Reports</td>
</tr>
<tr>
<td>Art. 72</td>
<td>Procedure</td>
</tr>
<tr>
<td>Art. 73</td>
<td>Chair</td>
</tr>
<tr>
<td>Art. 74</td>
<td>Tasks of the Chair</td>
</tr>
<tr>
<td>Art. 75</td>
<td>Secretariat</td>
</tr>
<tr>
<td>Art. 76</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER VIII</th>
<th>REMEDIES, LIABILITY AND PENALTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 77</td>
<td>Right to lodge a complaint with a supervisory authority</td>
</tr>
<tr>
<td>Art. 78</td>
<td>Right to an effective judicial remedy against a supervisory authority</td>
</tr>
<tr>
<td>Art. 79</td>
<td>Right to an effective judicial remedy against a controller or processor</td>
</tr>
<tr>
<td>Art. 80</td>
<td>Representation of data subjects</td>
</tr>
<tr>
<td>Art. 81</td>
<td>Suspension of proceedings</td>
</tr>
<tr>
<td>Art. 82</td>
<td>Right to compensation and liability</td>
</tr>
<tr>
<td>Art. 83</td>
<td>General conditions for imposing administrative fines</td>
</tr>
<tr>
<td>Art. 84</td>
<td>Penalties</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER IX</th>
<th>PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 85</td>
<td>Processing and freedom of expression and information</td>
</tr>
<tr>
<td>Art. 86</td>
<td>Processing and public access to official documents</td>
</tr>
<tr>
<td>Art. 87</td>
<td>Processing of the national identification number</td>
</tr>
<tr>
<td>Art. 88</td>
<td>Processing in the context of employment</td>
</tr>
<tr>
<td>Art. 89</td>
<td>Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</td>
</tr>
<tr>
<td>Art. 90</td>
<td>Obligations of secrecy</td>
</tr>
<tr>
<td>Art. 91</td>
<td>Existing data protection rules of churches and religious associations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER X</th>
<th>DELEGATED ACTS AND IMPLEMENTING ACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 92</td>
<td>Exercise of the delegation</td>
</tr>
<tr>
<td>Art. 93</td>
<td>Committee procedure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER XI</th>
<th>FINAL PROVISIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 94</td>
<td>Repeal of Directive 95/46/EC</td>
</tr>
<tr>
<td>Art. 95</td>
<td>Relationship with Directive 2002/58/EC</td>
</tr>
<tr>
<td>Art. 96</td>
<td>Relationship with previously concluded Agreements</td>
</tr>
<tr>
<td>Art. 97</td>
<td>Commission reports</td>
</tr>
<tr>
<td>Art. 98</td>
<td>Review of other Union legal acts on data protection</td>
</tr>
<tr>
<td>Art. 99</td>
<td>Entry into force and application</td>
</tr>
</tbody>
</table>

Index .............................................................................. 1169

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Authors

Jan Philipp Albrecht is a politician of the Greens-European Free Alliance. From 2018 to 2022, he has been serving as Minister for Energy, Agriculture, the Environment, Nature and Digitalization of Schleswig-Holstein. He has been a board member of the Heinrich Böll Foundation since June 2022. He was the rapporteur of the European Parliament for the EU’s General Data Protection Regulation as well as for the EU-US data protection framework agreement.

Marco Almada is a researcher at the European University Institute of Florence, where he is pursuing a PhD in the regulation of artificial intelligence. Before starting his doctoral research, he obtained degrees in law from the University of São Paulo and computing from the University of Campinas. He has published on law and digital technologies, with particular attention to theoretical issues and the legal frameworks for personal data protection and artificial intelligence in Brazil and the European Union.

Dr. Jens Ambrock is head of department at the Hamburg Commissioner for Data Protection and Freedom of Information. In this position as a GDPR regulator, he has been a rapporteur at the EDPB for several guidelines. He leads the Schrems II Taskforce coordinating the enforcement of the multiple German supervisory authorities concerning international data transfers. In addition, Dr. Ambrock is a lecturer for data protection law at Kiel University.

Dr. Sebastian Bretthauer is a senior research assistant and postdoc at the Chair for Administrative Law, Information Law, Environmental Law and Legal Theory of Prof. Dr. Indra Spiecker gen. Döhmänn, LL.M. and project leader at the Research Center for Data Protection at Goethe-University Frankfurt. His research interests are especially in data protection law, where he has contributed as an author to numerous publications.

Dr. Laura Carmichael LLB (Hons), MSc (Dist.), PhD is an interdisciplinary Research Fellow within the IT Innovation Centre, School of Electronics and Computer Science, University of Southampton. She has a degree in law, LLB (Hons), and an MSc (Dist.) and PhD in Web Science. She has been involved in various interdisciplinary research projects related to data sharing and re-usage, including the EU-funded Data Pitch open innovation programme. She is currently working as part of the Social Data Foundation initiative, and the PETRAS Data Sharing Foundation (PETRAS-DSF) project: Building a Trustworthy Data Sharing Ecology for IoT Data Assets.

Dr. Emma Cradock (LLB, LLM, MSc, PhD) is an academic and practitioner in the fields of Law, Computer Science and Web Science, with a keen focus on Privacy. Dr. Cradock received her interdisciplinary PhD from the University of Southampton in 2022 with her thesis entitled ‘A New Approach to Categorising Personal Data to Increase Transparency Under the Obligation to Inform’. The thesis focused on what privacy laws can learn from Computer and Information Science models, to increase the transparency of personal data processing. Dr Cradock currently works with commercial companies to apply her research and guides them in their compliance with other global privacy laws.

Dr. Alexander Dix, LL.M. (Lond.) is Vice-Chair of the European Academy for Freedom of Information and Data Protection in Berlin. From 1998 to 2005 he was Commissioner for Data Protection and Access to Information in Brandenburg. He was then elected as Berlin Commissioner for Data Protection and Freedom of Information, a post which he held until January 2016. From 2005 to 2015 he chaired the International Working Group on Data Protection in Telecommunications (also known as „Berlin Group“) and represented the German Länder in the Art. 29 Working Party of European Data Protection Authorities. He was a member of the Expert Group on Governance of Data
and AI in the UN Global Pulse Project. Dr Dix has published extensively on transborder data flows, privacy in global networks and freedom of information.

**Dr. Stefan Drewes** is an attorney based in Bonn/Germany. He has more than 20 years of professional experience in advising companies on all matters related to data protection law and has been working since 2002 as a data protection officer for several companies. He regularly gives lectures on data protection law topics and has contributed numerous publications in his specialised field.

**Jos Dumortier** studied law in Leuven, Nancy and Heidelberg between 1968 and 1975, obtained his PhD in 1981 and studied Information Science at the Université Libre in Brussels between 1981 and 1983. He has been a full professor of law at KU Leuven between 1987 and 2014. In 1990 he was the founder of the Interdisciplinary Centre for Law and Information Technology (currently ‘CITIP’) of which he acted as the director until 2014. Today, Prof. Dumortier is a member of the Bar of Brussels as a founding partner of Timelex, a law firm specialised in information technology and data protection law.

**Domingos Farinho** is an Assistant Professor at the University of Lisbon School of Law. His main areas of research are Administrative Law, Fundamental Rights, and Legal Theory. He has been especially interested in fundamental rights in the context of Public Administrations and Cyberspace. He has coordinated and participated in several courses regarding Data Protection, the GDPR and access to State-held information. He has written extensively on these topics.

**Pieter Gryffroy** works as a lawyer for Timelex, a Brussels-based law firm specialized in matching law and technology. In that capacity Pieter works with the GDPR on a daily basis, in particular in the context of implementing EU-funded research projects. Before joining Timelex, he worked as an academic researcher in the field of data of data protection law for the Europa-Institut at Saarland University, Germany.

**Prof. Paul De Hert** is a Professor at the Free University of Brussels (VUB, Vrije Universiteit Brussel), where he currently teaches Criminal Law, and an assistant-professor at the University of Tilburg, where he teaches a course about Privacy and Data Protection. His research interests are focused on privacy & technology and criminal law. His work testifies of a human rights approach with a concern for theory. At VUB, he is Director of the research group on human rights (FRC), Vice-Dean of the Faculty of Law and Head of the Department of Interdisciplinary Studies of Law. In the past he directed the Research group Law Science Technology & Society (LSTS). He is a board member of a number of leading international law reviews and is also co-editor in chief of several series relating to his areas of specialisation.

**Prof. Dr. Gerrit Hornung**, LL.M. is a Professor for Public Law, IT Law and Environmental Law at the University of Kassel, where he is also one of the directors of the university's Interdisciplinary Research Centre for Information System Design (ITeG). His research interests cover legal issues of data protection, IT security, electronic government and new surveillance technologies. Interdisciplinary research projects focus on legal criteria for IT design. He published books on the legal problems of biometric ID cards and patient data cards, and on fundamental rights innovations. He is also a co-editor of a comprehensive German commentary on the GDPR and a handbook on IT security law.

**András Jóri**, PhD, attorney-at-law, served as Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary from 2008 to 2011. Before and after his mandate, Dr Jóri worked as an attorney, advising his clients on data privacy and IT law; he also did extensive regulatory work, advising the state and industry groups on many fields of IT and data protection law, as well as e-commerce, e-signatures,
e-archiving, and e-procurement. He has published widely about data privacy in Hungary and abroad, and wrote the first commentary on data protection law in Hungary. As a honorary associate professor, he has been teaching data protection law at the University of Pécs since 2006.

**Dr. Irene Kamara** is Assistant Professor Cybercrime Law and Human Rights at the Tilburg Institute for Law, Technology, and Society in The Netherlands, Transatlantic Technology Law Forum Fellow at Stanford University, and affiliate researcher at the Vrije Universiteit Brussel in Belgium. Her research focuses on cybercrime and cybersecurity law, and the role of private regulation in the protection of fundamental rights, and in particular the right to protection of personal data, the right to private life, and non-discrimination.

**Dr. Moritz Karg** is head of the department of E-Government and Digitization in the State Chancellery of Schleswig-Holstein in Kiel. He worked for over 15 years for the supervisory authorities of Schleswig-Holstein and Hamburg with the focus on social media and telecommunications. Currently he is responsible for the digitization of public administration in Schleswig-Holstein. He has published on various topics related to data protection in the social media area and the activities of the supervisory authorities.

**Juliano Maranhão** has more than 20 years of experience in the areas of antitrust, regulatory, administrative and digital law, with an emphasis on artificial intelligence and data protection. He is currently an associate professor at the University of São Paulo (Universidade de São Paulo) Law School, president of Lawgorithm Institute for Artificial Intelligence (Instituto Lawgorithm de Inteligência Artificial), member of the Steering Committee of the International Association for Artificial Intelligence and Law and officer of the Legal Grounds Institute.

**Hans-W. Micklitz** is Professor for Economic Law, Robert Schuman Centre for Advanced Studies, European University Institute, Florence and Finland Distinguished Professor at the University of Helsinki. His research interest focus on Private Law, European and International Economic Law, Private Law Theory.

**Dr. Evangelia Papadaki** is a Legal Consultant in the field of cyber security and data protection. The interplay between law and technology has been her main research area of interest. Both her work and postgraduate studies focus on the legal issues arising from the use of technologies, and more specific, on the regulatory challenges posed by technological advances to cyber security and the protection of personal data. She is a certified Data Protection Officer. Her studies include an LL.B., an LL.M. in Cyberlaw, a MSc in Web Science and a PhD in Web Science.

**Vagelis Papakonstantinou** is a Professor on Personal Data Protection Law at the Free University of Brussels (VUB, Vrije Universiteit Brussel), focusing also on Cybersecurity, Intellectual Property, and the broader topic of technology regulation. He is the coordinator of VUB’s Cyber and Data Security Lab (CDSL), and also participates, as a core member, in VUB’s Research Group on Law Science Technology & Society (LSTS) and the Brussels Privacy Hub. For the period 2016-2021 he has been a member (alternate) of the Hellenic Data Protection Authority.

**Cristina Pauner Chulvi** is a Professor of Constitutional Law at the Universitat Jaume I of Castellón. She has made several research stays at European universities (Sorbonne University-Paris, Rome III University, London School of Economics and University of Oxford). She has completed various specialized courses on human rights in the International Institute of Human Rights (Strasbourg) and the Diploma of Specialization in Constitutional Law and Political Science at the Centre for Political and Constitutional Studies (Madrid).
Artemi Rallo Lombarte is a Constitutional Law Full Professor at the Jaume I University in Spain. He has served, among others, as Senator and Deputy of Spain, as well as, as Director of the Data Protection Spanish Agency. He has performed research activity at international centres such as the International Human Rights Institute (Strasbourg), La Sapienza University (Rome), Paris I-Panthéon-Sorbonne University and Montreal University. He is the author of numerous monographs, collective books and scientific articles in specialised national and international reviews. Graduate in Law with Extraordinary Prize Honours (1988) and Doctor in Law at the University of Valencia (1990).

Judith Rauhofer is a Senior Lecturer in IT Law at the University of Edinburgh. She holds professional legal qualifications in Germany (Rechtsanwalt) and England ( Solicitor). Her research interests include all areas of data protection, online privacy, data justice, electronic surveillance and technology law. Judith is a co-author of the Commonwealth Model Provisions on Data Protection.

Dr. Philipp Richter works as a legal officer for the Data Protection and Freedom of Information Commissioner of Rhineland-Palatinate (Germany). He has been publishing in the field of data protection for over ten years, especially with regard to the GDPR and its introduction. His main field of work nowadays are data protection in internet services, especially websites and social media as well as basic matters of GDPR interpretation and cooperation of the EU-Data protection authorities. He is also the host of his authority’s official Podcast “Datenfunk”.

Prof. Dr. Alexander Roßnagel is the Hessian Commissioner for Data Protection and Freedom of Information since 2021. He ist also a senior professor of public law with a focus on the law of technology and environmental protection at the University of Kassel. He heads the "Project Group for Constitutionally Compatible Technology Design (provet)" and is director of the Scientific Center for Information Technology Design (ITeG).

Giovanni Sartor is professor in Legal Informatics at the University of Bologna, and professor in Legal informatics and Legal Theory at the European University Institute of Florence. He coordinates the CIRSFID-AI for Law and Governance unit at the Alma-AI research center of the University of Bologna. He holds the ERC-advanced grant (2018) for the project Compulaw (2019 – 2025). He has published widely in legal philosophy, computational logic, and computer law, AI & law. He is co-director of the Artificial Intelligence and Law Journal and co-editor of the Ratio Juris Journal. His research interests include legal theory, early modern legal philosophy, logic, argumentation theory, modal and deontic logics, logic programming, multiagent systems, computer and Internet law, data protection, e-commerce, law and technology.

Burkhard Schafer is Professor for Computational Legal Theory at the University of Edinburgh where he was for many years also the director of the SCRIPT Centre for IT and IP Law. He joined Edinburgh in 1996, after having studied Theory of Science, Logic, Theoretical Linguistics, Philosophy and Law at the Universities of Mainz, Munich, Florence and Lancaster. His interest is the interaction between law, science and computer technology from doctrinal, comparative and legal-theoretical perspectives. He served as member of the government expert group “Ethical Digital Scotland” and the ethics advisory group of the UK Cabinet Office. He is currently the convenor of the “Legal Services Industry” working group of AI4People and member of the accreditation committee for legal technologists of the Law Society of Scotland.

Dr. Peter Schantz is Head of the Directorate General “Policy Planning & Communication” at the German Federal Ministry of Justice. As member of the Ministry’s data protection law unit he followed closely the negotiations on the GDPR and is author
of numerous publications on data protection law. Before joining the German Federal Ministry of Justice, he worked as a lawyer in an international law firm and was involved in several privacy-related cases before the German Federal Constitutional Court.

Prof. Dr. Stephanie Schiedermair holds the Chair for European Law, Public International Law and German Public Law at Leipzig University. She is Director of the university’s International Law Institute and coordinates the foreign affairs of the law faculty. Her research focuses on international and European media and data protection law (Right to be forgotten, GDPR, Artificial Intelligence) and on general questions concerning the interaction of international, European and national law. Research stays led her to Yale and Monash University. She is a regular speaker at international and national conferences and a member of the German Commission for the Determination and Review of the Financial Requirements of Public Broadcasting in Germany.

Achim Seifert, Dr. jur., is Professor of Private Law, German and European Labour Law and Comparative Law at the Friedrich-Schiller-University of Jena (since 2011). He previously taught European and International Labour Law at the University of Luxembourg. His fields of research are European as well as International Labour Law and specifically employee data protection law and employee participation in company boards. He is a member of the editorial Board of the European Labour Law Journal and the Comparative Labor Law & Policy Journal.

Prof. Dr. Dr. h.c. mult. Spiros Simitis († 2023) was Professor emeritus on Labor Law, Civil Law and Legal Informatics, Goethe University Frankfurt/Main, Germany. Numerous publications in the fields of Civil Law, Labor Law, Liability Law, Child Care Law, Legal Theory and Data Protection Law, often with interdisciplinary approaches. He was the founder of the Data Protection Research Institute thereof. Former Chief Data Protection Authority of Hessa. Honorary Member of the Deutscher Juristentag. Chair of the Expert Commission on Data Protection of the European Council. Advisor of the EU Commission; Commission’s High-Level Expert Commission on the Charter of Fundamental Rights; Chair of the German National Ethics Commission. Honorary Doctor of several universities; Bundesverdienstkreuz 1st Class, Officer of the French Legion of Honour, University of Berkeley-California’s Chancellor’s Citation. He also edited the leading commentaries on the DPD and German data protection law.

Dr. Eva Souhrada-Kirchmayer is a judge at the Federal Administrative Court in Austria, where she mainly deals with data protection cases. She worked for many years in leading positions in the field of data protection in the Prime Minister’s Office and in the Austrian Data Protection Commission. She gives lectures on data protection law topics and regularly writes publications in this field.

Prof. Dr. Indra Specker genannt Döhmann, LL.M. (Georgetown Univ.) holds the chair of Public Law, Information Law, Environmental Law and Legal Theory at Goethe University Frankfurt, Germany. She also heads the data protection research institute, and is director of the Institute of European Health Politics and Social Law, inege, both thereof. Her research, often interdisciplinary, concentrates on data protection and it-security law, artificial intelligence and digitalization regulation, also cover constitutional and administrative law under the perspective of uncertainty, trust and control. As one of the first lawyers, she was appointed to Germany’s National Academy of Technology, acatech.

Sophie Stella-Bourdillon is Professor in IT law at VUB and the Privacy Hub and Principal Legal Engineer at Immuta Research. She is also a visiting professor at the University of Southampton Law School of law, where she held the chair in IT law and Data Governance until 2022. Sophie is the author and co-author of several legal articles, chapters and books on data protection and privacy. She has also served as a
Authors

legal and data privacy expert for the European Commission, the Council of Europe, the Organisation for the Cooperation and Security in Europe, and for the Organisation for Economic Cooperation and Development.

Olivia Tambou is a professor at the Université Paris-Dauphine, PSL Research University since 2007 and External Scientific Fellow at the Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law in Luxembourg. She is also the founder-editor of blogdroiteuropeen. Olivia Tambou is the author of nearly 50 publications in French, English and Spanish mainly on data protection law including her Manuel de droit européen des données, Ed. Bruylant collection Droit administratif européen matériel, Bruylant 2020).

Niko Tsakalakis is a former Senior Research Fellow at the University of Southampton, where he conducted research into data protection by design for emerging technologies. He holds a PhD on data protection for electronic identification, and has worked as a legal engineer for eIDAS-compliant services, AI decision-making, and Mobility-as-a-Service systems. Since 2023 he has joined the Council of the European Union as a permanent official in data protection.

Jorge Viguri Cordero is Contracted Lecturer (holder of a PhD) in Constitutional Law at Universitat Jaume I. Law Degree (2010-2014), Master’s degree in Law (2014-2016). He has been a researcher in the EU projects CRISP (Evaluation and Certification Schemes for Security Products) and Phaedra II (Improving Practical and Helpful Cooperation between Data Protection Authorities) between 2014 and 2017, both funded by the European Commission. Predoctoral researcher financed by Generalitat Valenciana (under the program VALi+D, co-financed by the European Social Fund) for the realisation of his doctoral thesis (2017-2020) and postdoctoral researcher at UJI (2021). His research lines include the right to protection of personal data, the right to international protection, and transparency. He wrote the book “Security and Data Protection in the Common European Asylum System” (Tirant lo Blanch, 2020) and over twenty articles in various Scientific Journals, as well as book chapters.
of identification criteria regarding what was set in the DPD definition. Besides an ‘identification number’ the Comm proposed ‘location data’ and ‘online identifier’. The EP added ‘name’ to the list of criteria as well as “unique identifier” instead of ‘online identifier’. These changes were adopted in the GDPR definition with the option of ‘online identifier’. The Comm-P also added genetic identity as one of the domains where specific factors may be used to identify a person (→ Art. 4(13)). This change was also included in the GDPR. Overall, the changes proposed by the Comm and the EP broaden the scope of the concept thus amplifying the material scope of the GDPR.

The EP also put forth definitions of ‘pseudonymous data’ and ‘encrypted data’. The former was almost completely adopted under the definition of ‘pseudonymisation’ (→ Art. 4(5)). This reference shows that although the European legislator considered pseudonymisation as a means to reduce the risks of data processing it nevertheless allowed for the possibility that such data can still be linked to a person and they must thus be considered as personal data. Other than this new reference to pseudonymisation, both recitals 26, in the DPD and the GDPR, are in line with each other. The latter definition of encrypted data was not included in the GDPR, even though encryption is mentioned in several places in the text. This poses a difficulty when considering if encrypted data are personal data under the GDPR in situations where controllers, processors and third parties in general do not hold the key to perform the decryption operations,26 such as in messaging apps with end-to-end encryption. The EP also developed the identification criteria set out in recital 23 of the Comm-P. It added the direct or indirect singling out as one way to identify a person through data and it also added the demand to account for “all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development”.27 The first proposal had also been made by the Art. 29 WP28 and it seems to be its influencing source. These proposals were included in recital 26 of the GDPR. The Comm’s and the EP’s concern regarding online identifiers on recital 24 of the proposal were combined in recital 30 of the GDPR.

III. The constituent elements of the concept of personal data

1. Information

The GDPR does not define the term ‘information’. Furthermore, it states that personal data refers to ‘any’ information. As such, the CJEU has interpreted information in a broad implicit sense,29 building from the work of the Art. 29 WP.30 This means that anything that can be understood as information falls within the concept of personal data if the remaining constituent elements apply. What is to be understood as information remains for the interpreter to argue within the conventions of language,31 but it must surely denote a relational property as foreseen in Art. 4 no. 1: information, though a thing in

---

27 EU Parliament Report on the on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data and on the free movement of such data.
28 Cf. Art. 29 WP199, p. 5.
30 See Art. 29 WP136, pp. 6 et seq.
itself\textsuperscript{32}, always comprises the relation between the availability of certain knowledge and one or more entities, be they persons, objects, states of affairs or something else (and even if inaccurately identified as shown below).\textsuperscript{33} However, although information always relates to an entity, it is for the law to determine what are the relational criteria that can be used to consider that a piece of information relates to specific persons and should therefore be understood as personal data.

The Art. 29 WP recognises the relational property of information as an autonomous constitutive element ("relating to")\textsuperscript{34} of the definition of personal data and provides for a categorisation of criteria of connection between information and natural persons: i) content, ii) purpose or iii) result. Information relates to a natural person from the perspective of content when such information is about a natural person in a common sense, in as much as it provides knowledge of traits of a certain person.\textsuperscript{35} Regarding the purpose criterion, information relates to a natural person when it may be used, according to context, to evaluate, ground decisions or influence the “status or behaviour of an individual”.\textsuperscript{36} Finally, information may relate to a natural person concerning a result criterion when, although not about traits of a natural person or aimed at conforming behaviour, nonetheless affects the legal positions of a person, such as rights, liberties or interests.\textsuperscript{37} For example, when data about cars allow for the monitoring of their drivers or data about products tag to clients.\textsuperscript{38} The criteria through which information may relate to natural persons show that the crucial common element is the potential or existent effect of information on the legal sphere of a natural person, which also calls on the importance of context-dependant analysis.\textsuperscript{39}

Regarding the nature of the information, a distinction between objective and subjective information is usually made,\textsuperscript{40} both being admitted by the GDPR. This means that for the purpose of the concept of personal data, information is considered not only when an objective appraisal of knowledge is possible (physical traces for instance) but also when such knowledge relies on a subjective appreciation.\textsuperscript{41} This means that the information may be false, inaccurate or dependant on third party judgments (such as the opinion of a friend or the evaluation of a service provider) and can still be considered information under the GDPR.\textsuperscript{42} Indeed, evaluative information comprises an important part of personal data.\textsuperscript{43} There must always be a connection between the

\textsuperscript{33} See also the concept of information as "semantic information", Hallinan/Gellert, 'The Concept of Information', pp. 282-284.
\textsuperscript{34} See Art. 29 WP136, p. 9.
\textsuperscript{35} Ibid, p. 10.
\textsuperscript{36} Ibid.
\textsuperscript{37} Ibid, pp. 10-11.
\textsuperscript{38} See on this, in the context of RFID technology, Art. 29 WP105.
\textsuperscript{39} See Purtova, 'From knowing by name to targeting: the meaning of identification under the GDPR', IDPL, Vol. 12, No. 3 (2022), pp. 163-183.
\textsuperscript{40} See Art. 29 WP 136, p. 6; CJEU C-434/16, 20.12.2017, Nowak, ECLI:EU:C:2017:994, para. 34.
\textsuperscript{41} See Art. 29 WP 136, p. 6; see also Finck/Pallas, 'They who must not be identified', pp. 11-12.
\textsuperscript{42} See however CJEU Joined Cases C-141/12 and C-372/12, 17.07.2014, TS, EUC:2014:2081, para. 44 to para. 48. In this judgement, the CJEU found that, although information contained in an asylum request application was personal data, the assessment done by public officials was not, due to the understanding that such assessment did not contain information relating to the applicant but related to asylum law in as much as it would apply to any other applicant in similar circumstances. For this reason, the Court differentiates this situation which refers to access to administrative documents from a case of protection of personal data. This distinguishes the present case from the Nowak decision, as the CJEU recognises (see C-434/16, 20.12.2017, Nowak, ECLI:EU:C:2017:994, para. 56).
\textsuperscript{43} See Karg, 'Art. 4(1)', in Simitis/Hornung/Spiecker gen. Döhmann, 288, mn. 29.

Domingos Farinho

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
availability of certain knowledge and an entity, even if that connection is merely stated but not proved.

The GDPR does not limit the notion of Information to types of content within the spectrum of private/public sphere of information (although this spectrum is relevant within the GDPR, after certain knowledge has been qualified as information). This is in line with the distinction made in the EU CFR between the right of respect for private and family life in Art. 7 and the right to the protection of personal data in Art. 8.44 Information, in the broad sense adopted by the GDPR, confirms itself as a nexus between any knowledge and an entity identified by such knowledge: a certain (natural) person as we shall see infra concerning the second constituent element of the concept of personal data. This makes it clear that information, in the sense of the GDPR, comprises not only intimate and private information but also information related to public dimensions of a person, be it in a family, professional,45 leisurely or other capacity. Public information,46 even if divulged by the data subjects (for instance, in social networks), and whatever the context of relevance,47 is to be considered as information under the GDPR, unless exceptions to the material scope apply (→ Art. 2 para. 2 lit. c mn. 54). This is confirmed by the identifiers used as examples in Art. 4 no. 1.

The format of information also does not define it under the GDPR although the GDPR does mention certain types of formats such as “biological samples” (Art. 4 no. 13), “facial images and dactyloscopic data” (Art. 4 no. 14) or “electronic means” (for instance Art. 15 para. 3). All these formats may be sources of information and provided that the remaining conceptual constituents verify may allow for the acknowledgement of personal data. The key feature is that the processing of information may be done through such formats. The CJEU has considered as personal data information in several different formats – physically or electronically written text,48 Internet traffic data,49 IP numbers50 or cookies,51 graphic representations, such as fingerprints,52 and video

44 Art. 29 WP 136, p. 7.
45 The CJEU supports this interpretation, building on the interpretation of Art. 8 ECHR and the abovementioned distinction between Art. 7 and Art. 8 of the EU CFR, see Joined Cases C-465/00, C-138/01 and C-139/01, 20.05.2003, Österreichischer Rundfunk, ECLI:EU:C:2003:294, para. 73; C-73/07, 16.12.2008, Satakunnan Markkinapörssi and Satamedia, 16.12.2008, ECLI:EU:C:2008:727, para. 65; C-342/12, 30.05.2013, Worten, ECLI:EU:C:2013:355, para. 46; C-683/13, 19.6.2014, Pharmacocontinente – Saúde e Higiene, ECLI:EU:C:2014:2028, para. 13; See also the reference made in Art. 9 para. 2 lit. b which presupposes personal data relating to information processed in the context of an employment relationship.
47 Indeed, it can regard information concerning people passing through common parts of a residential building, see CJEU C-708/18, 11.12.2019, Asociatia de Proprietari, ECLI:EU:2019:1064; or even someone passing through a specific point on a street, see CJEU C-212/13, 11.12.2014, Rynes, ECLI:EU:C:2014:2428.
49 CJUE C-221/12, 22.11.2012, Probst, ECLI:EU:C:2012:748; Joined Cases C-293/12 and C-594/12, 08.04.2014, Digital Rights Ireland, ECLI:EU:C:2014:238.

Domingos Farinho

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Any format of access to knowledge regarding a certain natural person may provide information within the concept of personal data of the GDPR.

2. Natural person

As was mentioned at the beginning of the previous point, given the adopted concept, information necessarily relates to an entity, which means that the segment “relating to” in Art. 4 no. 1 is not an autonomous constituent element but a connecting term from the ‘information’ element to the ‘natural person’ element. For information to become personal data Art. 4 no. 1 deems it necessary for any information to relate to "an identified or identifiable natural person". ‘Natural person’ is thus the next constituent element of the concept of personal data in the GDPR as it narrows the information that is to be considered.

The first important distinction to be made, and called upon by the definition, is between natural and legal persons. The GDPR excludes the protection of data pertaining to legal persons, whatever form they may take in any Member State. The legislator establishes a direct connection with the fundamental rights recognised to natural persons, including the right to the protection of personal data, in the EU CFR. The latter also protects legal persons but the GDPR legislator chose to limit the concept of personal data in line with a teleological nexus between the human dignity principle (Art. 1 EU CFR) and natural persons but also in accordance with the mandate of Art. 16 para. 2 of the TFEU. Under the DPD, the CJEU had determined that "legal persons can claim the protection of Articles 7 and 8 of the Charter […] in so far as the official title of the legal person identifies one or more natural persons." This has changed under the GDPR. However, it seems to be the case that whenever information concerning members of bodies or statutory positions of legal persons refers to identifiable natural persons such information should be considered as personal data. Thus, following recital 14 of the GDPR although legal persons cannot claim the protection of the GDPR even for personal data which concern them, natural persons whose personal data are used by legal persons can claim protection of the GDPR if such personal data are processed in a context relating to these natural persons, on grounds of “content”, “purpose” or “result”.

Once established that only natural persons matter for the purposes of the definition of personal data, the limits of such personality must still be ascertained. One must look at the beginning and the end of natural personality. The relevant end of the natural person regarding the concept of personal data in the GDPR results clearly from recital 27 where it is stated that the GDPR "does not apply to the personal data of deceased persons."
persons”. Member States may, however, “provide for rules regarding the processing of personal data”\textsuperscript{64} of such persons.

As far as the beginning of personality is considered the GDPR is mute, making no consideration regarding another important legal distinction between \textit{unborn life} (\textit{nasciturus}) and already-born persons.\textsuperscript{65} Such silence must then be interpreted, especially as it contrasts with the above-mentioned recital 27 insomuch as the GDPR does not take a similar stance regarding the delimitation of the beginning of natural personality. On the one hand, this contrast seems to support the view that the legislator could have used some criteria to assure such delimitation and chose not to. On the other hand, although natural personality is acquired by birth, information regarding conceived human life may become information related to “an identified or identifiable natural person” and thus call for protection even before the birth of such a person as a condition to guarantee the freedoms and rights of the new natural person.\textsuperscript{66} This is especially clear in the case of genetic data.\textsuperscript{67} It would defeat the purpose of the GDPR of protecting the personal data of natural persons from the moment of their birth if some data that would qualify as personal data after birth could already be collected before birth without the application of the GDPR. This is especially illustrated by the references in Art. 4 no. 1 to such personality specific factors as “physical, physiological, genetic [and] mental” factors. Thus, the GDPR must apply to unborn natural persons whenever all the remaining constituent elements apply.\textsuperscript{68}

3. Identification

Once “any information” relates to “natural persons” within the framework analysed above, the concept of personal data begins to assume its complete definition under the GDPR. But the way in which “any information” can relate to “natural persons” still allows for a great margin of uncertainty. Thus, the legislator uses a third and final constituent element: identification. The GDPR defines personal data as information relating to natural persons if and only if such information relates to “an identified or identifiable” natural person. This means that the GDPR does not apply to non-personal data both in the sense of data that do not pertain to any person but also in the sense of data that pertain to someone but do not and cannot identify a specific individual and thus according to Art. 4 no. 1 do not relate to a natural person.

The legislator does not define “identified natural person” although it does explain on Art. 4 no. 1 what an “identifiable person” is. By doing so the legal interpreter can also understand what is meant by “identified natural person”. The CJEU has treated this constituent element of the concept of personal data through a two-step approach, where first it is to be determined if certain information identifies a natural person and, second, in case it does not, it must be determined if such information may allow for the identification of the natural person indirectly when combined with ulterior data (as, for example, an IP address from a client held by an online store combined with the Internet Service Provider client’s data).\textsuperscript{69}

\textsuperscript{64} Recital 27.

\textsuperscript{65} Under the DPD, the Art. 29 WP started from a position of considering that personal data was in principle referring to living individuals. But the Art. 29 WP admitted that in this regard the DPD left a margin of discretion to the legislation of Member States within the purpose of the data protection rules of the DPD, see Art. 29 WP 136, pp. 22 and 23.


\textsuperscript{68} Ibid, pp. 61 et seq.

\textsuperscript{69} Ibid, pp. 61 et seq.
The concept of ‘identification’ used by the GDPR is thus a referencing concept that allows for a *natural personal person to be singled out* among all admissible others. This means that identification stands on selected information that has the capacity to distinguish and individualise natural persons, be it one single piece of information (e.g., the name) or a combination of several pieces of information (e.g., address and age). This also means that only through identification does the information completely and fully relate to a natural person in the sense of personal data as defined by the GDPR.

The relevant information for the identification process is context dependent, meaning that the same identifier may be able to perform its task under certain conditions but may also be insufficient in other contexts. The most common identifier – the name – may be enough on most situations but it is not mandatory for identification. This is why Art. 4 no. 1 mentions than an identifier may work directly or indirectly depending on the identifier itself and other contextual factors. For example, in a certain group of natural persons the year of birth may be sufficient to identify one natural person when such natural person is the only one born on a different year, but in other situations where multiple individuals all share the same year of birth such information would not be a complete identifier. For instance, in a small village of only a few hundred persons publishing data referring to Covid-19 and stating only age may be sufficient to identify some of the persons.

A *directly identified natural person* according to the GDPR is a natural person regarding whom a certain piece of information allows for immediate individualisation. When referring to *indirectly identified natural persons* recourse to the combination of several pieces of information is necessary to achieve a *unique combination*. If such combination is done over time, the person is only considered to be identified when the resulting combination singles out the person. Until that moment the collected data are either non personal data or they must be considered as personal data of an identifiable individual if the data necessary to identify the person are deemed to be available though not yet processed. The distinction between indirectly identified personal data and identifiable personal data thus raises some challenges.

Information concerning an identified natural person presents a straightforward case: the information relates to an already identified person. It is thus unequivocally personal data. On the other hand, information concerning an ‘identifiable natural person’ not only presupposes that the information still needs to link to a certain natural person, but it raises the question of knowing how the identification can be done.

---

70 See recital 26.
71 For the implications of this broad understanding see Davis, ‘Facial Detection’, p. 369 et seq.
73 In this sense, CJEU C-582/14, 19.10.2016, Breyer, ECLI:EU:C:2016:779, para. 41.
74 See recital 26.
76 This is also the case when the information is gathered in the presence of a natural person (so-called handshake identification) for then all the gathered information is directly referenced to the persons for duration of their presence (although it may cease to be personal data after the person leaves the place where the information was collected if such information cannot be linked to the person by any other identifier information), see Karg, ‘Art. 4(1)’, in Simitis/Hornung/Spiecker gen. Döhmann, p. 293, mn. 55.
77 See Art. 29 WP 136, p. 13.
78 Ibid.
Identifiability is a possibility and information gathered on such possibility may only become personal data if a connection to a specific individual can be made under certain conditions. To this end, the legislator explains in Art. 4 no. 1 what must be understood as an identifiable person: "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In these cases, the information collected, if the other constituent elements apply, is known to relate to a natural person but further steps will need to refer such information to a specific person. The legislator states several identifiers, i.e., referencing criteria (name, identification number, location data, online identifier) as well as factors specific to the identity of a single person which may also be used as identifiers (physical, physiological, genetic, mental, economic, cultural or social). The GDPR explicitly accepts any referencing criteria that allow information to relate to a natural person. The identification of a natural person may be done using a combination of different sets of identifiers and, while some identifiers allow for a more immediate and direct identification, in their absence a natural person may still be identified through an adequate set of identifiers. The legal concept of personal data comprises all these possibilities of identification.

Recital 26 provides for some guidance on how to determine the limits of identifiability and thus the limits of the concept of personal data. It begins by stating that "[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used" and further determines that "[t]o ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". The most important aspect deriving from these excerpts concerning the limits of identifiability is the kind of judgment that it entails. For any given case, all the elements that can influence the identifiability of a person through the processing of information must be taken into consideration by the interpreter. This judgment turns on the means available to the entity or entities conducting processing operations, such as financial, technical and human resources, but also on the context of such operations, such as the legal framework and the resources available to third parties that might contribute to identify a natural person. The goal is to reduce risk to a minimum or to eliminate it for a given moment, using a risk management approach under a principle of reasonableness. This leads to an important discussion on the very notion of identifiability and the limits of anonymisation after the CJEU's Breyer judgement. This means that identification operates in an instant, that may or may not proceed over time: as soon as an identifier singles out or allows to single out a person, be it for a short period of time or a long one, we are in the presence of personal data and as such the GDPR applies. As Purtova has correctly argued, in Breyer, where the CJEU dealt with dynamic IP addresses (which change

---

80 See CJEU, C-101/01, 6.11.2003, Lindqvist, ECLI:EU:C:2003:596, para. 27.
82 See Art. 29 WP 136, p. 15.
83 On the framework of this risk analysis resulting from the GDPR, the Art. 29 WP and the national authorities, see Finck/Pallas, 'They who must not be identified', p. 15.
84 See, Finck/Pallas, 'They who must not be identified', pp. 34 et seq.
85 See Oostveen, 'Identifiability', p. 306.
86 See, for context on this discussion, Groos/van Veen, 'Anonymised Data and the Rule of Law', EDPLR, 4 (2020), pp. 499 et seq.; see also Urgessa, 'The Protective Capacity', p. 521 et seq.
with each Internet connection) there was, indeed, contrary to what the CJEU found, an identified individual, albeit during the duration of each specific connection. Since identification or identifiability is the connection or possible connection between information and a specific individual, avatars pose particular problems. Avatars, which are usually representations of persons on virtual environments, may give rise to data being classified as personal, when information relating to an avatar can be referred to the individual which the avatar represents. For instance, the information regarding the avatar used on an online gaming platform chat room or in the metaverse will be personal data if such information can be referred to the person represented by the avatar, singling out such person. There should be, however, caution in establishing such link as avatars can also be used by “bots”, computer programs that work automatically and interact with people. In these cases, it is evident that no personal data is involved.

Big Data, referring to the use of tools that analyse and establish connections between bulks of information, poses a great challenge to the category of “identifiable data” as it raises the question of the possibility of anonymisation and points to a scenario where all information relating to a natural person could in time become personal data.

Processed personal data may cease to be so. The Art. 29 WP has given opinion that the only way to safely determine a limit to identifiability is complete and irreversible anonymisation, which is presented as a standard for anonymisation techniques. Thus, the Art. 29 WP considers, following its own position on the concept of personal data that “[a]n effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Therefore, generally speaking, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended.”

The CJEU has considered, in Breyer, that the means available to controllers and processors should be taken into account in conjunction with the resources held by third parties. That is, even if a controller or a processor do not have the means to identify a person through data, given certain circumstances such data may still be considered personal if identification can be achieved through the intervention of a third party. The CJEU, however, draws some limits to this approach on identifiability, using two tests, namely “the identification of the data subject was [1] prohibited by law or [2] practically impossible on account of the fact that it requires a disproportionate

---

87 Purtova, ‘From knowing by name to targeting’, p. 180.
88 Ibid, p. 179.
89 Ibid; see also Papakonstantinou/de Hert, ‘Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an interim period of no regulation at all)’, computer law & security review 36 (2020), p. 9.
90 Ibid, pp. 306 et seq.
91 See Art. 29 WP 136, p. 21.
93 CJEU C-582/14, 19.10.2016, Breyer, ECLI:EU:C:2016:779, para. 44.
Index

Italic roman numbers refer to the main parts, bold numbers refer to articles, normal ones to margin numbers.

Absolute scope 90 22
Academic purposes 15 29, 19 11, 85 4, 17
Access 5 36, 86 1
- information 5 34
Access, Right of 15 1 et seq.; see also Rights of the data subject, Information
- access to information on guarantees in third countries 15 21
- administrative fines 15 31
- algorithms 15 19
- appropriate safeguards 15 21
- artificial intelligence 15 19
- automated decision-making including profiling 15 20
- available information 15 18
- blockchain 15 6
- categories of processed data 15 13
- categories of recipients 15 2, 14
- choice of data subject to request access/copy of data 15 8
- citizens of EEA Member States 15 6
- complete access (or information) 15 3, 10
- consequences of the processing 15 19 et seq.
- Convention 108 15 3, 19
- copy in an electronic format 15 24
- core of the right of access 15 8
- diagnoses 15 9, 19
- disproportionate effort 15 29
- duration of storage 15 16
- duty to give reasons 15 5
- enforced subject access 15 30, 23 27
- exemptions 15 29 et seq.
- existing rights 15 17
- explainability 15 19
- explicit request 15 23
- fees for additional copies 15 23
- future recipients 15 14
- health checks 15 9
- identifying the controller 15 6
- information about the purposes 15 12
- informational asymmetry 15 19
- inspection 15 11
- LED 15 4
- legal basis 15 2, 12
- limits to the right to copy 15 26 et seq.
- logic involved 15 19 et seq.
- Magna Carta of Data Protection 15 1
- notion of processed data 15 8
- passive transparency 15 2
- prohibition to give information in writing 12 14 et seq., 15 26
- public interest 15 29
- purpose of processing 15 12
- remote access 15 25
- right to copies of personal data 15 22 et seq.
- right to detailed explanation 15 19
- right to meaningful information about the logic involved 15 19
- right to negative information 15 7
- rights and freedoms of others 15 26 et seq.
- scope 15 7 et seq.
- scoring 15 19
- security 15 18 et seq., 25
- source of the data 15 18
- structured paper files 15 4
- whistleblowers 15 18, 28
Access to the personal data processed 29 11
Access to the premises 58 11
Accessibility of the group DPO 37 24
Accessible Information
- understandable Information 5 41
Accountability 5 63, 137, 6 18, 12 16, 15 19,
- 23 6, 24 2, 30 1, 32 35 et seq., 33 6, 14, 16
- proactive 24 6
Accountability instrument 42 1
Accountability mechanisms 24 47
Accounting firm 4(7) 36
Accreditation 43 1
Accreditation criteria 41 20
Accreditation of monitoring bodies 43 6
- consistency mechanism 64 18
- EDPB 64 18
- opinion procedure 64 18
Accreditation procedure 41 11
Accreditation requirements 41 14, 21, 43 6
Accuracy 5 61, 107 et seq., 110
- data minimisation 5 109
- exceptions 5 116
- factual data 5 111
- updated data 5 112
Accuracy, principle of 14 1, 16 1 et seq., 8,
18 8 et seq.
Action for annulment
- dispute settlement procedure 65 38 et seq.
- EDPB 65 41
- opinion procedure 64 7
- urgency procedure 66 21
Activity of the processor 4(8) 2, 9
Address book 14 3
Adequacy 5 91, 45 11
- Convention 108 45 20
- definition 45 6
- Effective judicial review 45 11
- governmental access 45 15
- independent supervisory authority 45 18 et seq.
- International commitments 45 20
- judicial review 45 16

1169

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

- legal remedies 45 16
- onward transfer 45 12
- sectoral legislation 45 13
- self-certification scheme 45 13
- surveillance measures 45 15

Adequacy decision
- competences of SA 45 5
- criteria 45 7 et seq.
- EDPB 45 21
- Existing adequacy decisions 45 29
- legal effect 45 3
- legal nature 45 3
- legal review 45 36
- monitoring 45 22 et seq.
- periodic review 45 22
- powers of supervisory authorities 45 33 et seq.
- procedure 45 21
- publication 45 28
- repeal 45 24 et seq.
- scope 45 4
- suspension 45 24

Administrative agreements 58 31

Administrative assistance 56 24

Administrative margin of appreciation
- supervisory authority, urgency procedure(s) 66 8

Advisory activities 57 11

Agency or body 4(10) 6, 4(9) 5

Aggravating or mitigating factor 42 30

Aggregate data 89 13

Alcohol consumption 4(15) 13

Algorithms 15 19

Allergies 4(15) 5

Anfechtungsklage
- dispute settlement procedure 65 41

Annual report 59 8

Anonymisation 4(1) 24 et seq., 29

Anticipation of the main case
- urgent procedure 66 10

Anticipatory design 25 26

Anti-FISA-Clause 48 3

Anti-money laundering measures 10 19, 29 12

Antragsbefugnis
- Comm 64 24
- EDPB 64 24

App counting the steps 4(15) 14

Appearance 4(13) 5

Application 40 34
- dispute settlement procedure 65 14 et seq.

Application Programming Interface 20 9

Appointment mechanism 53 5

Appointment of processors 28 8

Appointment of the member or members 54 10

Appropriate and effective measures 24 1

Appropriate data protection policies 24 44

Appropriate safeguards 58 33
- ad-hoc contractual clauses 46 58
- administrative agreements 46 59
- audits 46 13
- BCR 46 25
- certification 46 51 et seq.
- codes of conduct 46 47 et seq.
- data subject rights 46 6 et seq.
- effective remedies 46 9
- governing law 46 8
- governmental data access 46 14 et seq.
- independent supervision 46 10 et seq.
- judicial remedies 46 20 et seq.
- legal order of the third country 46 14 et seq.
- public authorities 46 23 et seq.
- purpose 46 1
- relation to adequacy decisions 46 4
- Rome I Regulation 46 8
- SA 46 11
- SA, powers of 46 17 et seq.
- standard data protection clauses 46 26 et seq.
- suspension of transfers 46 18
- termination 46 16

Appropriateness 25 34

Approval of criteria 42 23

Arbitration 48 4, 49 33

Archives 14 13, 16 14, 19 11, 20 13

Archiving purposes
- research purposes 49 8
- statistical purposes 5 82
- statistical purposes 5 82
- governmental data access 46 14 et seq.
- independent supervision 46 10 et seq.
- judicial remedies 46 20 et seq.
- legal order of the third country 46 14 et seq.
- public authorities 46 23 et seq.
- purpose 46 1
- relation to adequacy decisions 46 4
- Rome I Regulation 46 8
- SA 46 11
- SA, powers of 46 17 et seq.
- standard data protection clauses 46 26 et seq.
- suspension of transfers 46 18
- termination 46 16

Arrhythmia 4(15) 14

Art. 29 Group
- continuity of references 94 13
- opinion procedure 64 3
- Validity decisions 99 5

Artificial intelligence 6 91, 12 9, 13 10, 15 19

Artistic expression 15 29, 19 11, 85 17

Assistance provided by the processor 28 36

Assistance systems 3 52

Assistance to the controller 28 35

Associations 9 52 et seq.
- other bodies 40 19

Audit 28 54, 30 9

Authentication 4(14) 4
Index

Authorisation and advisory powers 58 1, 22
Authority 52 29
Automated decision-making 12 17, 13 10, 15 20, 22 1 et seq.
Automated individual decision-making, including profiling 22 1 et seq.
– algorithm(s) 22 2, 14, 32, 44, 47 et seq.
– automated individual decision-making 22 8, 11, 15
– contractual derogation 22 26 et seq.
– credit scoring 22 48
– decision based solely on automated processing 22 1, 3 et seq., 7, 16, 40
– explicit consent 22 4, 36 et seq., 52
– human bias 22 49
– human intervention 22 4, 14, 16 et seq., 20, 31, 34 et seq., 42 et seq., 46 et seq.
– legal effects 22 6, 9, 19, 45
– profiling 22 1, 4, 6, 8 et seq., 12, 15, 18, 22, 41, 44 et seq.
– right to explanation 22 47 et seq.
– sensitive data 22 6, 50 et seq.
– similarly significant impact 22 10, 20
– statutory authorisation 22 25, 29 et seq.
– suitable measures 22 4, 26, 29 et seq., 42 et seq., 52
Automated means 21 20
Automated tools 4(11) 41
Autonomous vehicles 9 9
Awareness raising 57 13
Background checks 10 19
Balance between data protection and freedom of expression and information 85 8, 18 et seq.
Balancing 69 18, 10, 21, 23, 90 20
– and accountability 6 71
– between data protection and freedom of information 86 3
– exercise 21 13
Balancing of interests 6 53
– search engines 6 56
Bank 4(7) 35
Banking secrets 9 4
Barristers 4(7) 41
BCR 47 7 et seq.
– approval 47 7 et seq.
– binding effect 47 13
– changes to 47 31
– complaint procedure 47 29
– compliance 47 28, 30
– cooperation with SA 47 32
– data protection principles 47 22 et seq.
– data subject rights 47 15 et seq., 24 et seq.
– implementing act 47 35
– intra-group-agreement 47 13
– judicial review 47 11
– liability 47 26
– material scope 47 20
– modifications 47 31
– national law of third countries 47 33
– onward transfer 47 5
– rationale 47 1 et seq.
– scope 47 4 et seq.
– substantive requirements 47 18 et seq.
– surveillance measures 47 35
– third-parties beneficiaries rights 47 15 et seq.
– training 47 34
– transparency 47 27
Beacon technology 12 14, 27
Begin of application of the GDPR 47 15
– Broad reference 94 10
– continuity legal basis 94 5 et seq.
– continuity of authority decisions 94 8
– continuity of Comm decisions 94 8
– continuity of consents 94 6
– Effects on national legislation 94 7
– individual reference 94 11
– reference to Art. 29 WP 94 13
– references in contracts 94 12 et seq.
– references to the DPD 94 9 et seq.
Behavioural advertising 6(1)(f) 3, 37 21
Behavioural traits 4(14) 8
Big data 5 88, 6(1)(f) 4, 6 38, 91, 37 17
– profiles 5 125
Binding and enforceable commitment 40 35
Binding Corporate Rules 58 32
– consistency mechanism 64 22
– opinion procedure 64 22
Binding nature 5 4
Binding power 40 46 et seq., 62
Biological sample 4(15) 4, 4(13) 6
Biometric data 4(14) 1 et seq., 9 6, 29 et seq., 84
– authentication 4(14) 4, 7, 11
– behavioural traits 4(14) 8
– biometric features 4(14) 4
– biometric information 4(14) 3
– biometric samples 4(14) 5
– biometric system 4(14) 5, 10
– body odour 4(14) 8
– dactyloscopic data 4(14) 2, 8
– ear shape 4(14) 8
– facial images 4(14) 2, 8
– finger images 4(14) 8
– fingerprints 4(14) 5, 8
– gait characteristics 4(14) 8
– genetic data 4(14) 1
– hand geometry 4(14) 8
– health data 4(14) 1
– iris (images of) 4(14) 8
– palm print 4(14) 8
– physical, physiological or behavioural characteristics 4(14) 2, 8 et seq.
– retina (images of) 4(14) 8
– signature 4(14) 8

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

1171

https://www.nomos-shop.de/isbn/978-3-8487-3372-9
Index

- special categories of personal data 414 1 et seq., 4, 11
- specific technical processing 414 2, 4 et seq.
- sweat pore patterns 414 8
- tattoos 414 9
- templates 414 5 et seq., 8, 10
- typing 414 8
- unique identification 414 2, 4, 7, 9, 11
- vein patterns 414 8
- verification 414 10 et seq.
- voice samples 414 8
- way of walking or moving 414 8
- Biometric features 414 5

Blind data subject 12 10
Blockchain technology 15 6, 16 13
Blocking 18 3 et seq.
Blocking period - dispute settlement procedure 65 31
Blogger 85 13
Blood and urine analysis 415 7
Bluetooth 12 14
Body odour 414 8
Breach notification see Personal data breach
Browser fingerprinting
- Territorial scope 3 51 et seq.
Brussels Effect 44 8
Burden of proof 5 145, 6 18, 21 5
Call center 418 9
- operators 417 37
Cameras 417 40
Canada
- transfers to 45 4
Capacity 411 3
Catch-all clause 57 16
Certification 23 6, 56, 42 1 et seq., 43 1 et seq.
- accountability 42 1
- accreditation 42 7, 23, 43 1 et seq., 4 et seq., 14 et seq.
- aggravating or mitigating factor 42 30
- certification body 42 13, 20 et seq., 43 1 et seq.
- certification criteria 42 11, 16 et seq., 20, 23 et seq., 29, 43 8, 14, 16 et seq.
- certification marks 42 7
- certification mechanism 42 1 et seq., 5, 7 et seq., 12 et seq., 15, 19 et seq., 22, 28 et seq., 43 3, 14, 16 et seq.
- common certification 42 23
- compliance 42 1, 3 et seq., 12, 15, 17 et seq., 23, 30, 43 4, 11
- conformity assessment 42 7, 43 4, 6, 9, 15, 17
- consistency mechanism 64 18
- data protection mark 42 3, 7
- data protection seals 42 2, 5, 43 17
- data subject rights 42 14
- data transfers 42 14, 30
- delegated and implementing acts 43 1, 16
- dual purpose 42 16
- European Data Protection Seal 42 3, 23, 29, 43 12
- impartiality 43 9
- national accreditation body 43 2, 4, 6, 15
- presumption of conformity 42 18, 30
- processing operations 42 2, 4, 6, 10 et seq., 17, 27
- purpose of certification 42 4, 17
- register 42 29, 43 14
- reliable evidence 42 1
- self-regulatory measures 42 30
- separation of powers 42 26 et seq.
- small and medium sized enterprises 42 4
- standards 42 2, 7, 20, 24, 43 3 et seq., 17
Certification bodies 43 1, 58 27
- consistency mechanism 64 18
- EDPR 64 18
- opinion procedure 64 18
Certification criteria 42 20
Certification mark 42 7
Certification mechanism 24 47
Change of purpose 13 13, 14 9
Children 6(1)(f) 42, 40 29
- interest 6 74
- Representatives of controllers and processors from third countries 27 16 et seq.
- special needs 12 12
Chilling effect 23 9, 85 18
Choice of law
- Territorial scope 3 62
Churches and religious associations 91 1 et seq.
- administrative enforcement 91 19
- administrative fine 91 19
- Catholic Church 91 5 et seq., 18, 20
- Federal Republic of Germany 91 5
- grandfather clause 91 1, 13, 16
- independent SA 91 1, 12, 17
- Italy 91 6
- notification duty 91 15
- philosophical and non-confessional organisations 91 8
- Poland 91 6, 18, 20
- Religion 91 7
- subsidiary competence 91 20
Churches, religious associations and communities
- application of existing law 99 3
Civil law claims, enforcement of 23 30
Claim of inaccuracy 18 8 et seq.
Clear affirmative action 411 52
Clinical treatment 415 4
CLOUD Act 48 2, 6
Cloud computing 49 23
- Market place principle 3 46
- Territorial scope 3 38, 46

1172

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

Cloud service 4, 6, 8
Cloud service provider 4(7) 37, 4(8) 9, 28 64
Codes of conduct 24 47, 40 1 et seq., 41 1 et seq.
   – accreditation criteria 41 20, 26 et seq.
   – accreditation procedure 41 2, 11
   – accreditation requirements 41 14, 21, 27
   – administrative discretion 41 12 et seq., 27
   – application (form of) 40 34
   – appropriate safeguards 46 47 et seq.
   – approved certification mechanisms 28 72
   – associations (and other bodies) 40 1 et seq., 11, 13, 19 et seq., 36, 38
   – binding and enforceable commitment 40 32, 34 et seq.
   – binding power 40 46 et seq., 61 et seq.
   – data protection impact assessment 5 143
   – certification 5 143
   – children 40 29
   – collection of personal data 40 25
   – compliance; guarantees; safeguards 40 9
   – conciliation 40 12, 23, 29
   – conflict of interest 41 18
   – consistency mechanism 64 15 et seq.
   – consultation 40 17, 21, 45, 55
   – corrective powers 41 22 et seq., 25
   – data breach 40 31
   – Data Protection Board 40 10, 49, 52
   – dispute resolution 40 33, 53
   – drafts 40 20, 39 et seq.
   – EDPB 64 15 et seq.
   – encouragement 40 10 et seq., 17
   – enforcement; execution 41 24
   – established procedures (complaints) 41 17
   – established procedures (eligibility) 41 16 et seq.
   – evaluation; opinion; approval 40 38
   – fair and transparent processing 40 23
   – fragmentation 40 60
   – general validity 64 16
   – implementing act; Commission 40 13, 54 et seq.
   – incentives 40 7, 16 et seq., 59
   – independence 41 15
   – information 40 27, 29
   – infringement; execution; enforcement 41 22
   – International data flows 46 47 et seq.
   – legal certainty 40 16, 18, 26, 28, 61
   – legitimate interests 40 24
   – monitoring bodies 40 10, 36 et seq., 56, 41 1 et seq., 26
   – monitoring mechanisms 40 37
   – monitoring responsibility 41 2
   – opinion procedure 64 15 et seq.
   – precision 40 18
   – privacy by design and by default 40 30
   – pseudonymisation; anonymisation 40 26
   – public bodies 41 3
   – register; publication 40 51
   – regulated self-regulation 64 17
   – revocation 41 19
   – rights of data subjects 40 28
– risk neutrality 40 14
– safeguards 40 9, 32, 34, 41, 52, 54, 41 23
– security 40 9, 30 et seq.
– self-monitoring 41 1, 26
– self-regulation 40 1, 3 et seq., 12, 61
– Small and Medium-Sized Enterprises 40 15, 40, 61
– stakeholders 40 21, 45, 61
– Supervisory Authority (or SA) 40 1, 3, 6 et seq., 9 et seq., 16 et seq., 20, 31, 38 et seq., 48 et seq., 56, 62, 41 1 et seq., 6 et seq., 11 et seq., 18 et seq., 24 et seq.
– third countries 40 32, 34
– third country transfer 46 47 et seq.
– time limit 41 2
Collection of personal data 13 4 et seq., 40 25
Collective agreements
   – covering works agreements 88 26 et seq.
Common decision 26 30
Common Foreign and Security Policy
Intro 126
Company providing general IT support 4(8) 9
Compatibility 5 64, 75, 77, 20 8
   – factors 6 90
Competence
   – and the judiciary 55 13
   – for public tasks 55 9
   – legal bases 6 79
   – negative conflict 26 3, 45
Competent authority
   – opinion procedure 64 4
Competent national bodies 90 16
Competent supervisory authorities 66 17
   – dispute settlement procedure 65 31
   – lead supervisory authority 65 13a et seq.
   – urgency procedure 66 1 et seq.
Competition 20 1
Complaint-handling mechanism 24 32
Complement, right to 16 4, 13
Complete independence 52 1 et seq.
Compliance 5 141, 144, 32 39 et seq., 39 11, 42 17, 90 18
   – guarantees 40 9
   – legal obligation 6 41
   – safeguards 40 9
Compliance activities 30 2
Compliance efforts
   – documentation 24 32
Compliance evidence 24 3
Compliance measures 49 28
Compliance-officer 38 26
Comprehensibility 12 9, 23 32
Comprehensive register of criminal convictions 10 21
Compromises 5 32, 43 et seq., 84, 104, 106, 117, 129, 136, 146
   – anonymisation 5 131

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Conditions applicable to child's consent in relation to information society services 81 et seq.

Access to information 813

Advertising 87, 20

Age limit 8, 3, 10, 17

Available technology 822 et seq.

Best interest (of child) 830, 16, 24

Consent by a child 811 et seq.

Contract law 827

Directly to a child 812, 21

Duty to consult 816

Enforcement 828

Freedom of expression 810, 13, 17

Holder of parental responsibility 84, 15, 24

Information society services 8, 1, 3, 8 et seq., 15, 17, 19 et seq., 24, 26 et seq.

Meaning and consequences (of consent) 82

Parental consent 88, 12 et seq., 16 et seq., 23 et seq.

Preventative and counselling (services) 818

Reasonable efforts to verify 823

Remuneration 820

Special categories of data 83

Third parties 825 et seq.

UN Convention of the Rights of the Child 88, 16 et seq.

Validity, formation or effect of a contract 827

Verification requirements 823 et seq.

Vulnerability 817

Confidential information 9015

Confidentiality 2829, 299, 904

Duty of 1418, 3310

Or professional secrecy 3819

Conflicts of interest 3823, 4118, 5218, 903

Conformity assessment 434

Connected vehicles 109

Consensus principle

Dispute settlement procedure 6514 et seq.

Consent 4(11) 1 et seq., 619 et seq., 30, 71 et seq., 1821, 207

Affirmative act 4(11) 15, 52, 54 et seq., 58, 61, 71, 23

As a direct statement 941

Automated tools 4(11) 41 et seq., 721

Autonomy 4(11) 6, 8 et seq., 15, 42, 44

Bundling 741 et seq., 49

Burden of proof 76, 10, 16, 49

Capacity (to consent) 4(11) 3

Clear affirmative action 4(11) 52 et seq., 71, 23

Clear and plain language 4(11) 50, 728

Conditions for consent 4(11) 62, 71 et seq.

Consent information 4(11) 38, 49 et seq., 722, 24, 28 et seq.

Continuity previous 946

Counter-performance 4(11) 10, 73, 45

Demonstrate consent (duty to) 712 et seq.

Detriment 4(11) 24, 31, 38, 735

Explicit 4(11) 1, 17 et seq., 34, 721, 499

Formal requirements 4(11) 50 et seq., 71, 22 et seq.

Freely given 4(11) 2, 15, 21 et seq., 37, 74 et seq., 10, 34 et seq., 44 et seq., 47 et seq., 4913

Genuine choice 748

Granular 4(11) 29, 37, 42

Imbalance of power 4(11) 15, 24, 28, 73, 9, 43, 46

Implied 4(11) 17 et seq.

Informed 4(11) 2, 9, 15, 18, 30, 38 et seq., 43 et seq., 714, 24 et seq., 29, 42, 4911 et seq.

Intelligible and easily accessible form 4(11) 50, 729

International data flows 498 et seq.

Layering 4(11) 47

Limits 4914

Limits on consent 4(11) 9, 12

Multiple controllers 4(11) 39, 49, 719 et seq.

Pre-formulated declaration 4910

Proxy consent 4(11) 41 et seq., 51, 721

Public interest 4(11) 11

Scientific research 4(11) 35

Situations of subordination 4(11) 26

Specific 4(11) 15, 30, 33 et seq., 57, 724 et seq., 40

Standard business terms 4910

Statement 4(11) 15, 41, 51 et seq., 55, 60 et seq., 71, 21, 23

Third country transfer 498 et seq.

Timing of consent 4(11) 4 et seq., 18

Unambiguous 4(11) 2, 17, 20, 32 et seq., 724, 26

Withdraw consent 4(11) 2, 31, 45, 72, 33 et seq.

Written declaration 4(11) 50, 56, 74, 6, 8, 22

Considered as a controller 2882

Consistency mechanism

Accreditation 6418

Binding Corporate Rules 6422

Certification 6418

Codes of conduct 6415 et seq.

Contractual clauses 6420 et seq.

Data protection seal. EU 6418

Dissent supervisory authorities 4(24) 1 et seq.

Draft decision 657

Information exchange, electronic 6446

Internal provisions 6422

Legal protection 6442

Majority principle 6439

Matters of general application 6425 et seq.
Index

- objection 4(24) 1 et seq.
- one-agency-one-vote 64 39
- standard contractual clauses 64 19
Consular posts
- Territorial scope 3 58
Contact for data subjects 38 18
Content personalisation 6(1)(f) 1 et seq.
- advertisement 6(1)(f) 6
- application-specific concerns 6(1)(f) 27 et seq.
- authorisation by Union or Member State law 6(1)(f) 25, 28
- automated decisions 6(1)(f) 13 et seq., 25, 34, 37
- automated processing 6(1)(f) 25
- business models 6(1)(f) 6 et seq.
- collaborative filtering 6(1)(f) 7, 12, 17 et seq., 22
- compatibility with the original purpose 6(1)(f) 28
- consent 6(1)(f) 16 et seq., 25 et seq., 35
- content personalisation in online platforms 6(1)(f) 32 et seq.
- content-based filtering 6(1)(f) 7
- controllers 6(1)(f) 2, 9, 19 et seq., 34, 36 et seq.
- dark patterns 6(1)(f) 10
- data subject rights 6(1)(f) 34 et seq.
- freedom of speech, thought, and the press 6(1)(f) 19
- human intervention 6(1)(f) 37
- journalistic purposes 6(1)(f) 30, 36
- lawfulness of processing 6(1)(f) 15 et seq.
- least infringing means 6(1)(f) 23 et seq.
- legal or similarly significant effects 6(1)(f) 25
- legitimate interest as grounds for content personalisation 6(1)(f) 21 et seq.
- location data 6(1)(f) 33, 35
- manipulation 6(1)(f) 1, 16, 25
- marketing 6(1)(f) 6, 27, 33
- necessary for performance of a task in the public interest or in the exercise of official authority vested in the controller 6(1)(f) 20
- necessary for protecting the vital interests of a natural person 6(1)(f) 20
- personalisation and contract 6(1)(f) 17 et seq.
- political propaganda 6(1)(f) 4
- preferences (of user) 6(1)(f) 1, 5 et seq., 15 et seq., 18, 26 et seq.
- profiling 6(1)(f) 8, 14, 18, 25 et seq.
- proportionality 6(1)(f) 24, 28
- recommender systems 6(1)(f) 7, 10, 15, 34
- special categories of personal data 6(1)(f) 29
- tailoring 6(1)(f) 1, 15, 22
- third-party 6(1)(f) 8, 34
- tracking online behaviour 6(1)(f) 6, 26
- traffic data 6(1)(f) 33, 35
- transparency 6(1)(f) 16, 34 et seq.
- value-added service 6(1)(f) 33
Continued responsibility 26 57
Continuity legal basis 94 5 et seq.
- grandfathering 94 5 et seq.
Contract 6 33
- necessity 6 37
- or other legal act 28 21
Contractual arrangements 24 32
Contractual clauses 58 30
- opinion procedure 64 20 et seq.
- transfer third country 64 20 et seq.
Control 4(7) 10
- of official authority 10 22
Controller 4(7) 1 et seq., 14, 28 et seq., 4(10) 7, 28 1, 45 20
- access (to the data) 4(7) 1, 14, 24, 31, 38
- accountability 4(7) 1, 25
- accounting firm 4(7) 36
- alone or jointly 4(7) 9 et seq.
- bank 4(7) 35
- barristers 4(7) 41
- call center operators 4(7) 37
- cameras 4(7) 40
- cloud storage providers 4(7) 37
- control 4(7) 1, 10, 22, 26, 28, 33 et seq.
- controller with regard to his/her own personal data 4(7) 6
- delegating decisions on non-essential means 4(7) 21
- email service providers 4(7) 37
- employer-employee 4(7) 7, 17, 32, 35
- essential and non-essential means 4(7) 19 et seq.
- expertise of the parties 4(7) 41
- factual influence 4(7) 10 et seq.
- group of individuals 4(7) 5
- hosting service provider 4(7) 37
- imbalance of knowledge and negotiating power 4(7) 13
- joint controllership 4(7) 1 et seq., 5, 9, 28, 31
- law firms 4(7) 34
- mail marketing 4(7) 39
- market research agency 4(7) 38
- municipal authorities 4(7) 33
- natural or legal person, public authority, agency or other body 4(7) 3 et seq.
- pivotal role 24 13
- processor 4(7) 1, 4, 6 et seq., 11 et seq., 17, 19 et seq., 27, 32, 35, 37, 39 et seq.
- processorship (factors indicating) 4(7) 32
- purpose and means 4(7) 14, 22
- responsibility 24 1, 11
- security company 4(7) 40
- single processing operation or to a set of operations 4(7) 22
- standard contractual clauses 4(7) 13
- status of accountants 4(7) 41
- SWIFT 4(7) 42
Index

- Territorial scope in case of natural persons 3, 19
- traditional role 4(7) 32, 41
- Union or Member State law 4(7) 26
Controller-concept
- function 24, 13
Controller-processor relationship 28, 2
Controlling undertaking 88, 35 et seq.
Convention 108
- Territorial scope 3, 8
Converging decisions 26, 25, 33
Cookies 6(1)(f) 32, 97, 14
- Territorial scope 3, 51 et seq.
Cooperation (of controller and processor) with the SA 31 et seq.
- access to all personal data 31, 4
- administrative act 31, 6
- automatic processing operation 31, 10
- business premises 31, 4, 11
- common cooperation obligation 31, 1
- controller 31, 1, 3 et seq., 6, 9 et seq.
- cooperation between the SAs 31, 10
- cooperation obligation 31, 1, 4 et seq., 10
- cooperative behavior 31, 3
- corrective powers 31, 3
- fines 31, 7
- implied powers 31, 8
- investigative powers 31, 3
- kind of data processing 31, 10
- legal remedy 31, 6
- nemo tenetur se ipsum accusare 31, 12
- processor 31, 1, 3 et seq., 6, 9 et seq.
- proposal of the Comm 31, 11
- records of the processing activity 31, 4
- reporting obligation 31, 4
- representative(s) 31, 1, 10
- special cooperation obligation 31, 4 et seq.
- supervisory authority (or SA) 31, 1 et seq.
- tasks of the SA 31, 1 et seq., 11
- unilateral obligation to notify the SA 31, 10
Cooperation credits 31, 1, 49, 28
- consistency mechanism 64, 22
- dispute settlement procedure 65, 14 et seq.
- opinion procedure 64, 22
Correction, right to 16, 4 et seq.; see also rights of the data subject
Corrective powers 41, 25 et seq., 58, 1, 12
Council of Europe Convention 108 15, 3, 23, 3
- 85, 2, 24
Counter-performance 4(11) 10
Covert data collection 14, 1
COVID-19 outbreak 9, 80
Credit institutions and investment firms 90, 6
Credit scoring 6(1)(f) 1 et seq., 37, 21
- AI Regulation 6(1)(f) 6
- automated decision making 6(1)(f) 2, 7, 10 et seq., 18, 20
- automatic refusal 6(1)(f) 9
- behavioural data 6(1)(f) 4 et seq., 16
- Consumer Credit Directive 6(1)(f) 2
- creditworthiness 6(1)(f) 1 et seq., 4, 6 et seq., 15 et seq., 20
- FinTech 6(1)(f) 5
- harmonisation 6(1)(f) 20
- legal bases 6(1)(f) 13 et seq.
- Mortgage Credit Directive 6(1)(f) 2
- Profiling 6(1)(f) 9 et seq., 17, 20
Creditworthiness 13, 10; see also Scoring
Criminal convictions 10, 2 et seq.
Criminal records 10, 7
Cross-border data processing 55, 1
- consistency mechanism 64, 5, 30
- dispute settlement procedure 65, 15
- opinion procedure 64, 5
Cross-border health care 15, 9, 20, 1
Cross-border processing 4(23) 1 et seq., 4, 55, 12, 56, 1
- affects or is likely to substantially affect 4(23) 1, 6
- effective exercise of activities 4(23) 4
- establishment in one Member State with a substantial impact on data subjects in more than one Member State 4(23) 6 et seq.
- establishments in more than one Member State 4(23) 3 et seq.
- lead supervisory authority 4(23) 1 et seq.
- main establishment 4(23) 9
- one-stop-shop 4(23) 1
- single establishment 4(23) 1, 6 et seq., 9
- stability of the arrangements 4(23) 4
Cross-border situations relating to freedom of expression and information 85, 26
Cyber-resilience approach 32, 32
Dactyloscopic data 4(14) 8
Data
- administrative sanctions 10, 5
- biometric data 4(14) 1, 9, 29
- concerning health 9, 9
- criminal records 10, 7
- criminal sanctions 10, 5
- Finger images 4(14) 8
- Fingerprints 4(14) 9
- generated by autonomous vehicles 9, 9
- generated by connected vehicles 10, 9
- hair color 4(13) 5
- political opinions, religious or philosophical beliefs 9, 21
- public 9, 56
- racial or ethnic origin 9, 18
- relating to income 9, 4
- relating to wealth 9, 4
- sex life and orientation 9, 38
- way of walking 4(14) 8
Data access 4(7) 14
Data breach 40, 31; see personal data breach
- reporting and handling procedures 24, 32
Index

Data concerning health 4(15) 1 et seq.
- alcohol consumption, tobacco consumption or drug use 4(15) 13
- allergies 4(15) 5
- analysing a person’s urine and blood 4(15) 7
- app counting the steps 4(15) 14
- arrhythmia 4(15) 14
- biological samples 4(15) 4
- diabetics 4(15) 14
- diet app 4(15) 14
- disease, disability, disease risk, medical history, clinical treatment 4(15) 4 et seq., 13
- exercise habits or diet 4(15) 13
- genetic data 4(15) 1, 4
- glucose metering 4(15) 7
- health care services 4(15) 4, 10 et seq.
- height professional 4(15) 4, 10
- health status 4(15) 2, 4 et seq., 8, 11 et seq., 16
- heart rate monitor 4(15) 14
- hereditary or genetic predisposition 4(15) 13
- high or low blood pressure 4(15) 13
- hospital 4(15) 4
- IQ 4(15) 5
- measuring blood pressure or heart rate 4(15) 7
- medical data 4(15) 5, 8
- medical device 4(15) 4 et seq., 7, 10
- obesity 4(15) 13 et seq.
- patient support group 4(15) 5
- physical or mental health 4(15) 2, 4 et seq., 11 et seq.
- physician 4(15) 4
- pulse/heart rate 4(15) 14
- screening tests 4(15) 6
- self-help and support groups 4(15) 5
- sleep diary 4(15) 14
- smoking and drinking habits 4(15) 5
- testing or examination of a body part or bodily substance 4(15) 4
- wearing glasses or contact lenses 4(15) 5
- weight 4(15) 5, 14

Data governance 30 1
Data minimisation 5 60, 89 et seq., 97 et seq., 11 1, 19, 25 43
- big data 5 99
- consistency mechanism 64 44
- data subjects 5 102
- personal data 5 96
- processing 5 100 et seq.

Data protection 12 17, 15 15, 23 31
Data processing 37 8
- concerning health 9 34 et seq.
- protection of vital interests of the data subject 9 48
- purposes set out by employment, social security and social protection law 9 47
- statistical purposes 9 81
- statutory duties 88 15

Data processing agreements 28 20
Data processing legitimate 9 11
Data protection adaptation laws 94 4
Data protection audits 58 7
Data protection board
- commission 40 54
- implementing act 40 54
- opinion 40 52 et seq.
Data protection by default 25 1, 40
Data protection by design 12 17, 25 1 et seq.
- principles 25 12
Data protection by design and by default 5 37, 103, 25 1 et seq., 19, 89 15
- accountability (principle of) 25 12, 31 et seq., 56
- accuracy (principle of) 25 12, 31
- anonymization 25 2, 10
- anticipatory design 25 26
- Artificial Intelligence 25 19
- automated decision-making 25 5, 19, 30, 32 et seq., 39
- Big Data 25 35
- certification 25 6, 13, 19, 57 et seq.
- codes of conduct 25 19
- cost of implementation 25 16, 34
- dark patterns 25 53
- data minimisation (principle of) 25 8, 12, 27, 31 et seq., 42 et seq., 53
- data protection principles 25 31 et seq.
- DPRA 25 5, 11, 16, 19 et seq., 32, 37, 60 et seq.
- GDPR 25 5, 13, 32, 57
- enforcement 25 59 et seq.
- fairness (principle of) 25 12, 31 et seq.
- information system(s) 25 2, 15, 18, 20
- integrity and confidentiality (principle of) 25 12, 31, 43
- Internet of Things 25 11
- interoperability 25 9
- lawfulness (principle of) 25 12, 31
- legal basis 25 53 et seq., 63
- penalties 25 59 et seq.
- preventing measures 25 7, 12 et seq., 30 et seq., 39, 57
- privacy by design 25 2, 7, 9 et seq., 32, 34, 63
- privacy-enhancing technologies 25 10
- proactive risk-prevention approach 25 2
- proportionality 25 17, 32
- pseudonymisation 25 2, 10, 27 et seq., 33
- purpose limitation (principle of) 25 12, 31, 42, 51, 53
- risk-based approach 25 16, 37
- role of controllers 25 22
- safeguards 25 1, 5, 11 et seq., 14, 18, 23 et seq., 30 et seq., 33, 35 et seq., 56 et seq., 60 et seq.
- sanctions 25 59
- scope 25 17
- sensitive data 25 35
- state of the art 25 3, 16 et seq., 19, 24, 34, 36, 38, 58

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

- storage limitation (principle of) 25 12, 27, 31, 42 et seq.
- technical and organizational measures 25 1, 3, 5, 7, 9, 13 et seq., 18, 20, 24, 28, 31, 33, 37, 56, 60, 62
- training 25 2
- transparency (principle of) 25 12, 31 et seq., 53

Data protection certification mechanisms 42 2

Data protection officer 37 27, 38 16

Data protection directive 5 5

Data protection impact assessment 23 37, 35 1 et seq.
- advertising 35 20, 23
- authentication 35 58
- automated processing 35 22 et seq.
- black list 35 29, 31
- Bluetooth 35 28
- bring-your-own-device 35 17
- camera 35 27, 31
- CCTV 35 28, 31
- child 35 6, 18, 54
- codes of conduct 35 47
- consistency mechanism 64 13 et seq.
- consistency procedure 35 30
- criminal convictions 35 18, 24
- DPO 35 41 et seq., 46
- e-commerce 35 19
- EDDB 64 13
- employee 35 6, 18, 31
- encryption 35 58
- fundamental rights 35 4 et seq., 53
- health data 35 31, 54
- high risk to the rights and freedoms 35 2, 10, 12, 19
- historical data 35 31
- in-house organisation 35 40
- joint controller 35 31
- large scope of data processing 35 19
- legal basis 35 33
- likelihood of damage 35 13
- location data 35 6
- microphone 35 28
- monitoring 35 23, 26 et seq., 30 et seq.
- negative list 35 11, 29 et seq., 32, 64 14
- occurrence of harm 35 14
- opening clause 35 34
- opinion procedure 64 13 et seq.
- patient records 35 24
- positive list 35 29, 64 14
- preliminary assessment 35 10
- pricing 35 23
- principles of personal data processing 35 56
- processing operations 35 2, 9 et seq., 12, 15, 31, 33, 51
- process-oriented inventory 35 50
- profiling 35 6, 20, 22 et seq.
- public interest 35 35
- purpose of the data processing 35 20
- review 35 13, 39, 46
- RFID 35 5, 58
- risk minimisation 35 4
- risk-based approach 35 1
- SaaS 35 17
- scoring 35 23
- security service 35 24
- sensitivity 35 15, 18, 24
- severity 35 14, 52
- smart meter 35 5, 23
- special categories of personal data 35 6, 18, 24
- surveillance 35 6, 25, 27 et seq., 54
- systematic and extensive 35 23
- technical and organisational measures 35 57
- third countries 35 19
- tracking 35 23, 28
- white list 35 29, 32
- works council 35 44

Data protection law
- responsibilities 26 5

Data protection management 5 78, 139, 19 5, 24 44

Data Protection Officer (DPO) 24 31, 37 1 et seq., 39 1 et seq., 39 1 et seq.
- abstract assessment 39 13
- access to any IT application processing personal data 38 8
- accessibility from branch office 37 28
- activities of companies that are generated by default 37 11
- additional qualifications 37 37
- additional specialists 39 8
- adverse consequences 38 13
- advising the DPO 39 24
- advisory or control obligations 37 42
- ancillary activities 37 11
- appointment of DPO 37 1 et seq., 12, 29
- association(s) 37 31
- attorneys 38 27, 39 8
- auditing 37 42, 38 19, 39 1
- auxiliary arm 39 22
- awareness-raising and training of employees 39 16
- basic rules on the appointment of DPOs 37 1
- basic task 39 1, 4
- big and smart data applications 37 17
- business goals 37 10, 12
- business secrets 38 8
- check policies and procedures (duty to) 39 14
- communicate audit findings (duty to) 39 20
- compliance 37 2, 8, 15, 40, 38 15 et seq., 25 et seq., 39 1, 3, 8, 11, 14 et seq., 19 et seq., 27 et seq.
- compliance department 38 26
- Compliance Officer 38 26
- comprehensive, regular, and systematic monitoring 37 20
- confident in the assessment of risks 39 27
- confidentiality 37 42, 38 8, 19 et seq.
- confidentiality obligations 37 42, 38 8

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index
Index

– resign 37 43
– responsibility 39 3
– responsibility of DPO 39 1, 3, 20, 28
– risk-based approach 37 6, 39 9
– risk-oriented approach 37 14, 38 11, 39 25 et seq.
– risk-oriented assessment of the data processing activities of a controller or processor 37 15
– sensitive data 37 15
– separate appointment 37 23
– serious deficiencies 39 20
– serious infringement 39 23
– service contract 37 38
– skills, knowledge and qualification 39 27
– smaller authorities or institutions 37 29
– spatial distribution or sensitivity of data 37 20
– special categories of personal data 37 22
– special knowledge 37 36
– sufficient and adequate technology, literature, travel expenses and premises 38 6
– support 38 5
– support of DPO 38 5 et seq.
– supported by a team 38 7
– target-oriented planned procedure 37 21
– tasks of DPO 37 29 et seq., 33, 35 et seq., 40, 45, 38 1 et seq., 5, 7 et seq., 10, 13, 18, 23 et seq., 26, 39 1 et seq.
– technical developments 39 5
– time necessary to fulfil the tasks 38 5
– time of designation 37 33, 36
– transfer of additional tasks 39 3
– translation service 37 26
– unannounced check(s) 39 12
– valued asset within the company 39 27
– website 37 44
– with a sense of proportion 39 25
– without much effort (contact) 37 24
Data protection policies 24 32
Data protection right
– legal bases 6 8
Data protection risks 25 37
Data protection seals 42 5
Data protection training/education 24 32
Data quality 16 8
Data retention
– profiling 5 86
Data Retention Directive Intro 132
Data security 85 2, 24
Data subject 4(10) 7, 12 et seq., 37 20; see also Rights of the data subject
– liability 24 5
– standard contractual clauses (SCC) 46 36
Data subjects in third countries
– Territorial scope 3 15
Data transfers 42 13
Data-first approach
– access 32 30
– availability 32 30
Datasets
– ad hoc sharing 26 41
Date of application 99 1
Deadline
– opinion procedure 64 36 et seq., 45
Decision
– dispute settlement procedure 65 19, 34 et seq.
– opinion procedure 64 12
– supervisory authority, lead 65 35 et seq.
Defaults and dark patterns 25 53
Defaults and data subject choices 25 52
Defence 23 19
De-identification 11 4
– measures 11 16
Delegating decisions on non-essential means 4(7) 21
Deletion of the data by the processor 28 46
Deletion, right to 16 4, 20 3
Demonstrable accountability 24 8
Demonstrating compliance 11 14, 24 1
Departments within a company 40(8) 6
Derogation 9 11, 21 23, 89 1 et seq.
Derogations from the standards of the GDPR
– power to adopt provisions 88 22
– standard of protection 88 23
Design objectives 5 12
Designate a DPO 37 4
Detriment 4(11) 31
Device fingerprinting 13 4
Diabetics 4(15) 14
Diagnosis 15 9, 16 6
Diet app 4(15) 14
Digital content 20 1
Digital estates 15 6
Diplomatic missions
– Territorial scope 3 58 et seq.
Direct authority 4(10) 7
Direct identifier 87 6
Direct influence 52 15
Direct marketing 6(1) 9, 35, 21 2
Disability 4(15) 4
Disclosure 4(9) 6
– to a third party 4(10) 4
Discretion
– opinion procedure 64 12
– urgency procedure 66 16 et seq.
Discrimination 10 1
Disease 4(15) 4
Disease risk 4(15) 4
Disproportionate effort 11 3, 15 29, 19 8
Dispute Resolution  40 33  
Dispute settlement procedure  65 1 et seq. 
  – action for annulment  65 38 et seq.  
  – application  65 14 et seq., 18  
  – binding nature  65 30  
  – blocking period  65 31  
  – consensus principle  65 14 et seq.  
  – content  65 8  
  – cooperation principle  65 14 et seq.  
  – data processing, cross-border  65 15  
  – deadline  64 60, 65 21 et seq.  
  – decision  65 4a, 8, 19, 25, 34 et seq.  
  – duty to inform  65 32 et seq.  
  – EDPB  65 4a, 11 et seq.  
  – EDSA  65 17 et seq.  
  – form  64 61  
  – format  65 33  
  – hearing, legal  65 24  
  – history  65 3  
  – infringement proceeding  65 43  
  – legal consequence  65 9a et seq., 26, 30  
  – legal protection  65 38 et seq.  
  – main establishment  65 15  
  – majority principle  65 20, 23, 27 et seq.  
  – Novelty  65 1  
  – objection, relevant and reasoned  65 7  
  – obligation to state reasons  65 24, 30  
  – one-agency-one-vote  65 23  
  – One-Stop Shop procedure  65 13a et seq.  
  – opinion procedure  65 17 et seq.  
  – precondition  65 2a, 4a et seq., 14 et seq., 21 et seq.  
  – preliminary ruling procedure  65 42  
  – procedure  64 61, 65 16  
  – proceeding(s)  65 20 et seq., 35 et seq.  
  – purpose  65 1  
  – relation to opinion procedures  64 59 et seq.  
  – supervisory authority, concerned  65 13a et seq., 16, 26  
  – supervisory authority, lead  65 6, 11, 13a et seq., 26  
  – systematic  65 2a  
  – the public  65 25, 34  
  – time limit  65 27 et seq., 31  
  – transparency  65 24  
  – triangular constellations  65 22  
  – vote  65 27 et seq.  

Distinguishing between controller and processor  4(7) 1  
Division of responsibility  26 46  
  – arrangement  26 43  
Doctor  14 18, 15 9, 26, 16 6, 23 27  
Documented  28 24  
“Do-not-track” standard  12 4  
Doping  49 29  
DPD  
  – and EDPB  64 53  
  – employee data protection  88 1 et seq.  
  – repeal  94 1 et seq.  

– Representatives of controllers and processors from third countries  27 2 et seq.  
– Territorial scope  3 5 et seq.  
– Transition  99 5  
– transition period  99 1  
– Transitional rule  94 3  
DPIA  39 17  
  – and prior consultation  28 45  
Draft decision  
  – opinion procedure  64 10, 31  
Drones  6(1)(f) 41  
Drug use  4(15) 13  
Due diligence process  13 13  
Duties of the members and employees  54 13  
Duty of secrecy  90 4  
Duty to inform  
  – dispute settlement procedure  65 32 et seq.  
  – urgency procedure  66 14, 19  
Duty to notify  88 42 et seq.  
  – the Commission  85 27  
Duty to provide information  18 23 et seq.  
eCommerce Directive  Intro 144  
EEA states  
  – Application of the GDPR  3 61  
  – Territorial scope  3 61  
Eledgated acts  43 1  
E-Evidence Regulation  48 2  
Effectiveness  5 14  
Electronic communications  90 17, 97 13  
Electronic form  28 79  
Electronic health records  20 8  
Electronic information exchange  
  – opinion procedure  64 46  
Electronic payments  9 10  
Electronic signatures  28 80  
Email service providers  4(7) 37  
Employee data protection  4(8) 7  
  – dependence of the employee  88 12 et seq.  
  – information expectations of employers  88 14  
Employees  6(1)(f) 17  
  – consent  49 13  
  – fundamental rights  88 37  
  – multinational corporation  49 18  
Employer-employee relationship  4(7) 7  
Empower the data subject  26 55  
Encouragement  40 17  
Encryption  32 26  
Enforcement  13 15, 14 19, 15 31, 19 12, 20 14, 33 17 et seq., 34 15 et seq., 57 8, 65 17 et seq.  
  – consistent  64 1, 26  
  – execution  41 24  
Entities  4(9) 6  
Entry into force  90 24, 94 3, 99 1  
  – applicable law  99 4  

Index
Index

- law of the Member States 99 6
- legal consequences 99 4
Equal control 26 29
Erasure 18 2, 5, 10 et seq.
Essential and non-essential means 4(7) 20, 26 22 et seq.
Essential content 5 19
Established procedures - complaints 41 17
- eligibility 41 16
Establishment - Definition 3 16 et seqq.
- Flexible definition by the ECJ 3 17
- Of Representatives of controllers and processors 27 19
Establishment, exercise or defence 9 59 et seq.
Ethics approval 89 15
Ethics for regulated professions, breaches of 23 24
EU Charter of Fundamental Rights 13 1, 14 1, 15 1, 3, 16 2, 23 1, 3, 7 et seq., 10, 12, 22, 85 7 et seq., 18 et seq., 22
EU Ombudsman 86 4
European Administrative Law - dispute settlement procedure 65 1
- opinion procedure 64 36
European Commission, delegated acts and implementing acts 12 30, 92 1 et seq., 93 1 et seq.
- action for annulment 92 15, 17
- committee to support the Comm 93 1
- duration of the delegation 92 10, 12
- EDPB 93 3, 5
- European primary/secondary law (consistency with) 92 4
- examination procedure 93 4 et seq.
- executive nature 92 5
- exercise of the delegation 92 1 et seq.
- extensive system of revocation and opposition options 92 13
- legislative act 92 3 et seq., 8 et seq.
- legislative powers (of Comm) 92 3, 5
- legislative process 92 6
- notify the Council and the EP of delegated acts simultaneously and in a timely and appropriate manner (duty to) 92 15
- objection 92 12 et seq., 16
- objectives, content, scope and duration of the delegation 92 10
- overlap 92 5
- principle of democracy 92 8 et seq.
- principle of materiality 92 9, 13
- procedure for adopting delegated acts 92 11
- Regulation (EU) No 182/2011 93 1, 6
- representatives of the Member States 93 3
- right of opposition 92 13, 15
- right of revocation 92 13
- subordinated legal acts 92 4
- supplement or amend certain non-essential elements of the legislative act 92 9
- tertiary EU law 92 4
- TFEU 92 3 et seq., 8 et seq., 15, 17 et seq., 93 1
European Commission, reports 97 1 et seq.
- adequate level of protection 97 6
- application and functioning of Chapter VII of the GDPR 97 9
- content 97 5
- deadline 97 11
- EU-US Privacy Shield 97 7 et seq.
- evaluate and review the GDPR 97 5
- proposals to amend the GDPR 97 12
- public (report) 97 1, 5, 7
- reporting obligation 97 3, 15
- request information 97 11
European Convention on Human Rights 23 3 et seq., 12, 22, 34, 33 18, 85 8, 20
European Court of Justice
- action for annulment, dispute settlement procedure 65 39 et seq.
- infringement proceeding 65 43
- preliminary ruling procedure, dispute settlement procedure 65 42
European Data Protection Board 68 1 et seq., 69 1 et seq., 70 1 et seq., 71 1 et seq., 72 1 et seq., 73 1 et seq., 74 1 et seq., 75 1 et seq., 76 1 et seq., 86 4
- access to documents (confidentiality) 72 3, 76 3 et seq., 9
- accreditation 64 18
- accreditation of certification bodies 70 8
- action for annulment 70 10, 12
- activities of the SAs 69 3
- advise the Comm 68 4, 70 4
- and EDPB 65 34
- annual report (publication/transmission) 70 9, 71 1 et seq.
- Art. 29 WP 68 2 et seq., 70 4, 71 1, 3, 72 1 et seq., 73 1 et seq., 74 1 et seq., 75 1 et seq., 76 1 et seq., 86 4
- as legal successor of the Art. 29 WP 94 13
- balance between the federal government and the states 68 10
- BDSG 68 6 et seq.
- binding decision 68 3, 70 2 et seq., 10 et seq., 71 2 et seq., 72 2 et seq.
- central data protection authority for the EU 68 1
- certification 70 8
- certification body 64 18
- Chair 64 47 et seq., 65 28 et seq.
- chair (of EDPB) 68 5, 11, 69 6, 70 3, 72 3, 73 1 et seq.
- chair represents EDPB in its external relations 73 2
- CJEU 69 2, 70 4, 12, 71 1, 72 3, 76 5
- codes of conduct 64 15 et seq.
- collaborate with the aim of ensuring the consistent application of the GDPR 68 9

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

- collaboration and dialogue between the SAs 70 9
- composition 68 6, 72 3
- confidentiality 76 1 et seq.
- consistent application of the GDPR 68 3, 9, 70 2 et seq., 6
- contractual clauses 64 20 et seq.
- cooperation between the SAs 68 4, 70 9
- cooperation with supervisory authorities 64 57
- Council negotiations 68 1
- data protection impact assessment 64 13 et seq.
- data protection supervision 69 3, 70 7
- deputy 68 7 et seq., 72 3, 73 1 et seq.
- discretion 66 15, 20, 70 2
- dispute settlement procedure 65 11 et seq., 17 et seq.
- EDPS 68 2, 11, 72 2, 73 1
election of chair of EDPB (incl. duration) 73 1 et seq.
- European data protection standards 70 7
- expedient information 68 9
- Federal Commissioner for Data Protection and Freedom of Information 68 7, 9 et seq.
- federal states 68 7, 9 et seq.
- guidelines 42(4) 1, 69 9, 70 2, 6 et seq., 71 2 et seq., 72 3
- head of one SA of each EU Member State 68 6
- implement the duties 70 2
- independence 65 1, 68 2, 69 1 et seq.
- joint position 68 9 et seq.
- joint representative 68 6 et seq., 9
- joint representative of the Federal Republic of Germany on the EDPB 68 7
- justiciable 69 3
- legal personality 68 5, 70 11
- legal protection 64 42, 65 38 et seq.
- legislative process 68 1
- Leitlinien 65 4 et seq.
- level of data protection in a third country (adequate) 70 4
- majority principle 65 23, 27 et seq.
- material 64 50
- non-exhaustive (list of tasks) 70 1
- not bound by instructions 69 1, 70 2
- objection, relevant and reasoned 65 7
- Öffentlichkeit 64 53
- opinion procedure 64 1 et seq., 6, 8 et seq., 23 et seq., 31, 41, 47
- Opinion upon request 64 23 et seq.
- opinions 70 2 et seq., 13, 72 3
- powers of SAs 68 1
- procedure 72 1 et seq.
- proposals for amendments to the GDPR 70 4
- public electronic register 70 9
- recommendations 70 2, 6, 71 2 et seq., 72 3
- re-election 68 8, 73 2
- register 64 53
- reporting obligation 70 9, 71 1 et seq., 72 3
- reports 71 1 et seq.
- representative of the Comm 68 11, 72 2
- resources 64 1
- role in determining the success of the GDPR 70 7
- rules of procedure 64 31, 72 1 et seq., 73 3, 74 3 et seq., 76 1 et seq., 4, 6, 8
- secretariat 64 50, 68 2, 72 3, 73 2, 74 4, 75 1 et seq.
- simple majority (EDPB procedure) 70 3, 72 1 et seq., 73 2
- supervisory authority 65 17 et seq.
tasks of EDPB) 70 1 et seq.
- TFEU 69 1, 70 10 et seq., 76 4
- the public 65 34
- translation 64 50
two-thirds majority (EDPB procedure) 72 2
urgency procedure 66 18, 70 3
European Data Protection Seal 42 3, 23
- consistency mechanism 64 18
- opinion procedure 64 18
European Essential Guarantees 23 11
European Research Area (ERA) 89 2
Evaluation
- approval 40 38
- opinion 40 38
Ex post right 21 18
Exchange of information 57 9
Exemption 5 18, 21 10, 30 15 et seq., 90 7, 22
Exemptions
- and derogations for privileged purposes 85 23 et seq.; see also Rights of the data subject
Exercise habits 4(15) 13
Exercise of official authority 20 11
Expertise of the parties 4(7) 41
Explainability 13 10, 15 19
Explicit arrangement 26 6
Explicit consent 9 40 et seq.
External DPO 37 38, 38 9
External influence 52 1
External oversight 24 32
Extraordinary termination 53 12
Facial images 4(14) 8
Facial recognition 16 7
Factors indicating processorship 4(7) 32
Factual influence 4(7) 10, 26 21
Fair and transparent processing 5 29 et seq., 13 1, 7, 40 23
Fair trial 33 18, 34 16

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

Fashion ID 47 31, 26 10, 35, 38
Federführende Aufsichtsbehörde
- urgency procedure 66 5

Filing system 46 1 et seq.
- accessible 46 11, 15, 21 et seq., 31
- automated (or non-automated) processing
  46 1 et seq., 5, 32
- automated filing system 46 4 et seq., 18
- centralised 46 31
- database 46 1, 4, 11, 23 et seq., 28,
  31 et seq.
- decentralised 46 31, 33
- dispersed on a functional or geographical
  basis 46 31
- single filing system 46 31 et seq.
- specific criteria 46 15, 19, 21 et seq.,
  24 et seq., 28
- structured (set of personal data)
  46 15 et seq., 18 et seq., 21 et seq., 25,
  29, 31
- systematic records 46 18

Financial independence 52 21
Financial oversight 52 13
Financial resources 52 22
Fines 24 48, 58 20
Finger images 414 8
Fingerprints 414 8
Foreign Intelligence Surveillance Act (FISA) 45 41

Forensic laboratories 10 19
Format
- opinion procedure 64 46
Foreseeability 13 10, 14 17, 23 7
Forum shopping 3 31
Foundations 9 52 et seq.
Fragmentation 40 60
Free flow of non-personal data 20 1
Free flow of personal data 424 3, 51 1

Freedom of expression and information 16 14,
  20 13, 85 1 et seq., 19, 21, 25
- academic, artistic and literary purposes
  85 5, 17
- academic purposes 85 4, 17
- administrative and commercial activity
  85 14
- application at national level 85 9
- blogger 85 13
- channel of publication 85 13
- chilling effect 85 18
- commercial speech 85 14 et seq.
- cross-border situations 85 26
- data security 85 2, 24
- effectiveness 85 18
- exemptions and derogations from data
  protection 85 23 et seq.
- fundamental rights and freedoms 85 8
- informational self-determination 85 1
- intermediaries 85 22
- Internet communications 85 22
- journalistic and other privileged purposes
  85 11
- manual processing 85 6
- news archives 85 16
- non-journalistic and other expressions 85 5
- online archives 85 16, 25
- online media 85 13, 25
- political actors 85 23
- press libraries 85 16
- processing and freedom of expression and
  information 85 1 et seq.
- processing for journalistic purposes 85 12,
  16 et seq.
- ranking platforms 85 22
- regulated self-regulation 85 10
- regulatory measures 85 9
- sanctions 85 23 et seq.
- search engine 85 15 et seq., 21 et seq., 25
- self-regulation 85 10
- underlying legal framework 85 10

Freedom of speech 85 1 et seq.; see also Freedom of expression and
information
Freely given 411 2, 21
Functional independence 52 8
Functionality creep 87 5

Fundamental rights Intro 126 et seq.
Fundamental rights and freedoms 23 9 et seq.,
  51 1, 85 1 et seq.

Further processing 5 74, 6 85
- compatibility 6 86
- legal basis 6 87
- permission 5 76

Future health status 415 13

Gait characteristics 414 8

GDPR proposal Intro 152

Genetic data 415 4, 414 1, 413 1 et seq., 4,
  9 26 et seq., 34, 84
- appearance 413 5
- biological sample 413 6 et seq.
- genes 413 4 et seq.
- genetic characteristics 413 4
- genetic information 413 4 et seq.
- health 413 1, 5
- phenotype 413 4
- physiology 413 5
- skin or hair color 413 5

Geo data 3 43

Geoblocking 64 28

Glasses or contact lenses 415 5

Glucose metering 415 7

Google Spain 417 28

Grandfathering
- data processing according to the DPD 94 5

Granularity 411 29
- purposes 26 41

1184

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

Group of companies 4(8) 6
  – DPO 37 23
Group of individuals 4(7) 5, 4(8) 5
Group of undertakings 47 4, 56 11, 88 34
Guarantees provided by the processor 28 8
Guidelines
  – EDPB 4(24) 1, 65 4 et seq.
Hair color 4(13) 5
Hand geometry 4(14) 8
Harmonisation 89 19
  – opinion procedure 64 1 et seq.
Health care services 4(15) 4
Health data
  Intro 128, 4(14) 1
  – alcohol consumption 4(15) 13
  – allergies 4(15) 5
  – analysis of urine and blood 4(15) 7
  – blood pressure 4(15) 13
  – diabetics 4(15) 14
  – diet 4(15) 13
  – disability 4(15) 4
  – disease 4(15) 4
  – hereditary or genetic predisposition
    4(15) 13
  – medical history 4(15) 4
  – obesity 4(15) 13
  – pulse/heart rate 4(15) 14
  – sleep diary 4(15) 14
  – smoking and drinking habits 4(15) 5
  – Territorial scope 3 48
  – weight 4(15) 14
Health professional 4(15) 4
Health status 4(15) 4
Heart rate monitor 4(15) 14
Hereditary or genetic predisposition 4(15) 13
Historical research 15 29, 16 14, 20 13
Hospital 4(15) 4
Hosting service provider 4(7) 37
Household activity 6(1)(f) 15
Household exemption 20 4, 85 5
Human dignity, respect for 23 10
Human resources 52 23
Identifiability 4(1) 23 et seq., 29
Identification 4(14) 4, 4(1) 17, 11 1 et seq.
Identifier 4(1) 23, 87 1 et seq.
  – of general application 87 1 et seq.
Identity theft 12 26
Imbalance of power 4(11) 24
Immigration control 23 10, 22
Impartiality 43 9
Implementation 5 7
Implementing act 40 55 et seq., 43 1, 64 16
Inaccuracy 16 8 et seq.
Incapable 9 51
Incentives 40 59
  – legal certainty 40 16
Incompatible occupations 52 20
Independence 41 15, 52 1
  – consistency mechanism 64 2
  – limitations 52 2
  – of SAs 51 4
  – supervising authorities 64 24
  – supervisory authority 66 16
Independent authority 52 5
Individual investigations 4(9) 10
Influence of controllership 26 22
Information 5 35, 12 1 et seq., 40 27;
  see also Rights of the data subject, Access, Right of
  – accessibility (eg. for blind persons)
    12 9 et seq.
  – actual disclosure 14 8
  – administrative fines 13 15
  – any relevant further information 13 13
  – artificial intelligence 13 10
  – automated decision-making 13 10
  – balance 14 12
  – between supervisory authority 65 14
  – burden of proof 14 10 et seq.
  – categories of processed data 14 4, 15 13
  – children, special needs of 12 12
  – cognitive overload 12 9
  – collected from the data subject 13 1 et seq.
  – collecting data 13 1 et seq., 4, 14 1, 3 et seq.,
    17
  – communication of all information 13 7
  – compensate for the lack of transparency
    14 7, 16
  – complaint 13 8, 15
  – confidentiality 14 18 et seq.
  – direct data collection 13 1 et seq.
  – disproportionate effort to provide 14 12, 16
  – duration of storage 15 16
  – duty to inform 13 2 et seq., 6, 9 et seq., 13
  – electronic means 12 15
  – excessive requests for information
    12 23 et seq.
  – exemptions from information obligations
    14 10 et seq., 23 1 et seq.
  – explainability 13 10
  – form 12 9
  – gratuitousness 12 21
  – icons 12 9, 11 23 et seq.
  – impossibility to provide the information
    14 11, 19 8
  – indirect data collection 14 1 et seq.
  – inspection of a file or computer 15 11
  – intelligibility 12 9 et seq., 13 10
  – judicial remedy 13 15
  – language 12 9 et seq.
  – layered notices 12 9, 15
  – legal basis 13 6, 9, 13
  – legal consequences for obtaining and ensuing
    processing 14 19
  – legitimate interests 13 2, 6
Index

- length of storage 13 9
- Like-Button 13 4
- machine learning 13 10
- meaningful information about the logic involved 13 10, 15 19
- means 12 14 et seq.
- messenger service 14 3
- monitoring 13 4
- name and contact details (of controller) 13 6
- of an infringement to the controller 28 60
- oral information 12 15
- principles of fair and transparent processing 13 1
- privacy policy 13 3, 12
- professional secrets 14 18
- publication of data 14 8
- purpose limitation (principle of) 13 13
- purpose of processing 13 6, 9 et seq., 13, 14 9, 15 12
- reasonable period 14 8
- recipient in a third country 14 4
- recipients 13 6, 13, 15 14 et seq.
- refusal to disclose 13 9
- relevant 64 44
- right to be informed about restrictions 23 38
- scoring 13 11
- seriously impair 14 14 et seq.
- social network 14 3
- source of the collected data 14 2, 7, 15 18, 19 7
- sufficient information about the processing 14 17
- time 12 18 et seq., 14 8
- undue delay 12 19
- whistleblower 14 7, 15

Informational self-determination, right to 12 1 et seq.

Informed 4(11) 2, 43
Infringement 11 20, 89 23, 90 9
- enforcement 41 22
- execution 41 22
Infringement procedure 90 24
- dispute settlement procedure 65 43
- opinion procedure 64 63
Initial purpose
- collection context 5 73
Inspections 28 54
Instructions of the controller 28 26, 29 1, 4

Intermediaries 85 22
Internal DPO 37 38, 38 9
Internal provisions
- consistency mechanism 64 22
International cooperation for the protection of personal data 50 1 et seq.
- CoE 50 6, 10
- considerable room for manoeuvre 50 1
- engagement of relevant stakeholders 50 7
- facilitate international mutual assistance 50 3
- Global Privacy Assembly (GPA) 50 8
- International Conference of Data Protection and Privacy Commissioners (IDPPC) 50 8
- international cooperation on data protection matters 50 9
- international organisations 50 1, 3, 6
- large number of mechanisms 50 7
- legal protection in cases with an international context 50 2
- mutual assistance 50 3, 7
- national SAs 50 1
- obligation to cooperate 50 1
- OECD 50 4
- promotion of the exchange and documentation 50 7
- third countries 50 1, 7
- United Nations 50 4 et seq.
International Covenant on Civil and Political Rights Intro 122
International data flows 44 4 et seq.
- Important reason of public interest 49 25
- international treaties 44 23 et seq.
- judicial proceedings 49 33
- LED 44 3
- necessity 49 7
- pre-contractual measures 49 20
- public registers 49 41 et seq.
- third-party beneficiary contracts 49 21 et seq.

International organisation 4(26) 1 et seq.
- association of two or more subjects of international law based on an international treaty in the field of international law to pursue a common purpose with at least one effective institution 4(26) 2
- effective data protection 4(26) 1
- effective institution 4(26) 2, 5
- intergovernmental organisation 4(26) 3, 7
- international law treaty 4(26) 4
- international legal subjects 4(26) 6
- Internet age 4(26) 1
- not necessarily have a solid institutional structure 4(26) 7
- not necessarily subject to international law 4(26) 7
- organisational units that can be allocated to the international organisation as a legal entity 4(26) 5

1186

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
# Index

- consent 6 2, 5, 8 et seq., 12, 15, 17 et seq., 33, 38, 43, 45, 53, 63, 67, 89 et seq.
- contract 6 2, 9, 23, 26 et seq., 30, 32 et seq., 47, 53, 59, 65, 80, 86, 88
- further processing 6 5, 33, 66, 85 et seq., 90
- lawfulness 6 6, 11 et seq., 18, 20, 83
- legal base (or basis) 6 1 et seq., 25 et seq., 30 et seq., 33 et seq., 38 et seq., 41 et seq., 47, 53 et seq., 58, 63, 65 et seq., 71, 73, 79 et seq., 85 et seq.
- legitimate interests 6 17, 25 et seq., 28, 30, 51 et seq., 57, 59, 61 et seq., 67, 69, 78, 88, 90
- machine Learning 6 38
- national laws 6 7, 15 et seq., 59, 75 et seq., 83
- necessity 6 2, 9, 20, 25, 33, 35, 49 et seq., 57, 67 et seq., 79, 86, 88
- pandemic 6 44
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller 6 44, 46 et seq., 82
- precontractual phase 6 39 et seq.
- privacy 6 7, 20 et seq., 37, 56, 59, 62, 73, 84
- processing in the public sector 6 47
- proportionality 6 8, 20, 42, 53, 57, 67, 84
- public interest 6 2 et seq., 5, 31, 44, 46 et seq., 53, 75, 78 et seq., 84
- public sector 6 87, 78, 84
- purpose of the processing 6 68, 82
- reasonable expectations (and reasonable expectations of privacy) 6 52, 73
- regulatory competence for Member States 6 75 et seq.
- Risk assessment 6 62
- Special categories of data (sensitive data) 6 11, 16 et seq., 45, 77, 90
- Two side markets 6 29
- vital interests 6 2, 43 et seq., 53

Lawyer 14 18

- Representatives of controllers and processors from third countries 27 12

Layering 4(11) 47

Lead supervisory authority 4(24) 1 et seq., 56 1
- competence 65 13a et seq.
- decision 65 35 et seq.
- decision EDPB 65 34 et seq.
- decision-making power consistency mechanism 65 11
- dispute settlement procedure 65 6, 13a et seq., 26
- legal protection 65 38
- Not for controllers and processors from third countries 3 57, 27 22

LED
- adequacy decision 45 2
- Transfer to third country 44 3

Legal and financial consequences 32 38

Legal basis 6 1 et seq., 9, 21 9
- continuity legal basis 94 5 et seq.
- national law 6 75

Legal certainty 5 16, 40 61

Legal claim 9 59 et seq.

Legal hearing
- consistency mechanism 64 51
- dispute settlement procedure 65 24

Legal incapability 9 51

Legal persons 4(1) 14

Legal protection
- consistency mechanism 64 42
- decision supervisory authority 64 7
- dispute settlement procedure 65 38 et seq.
- EDPB 64 42, 65 38 et seq.
- opinion procedure 64 7, 42, 63
- supervisory authority, lead 65 38

Legal regulation
- of secrets 9 2

Legal requirements 5 26 et seq.

Legality 6 7

Legislative history Intro 146 et seqq.

Legislative procedure Intro 146 et seqq.
- role of EP Intro 154 et seq.
- trilogue Intro 158

Legitimate interest 4(10) 1, 6 25, 51, 13 6, 19 11, 21 5, 40 24
- concept 6 58
- economic rights 6 63
- of third person 6 64
- processors 6 65

Legitimate purpose 5 59, 70

Length of time for which data will be stored 13 9

Letterbox corporation
- Territorial scope 3 17

Level of abstraction 5 148

Liability of the sub-processor 28 70

Liability towards the data subject 24 49

Like button 13 4

Limiting effect 5 52

Limits of more specific national data protection 88 28 et seq.

Limits on consent 4(11) 9

Lindquist judgement 3 19, 44 18 et seq.

List of tasks 39 2

List of technical and operational measures 24 30

Literary purposes 15 29, 19 11, 85 17

Living document 30 7

"Lock-in" effect 20 1

Logic involved see meaningful information about

Machine learning 6 38, 13 10

Machine readability 20 7 et seq.

Mail marketing 4(7) 39
Main establishment 56 6
– consistency mechanism 65 15
– dispute settlement procedure 65 15
Main establishment of controller and processor 4(16) 1 et seq.
– central administration in the Union 4(16) 7 et seq., 10, 13
– change of the main establishment 4(16) 15
– cross-border processing 4(16) 1, 16 et seq., 20 et seq.
– establishments in more than one Member State 4(16) 4 et seq., 7 et seq., 15
– group of undertakings 4(16) 2, 16
– interaction of a controller and a processor 4(16) 2, 17 et seq.
– joint controllers 4(16) 2, 19
– lack of a central administration in the Union 4(16) 20 et seq.
– lead supervisory authority 4(16) 1, 15, 17, 20 et seq.
– main establishment in the case of a controller 4(16) 10 et seq.
– main establishment in the case of a processor 4(16) 13 et seq.
– main processing activities 4(16) 13 et seq.
– one-stop-shop 4(16) 1
– purposes and means of the processing 4(16) 8, 10 et seq., 13, 16
– specific obligations 4(16) 13 et seq.
Majority principle
– consistency mechanism 64 31
– dispute settlement procedure 65 20, 23, 27 et seq.
– EDPB 65 23, 27 et seq.
– opinion procedure 64 39 et seq.
– urgency procedure 66 18
Manual processing 85 6
Market place principle 3 3 et seq., 32 et seq.
– Cloud computing 3 46
– Competent supervisory authority 3 57
– controller 3 54 et seq.
– Delimitation to the principle of establishment 3 22 et seq., 36 et seq.
– Field staff 3 43
– Invitatio ad offerendum 3 42, 44
– Irrelevance of the location of processing 3 38
– Legitimation under international law 3 33
– Mobile stalls or trade fair stands 3 43
– Monitoring of behaviour within the Union 3 47 et seq.
– Offering of goods and services in the Union 3 40
– Offers without payment 3 41
– processor 3 54 et seq.
– Representatives of controllers and processors from third countries 3 57
– Websites 3 45
Market research agency 4(7) 38
Marketing 6(1)(f) 1
Material scope 2 1 et seq.
– automated assistance 2 25
– automated data processing 88 19
– automated means 2 23 et seq., 33, 41
– automated processing 2 9, 25, 55
– competent authority/ies 2 70, 74 et seq.
– Convention 108 2 7 et seq., 21, 52, 55, 85
– course of an activity 2 49 et seq.
– cross-border 2 1, 18
– data portability 2 23, 45
– Digital Single Market 2 46, 90
– Directive 2000/31/EC 2 92
– electronic commerce 2 90 et seq.
– ePrivacy Regulation 2 1, 91, 99 et seq.
– EU organisations 2 86 et seq.
– exemptions 2 1, 15, 33, 47 et seq., 65, 69, 82, 85
– filing system 2 15, 26, 32 et seq., 85
– intermediary service providers 2 95, 98 et seq.
– internet service providers 2 96 et seq.
– judicial authority/ies 2 77 et seq.
– LED 2 4 et seq., 9, 14 et seq., 68 et seq., 84, 86, 90
– manual processing 2 11, 23, 31, 36, 40 et seq., 85
– online activity/ies 2 60 et seq., 65 et seq.
– personal or household (activity) 2 56, 58, 60, 67
– Regulation (EC) No 45/2001 2 15, 86, 89
– risk of circumvention 2 39 et seq.
– social network 2 60, 63 et seq.
– techniques used 2 39 et seq.
– technologically neutral 2 39 et seq.
– TEU 2 15, 53
– TFEU 2 4 et seq., 48, 53
– verification (process) 2 1, 7, 18
– wholly or partly 2 21 et seq.
Matters of general application
– examples 64 28
– opinion procedure 64 25 et seq.
Media 85 1 et seq.
– administrative and commercial activities 85 14
– media archives 85 16, 25
– media privilege 85 11, 18
Medical data 4(15) 5
Medical device 4(15) 4
Medical history 4(15) 4
Medical record 16 6, 11
Mergers and acquisitions 13 13
Messenger service 14 3
Micro, small and medium-sized enterprises 30 15 et seq.
Microsoft Ireland v. US 48 6
Minimisation of data 25 46
Minimisation of processing 25 47
Minimisation of storage 25 48
Minimising access 25 49

Index

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
## Index

<table>
<thead>
<tr>
<th>Topic</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misinformation</td>
<td>16 1</td>
</tr>
<tr>
<td>Mobility related applications</td>
<td>10 9</td>
</tr>
<tr>
<td>Money laundering</td>
<td>90 6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>57 8, 89 5</td>
</tr>
<tr>
<td>Monitoring bodies</td>
<td>40 36, 41 7</td>
</tr>
<tr>
<td>Monitoring, inspection or regulatory functions</td>
<td>23 25</td>
</tr>
<tr>
<td>Monitoring mechanisms</td>
<td>40 37</td>
</tr>
<tr>
<td>Monitoring responsibility</td>
<td>41 2, 8 et seq.</td>
</tr>
<tr>
<td>Monitoring systems</td>
<td>88 38 et seq.</td>
</tr>
<tr>
<td>Moving</td>
<td>4(14) 8</td>
</tr>
<tr>
<td>Multiple controllers</td>
<td>4(11) 49</td>
</tr>
<tr>
<td>Multiple processors</td>
<td>4(8) 8</td>
</tr>
<tr>
<td>Municipal authorities</td>
<td>4(7) 33</td>
</tr>
<tr>
<td>Mutual legal assistance treaties</td>
<td>48 2, 9, 49 30</td>
</tr>
<tr>
<td>National accreditation body</td>
<td>43 2</td>
</tr>
<tr>
<td>National derogations</td>
<td>90 11</td>
</tr>
<tr>
<td>National Identification Number (NIN)</td>
<td>87 1 et seq.</td>
</tr>
<tr>
<td>National law specifications</td>
<td>90 12</td>
</tr>
<tr>
<td>National margin of appreciation</td>
<td>90 13</td>
</tr>
<tr>
<td>National security laws</td>
<td>23 15 et seq.</td>
</tr>
<tr>
<td>– divergences</td>
<td>32 6 et seq.</td>
</tr>
<tr>
<td>Natural or legal person</td>
<td>4(10) 6, 4(9) 5</td>
</tr>
<tr>
<td>Natural or legal person, public authority, agency or other body</td>
<td>4(7) 3, 4(8) 5</td>
</tr>
<tr>
<td>Necessity</td>
<td>5 49, 93, 6 67, 90 19</td>
</tr>
<tr>
<td>– in public interest or in exercise of official authority</td>
<td>6 49</td>
</tr>
<tr>
<td>Negative list</td>
<td>64 14</td>
</tr>
<tr>
<td>Nemo tenetur se ipsum accusare</td>
<td>31 12, 33 18, 34 16</td>
</tr>
<tr>
<td>Network and information security</td>
<td>32 2</td>
</tr>
<tr>
<td>New accountability</td>
<td>24 8</td>
</tr>
<tr>
<td>Non-active supervisory authorities</td>
<td>66 17</td>
</tr>
<tr>
<td>– urgency procedure</td>
<td>28 30</td>
</tr>
<tr>
<td>Non-disclosure agreement</td>
<td>6 67 et seq.</td>
</tr>
<tr>
<td>Notice of an infringement</td>
<td>58 9</td>
</tr>
<tr>
<td>Notification about rectification, erasure and restriction of processing</td>
<td>19 1 et seq.</td>
</tr>
<tr>
<td>– administrative sanctions</td>
<td>19 12</td>
</tr>
<tr>
<td>– archiving purposes</td>
<td>19 11</td>
</tr>
<tr>
<td>– data protection management system</td>
<td>19 5</td>
</tr>
<tr>
<td>– direct disclosure</td>
<td>19 4 et seq.</td>
</tr>
<tr>
<td>– DPD</td>
<td>19 2, 9</td>
</tr>
<tr>
<td>– exemptions</td>
<td>19 11</td>
</tr>
<tr>
<td>– inform the data subject (duty to)</td>
<td>19 1, 9, 11 et seq.</td>
</tr>
<tr>
<td>– LED</td>
<td>19 3</td>
</tr>
<tr>
<td>– legitimate interests (of the data subject)</td>
<td>19 11</td>
</tr>
<tr>
<td>– notification impossible or involving disproportionate efforts</td>
<td>19 8 et seq.</td>
</tr>
<tr>
<td>– notification in advance</td>
<td>19 5</td>
</tr>
<tr>
<td>– notify recipients (duty to)</td>
<td>19 1, 5, 12</td>
</tr>
<tr>
<td>– publication of data</td>
<td>19 4, 8</td>
</tr>
<tr>
<td>– regulatory gap</td>
<td>19 7</td>
</tr>
<tr>
<td>– request (of the data subject)</td>
<td>19 1, 5, 10</td>
</tr>
<tr>
<td>– Streisand effect</td>
<td>19 11</td>
</tr>
<tr>
<td>– without undue delay</td>
<td>19 5</td>
</tr>
<tr>
<td>Notification to the Commission</td>
<td>51 25</td>
</tr>
<tr>
<td>Notify</td>
<td>90 23</td>
</tr>
<tr>
<td>Obesity</td>
<td>4(15) 13</td>
</tr>
<tr>
<td>Objection</td>
<td>64 43 et seq.</td>
</tr>
<tr>
<td>– processor</td>
<td>64 44</td>
</tr>
<tr>
<td>– responsible</td>
<td>64 44</td>
</tr>
<tr>
<td>Obligation to inform</td>
<td>66 15</td>
</tr>
<tr>
<td>– opinion procedure</td>
<td>64 1 et seq.</td>
</tr>
<tr>
<td>– processor</td>
<td>64 44</td>
</tr>
<tr>
<td>– public data</td>
<td>86 1</td>
</tr>
<tr>
<td>– re-use of public sector information</td>
<td>86 7, 12</td>
</tr>
<tr>
<td>– transparency</td>
<td>86 3 et seq., 11</td>
</tr>
<tr>
<td>Ombudspersons</td>
<td>14 15</td>
</tr>
<tr>
<td>One-agency-one-vote</td>
<td>64 39</td>
</tr>
<tr>
<td>One-member-one-vote</td>
<td>64 39 et seq.</td>
</tr>
<tr>
<td>One-stop shop</td>
<td>55 2, 56 1</td>
</tr>
<tr>
<td>One-Stop Shop procedure</td>
<td>65 13a et seq.</td>
</tr>
<tr>
<td>Online archives</td>
<td>85 16, 25</td>
</tr>
<tr>
<td>Online media</td>
<td>85 13</td>
</tr>
<tr>
<td>Onward transfers</td>
<td>44 27 et seq., 45 12</td>
</tr>
<tr>
<td>– Standard contractual clauses (SCC)</td>
<td>46 35</td>
</tr>
<tr>
<td>Opening clause</td>
<td>58 34</td>
</tr>
<tr>
<td>Opening clauses</td>
<td>3 9 et seq., 29</td>
</tr>
</tbody>
</table>
Index

Opinion procedure 16 10, 64 1 et seq.
- acceptance 64 51
- accreditation 64 18
- Administrative Law, European 64 36
- administrative procedure, staged 64 1
- Art. 288 para. 5 TFEU 64 6
- Art. 29 Group 64 3
- binding 64 13
- Binding Corporate Rules 64 22
- binding decision 64 12, 23, 33 et seq.
- binding legal force 64 6
- binding supervisory authority 64 6 et seq.
- blocking period 64 54
- certification body 64 18
- codes of conduct 64 15 et seq.
- Comm 64 4, 16
- competent authority 64 4
- competent supervisory authority 64 10
- competition 64 14, 20 et seq., 25
- compulsory 64 8 et seq.
- consistency mechanism 64 1 et seq., 8
- Content 64 1
- contractual clauses 64 20 et seq.
- data processing, cross-border 64 5
- data protection impact assessment 64 13 et seq.
- data protection seal, EU/European 64 18
- deadline 64 36 et seq., 45, 57
- decision 64 10
- dispute settlement procedure 65 17 et seq.
- draft decision 64 31, 54
- draft resolution/of decision 64 10
- EDPB 64 8 et seq., 41, 47
- effect, de facto 64 6
- effect, legal 64 6
- effect, procedural 64 7
- enforcement 65 17 et seq.
- form 64 57
- format 64 46
- Grenzen 64 32
- Harmonisation 64 1 et seq.
- hearing, legal 64 51
- history 64 4
- independence supervisory authorities 64 2
- information exchange, electronic 64 46
- information, relevant 64 44
- legal consequence 64 12, 16 et seq., 33 et seq., 38, 55 et seq., 59, 65 17 et seq.
- legal force 64 34 et seq.
- legal protection 64 7, 42, 63
- Lis pendens 64 34 et seq.
- majority principle 64 31, 39 et seq.
- Mandatory
- matters of general application 64 25 et seqq.
- obligation to inform 64 43 et seq.
- one-agency-one-vote 64 39 et seq.
- opinion, unterlassene Einholung 64 7 et seq.
- participation of third parties 64 51
- positive list 64 14
- preclusion 64 60
- precondition 64 9 et seq., 33 et seq., 41
- presumptive examples 64 26
- procedure 64 16, 31 et seq., 50, 52
- proceeding 64 11, 56 et seq.
- purposes 64 1, 6, 8
- reinterpretation 64 10
- relation to dispute settlement procedures 64 59 et seq.
- request 64 1, 23 et seq.
- requirements 64 23 et seq.
- scope 64 32
- scope of application 64 5, 9
- soft law 64 6
- standard contractual clauses 64 19
- Structure 64 1
- supervising authority 64 52
- supervisory authority, competent 64 54
- Systematic 64 1
- the public 64 51, 53
- Time limit 64 31
- transparency 64 57
- triangular constellation/case 64 37
- urgency procedure 66 15
Organisational independence 52 10
Organisational measures 25 24, 28 et seq., 32 27
- effectiveness review 32 31
Outsourcing 49 23
Over-accuracy 16 8
Overriding defaults 25 50
Palm print 4(14) 8
Pandemia 6 44
Paper files 15 4
Particular inquiry 4(9) 9
Passenger name records 45 31
Patient 14 18, 15 9, 26, 16 6, 23 27, 33 7
Patient support group 4(15) 5
Penalties 90 9
Performance
- in public interest or in exercise of official authority 64 66
Performance indicators 25 57
Performance of a contract
- Backups 49 16
- centralization 49 17
- employment contract 49 17
- international data flows 49 15 et seq.
- marketing 49 16
- outsourcing 49 17
- PNR 49 16
- third country transfer 49 15 et seq.
Permissibility 5 23 et seq.
Permissive norms
- purpose specification 5 67
- rights of data subjects 5 65
Person acting under the authority of the controller or the processor 29 1
Personal data 9 24, 37 22
- anonymization 4(1) 24 et seq., 29
Index

- anonymous data 4(1) 2, 5
- Big Data 4(1) 25, 28
- encrypted data 4(1) 7
- evaluative information 4(1) 10
- format of information 4(1) 12
- identifiability 4(1) 23 et seq., 26 et seq.
- identification 4(1) 1, 5 et seq., 17 et seq.
- identifier(s) 4(1) 6 et seq., 11, 20, 23
- legal person 4(1) 14
- natural person 4(1) 1 et seq., 5, 9 et seq., 28
- non-personal data 4(1) 2, 17, 28
- privacy 4(1) 1, 4
- relating to criminal convictions and offences or related security measures 10 1
- security 32 1
- third party(ies) 4(1) 3, 7, 10, 24, 27
- unborn life 4(1) 16
- personal data breach 4(12) 1 et seq., 23 6, 33 1 et seq., 34 1 et seq., 58 16
- accidental breach 4(12) 7 et seq.
- accountability 33 6, 14, 16
- administrative sanctions 33 17 et seq., 34 15 et seq.
- alteration 4(12) 7, 34 4
- alternative exemptions 34 9
- appropriate technological protection measures 34 2
- availability 4(12) 1, 7, 34 4
- awareness 33 4
- back-up 4(12) 7
- bank and credit card data 34 4
- becoming aware of 28 43
- clear and plain language 34 6
- communication to the data subject 33 8, 13 et seq., 34 1 et seq.
- competent authority 33 5
- concise, transparent, intelligible and easily accessible form 34 6
- confidentiality 4(12) 1 et seq., 33 9 et seq., 16, 34 4, 10
- confidentiality breach 4(12) 1, 34 4
- controllers 33 5 et seq., 10 et seq., 15, 17. 34 4 et seq.
- coordinated approach 33 11
- cross-border breach 33 10
- daily press 34 13
- data breach response plan 33 11
- data exfiltration attack 4(12) 1
- data protection officer 33 5, 13
- definition 4(12) 1 et seq.
- destruction 4(12) 1, 7, 34 4
- disproportionate effort to communicate to the data subject 34 2, 12 et seq.
- documentation 33 16
- encryption 4(12) 5, 33 8, 34 10
- enforcement 33 1, 10, 17 et seq., 34 15 et seq.
- exemptions 33 10, 34 9
- fair trial 33 18
- form of the notification 33 13 et seq.
- gagging order 33 10
- high risk to the rights and freedoms of natural persons 34 2 et seq.
- human errors 33 1
- inform the data subject (duty to) 34 3, 9, 12
- information on the type, circumstances, time of the security breach and the categories of data affected by the breach 33 4
- insider attack 4(12) 4
- integrity 4(12) 2, 33 16
- integrity breach 4(12) 1
- internal human risk source 4(12) 4
- internal register of all data breaches 33 16
- internal reporting system 33 7, 11
- joint controllers 33 5, 34 5
- law enforcement 34 8
- LED 34 2
- likely to adversely affect 34 2
- loss 4(12) 7, 33 9, 34 4, 10
- loss of access 4(12) 1, 6
- measures for self-protection and mitigating the damage 34 1
- mispostal 4(12) 6
- nemo tenetur se ipsum accusare 33 18, 34 16
- no longer likely to materialise 34 2, 10
- notification 33 1 et seq., 34 1, 3
- “overreporting” 33 11
- persons outside the European Union 34 5
- phased notification 33 15
- potentially affected data subjects 34 5
- powers of the supervisory authority 34 14
- processors 33 5, 11 et seq., 34 5
- processors’ duties 33 5, 12
- pseudonymisation 33 9, 34 10
- public communication 34 2, 13
- ransomware 4(12) 7
- risk analysis 33 7, 9, 11, 34 3 et seq.
- risk to the rights and freedoms of natural persons 33 8 et seq., 34 3
- security breach 4(12) 1, 3 et seq., 7, 33 1 et seq., 6 et seq., 13
- simultaneous communication via parallel offline channels 34 13
- special categories of personal data 34 4
- standard notification form 33 13
- subsequent measures 33 8, 34 2, 10
- substantial precondition 34 3
- sufficient awareness 33 4
- suspicion 33 4
- systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences 34 4
- systematic monitoring of a publicly accessible area on a large scale 34 4
- time limit 33 3, 11 et seq., 34 8
- trade secrets 33 10
- transborder breaches see cross-border breaches

1192

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

– two-tier concept of transparency 33 1, 34 1
– undue delay 33 3, 11 et seq., 34 8
– website 34 13

Personal independence 52 7, 11

Personal scope
– self-employed workers 88 18
– the concept of ’employee’ 88 16 et seq.

Personalization
– Advertising 3 52
– Territorial scope 3 52

Persons that can act as data controllers 4(7) 3

Phenotype 4(13) 4

Physical or mental health 4(15) 4

Planet49 Intro 138

Pluralistic control 26 3

Political opinions 9 21

Portability, right to 15 24, 20 1 et seq.
– accept data (obligation to) 20 10
– Application Programming Interfaces 20 9
– archiving purposes 20 13
– automated processing 20 2, 7
– choice to receive data or have them transmitted 20 9
– cloud service provider 20 4, 6
– compatible data 20 8
– competing rights 20 12
– competition 20 1
– complaint 20 14
– consent 20 5 et seq., 11 et seq.
– contract 20 1, 3, 7, 10 et seq.
– cooperate (obligation to) 20 10
– cross-border health care 20 1
– data provided by the data subject 20 6
– deletion (right to) 20 3, 13
– download 20 8 et seq.
– freedom of expression and information 20 13
– intellectual property 20 12
– interoperable format 20 8
– judicial remedy 20 14
– LED 20 2
– lock-in effect 20 1
– machine-readable 20 7 et seq., 10
– new provider 20 4 et seq., 8, 10
– offline-media 20 8
– online transmission 20 8
– performance of a task carried out in the public interest or in the exercise of official authority 20 2, 11
– processor 20 6
– receive data (entitled to, right to) 20 2 et seq., 7 et seq., 12
– restriction of processing 20 4
– results of evaluating raw data created or inferred by controller (data as) 20 6
– rights and freedoms of others 20 3, 12 et seq.
– same branch of industry 20 10
– social media 20 1 et seq., 5, 8 et seq.
– social network(s) 20 2, 10, 12
– technically feasible 20 9
– trade secret 20 12
– transmit data (entitled to, right to) 20 3, 8 et seq.
– without technical or legal hindrance 20 8

Positive list
– opinion procedure 64 14

Potential threats 32 19

Practical concordance 5 25

Pre-contractual measures 49 20

Precontractual phase 6 39

Preliminary ruling procedure
– dispute settlement procedure 65 42

Press libraries 85 16

Pre-trial discovery 48 4, 49 34, 38

Preventive or occupational medicine 9 68

Principle of accountability 4(7) 25, 24 2
– debate 24 8

Principle of establishment
– Controller 3 24 et seqq.
– Definition of establishment 3 16 et seqq.
– Delimitation to the market place principle 3 22 et seqq., 36 et seq.
– GDPR 3 13 et seqq.
– Irrelevance of the location of processing 3 21
– Limited transferability of the CJEU-jurisdiction 3 22 et seqq.
– Problems of competence 3 30
– Processing in the context of activity 3 20 et seqq.
– Processor 3 24 et seqq.

Principle of scalability 24 34

Principle of territoriality
– urgency procedure 66 13

Principles (relating to processing of personal data) 5 1 et seq.
– access (right to) 5 1, 5, 33 et seq., 36, 65, 101, 135
– accountability (principle of) 5 63, 137, 146
– accuracy (principle of) 5 1, 12, 14, 19, 54, 61, 93, 107 et seq., 111 et seq., 114 et seq., 117 et seq., 148
– accurate data (and kept up to date) 5 107 et seq.
– adequate (in relation to the purpose) 5 42, 52, 60, 89 et seq., 105
– archiving purposes 5 75, 79, 81, 116, 128
– basic principles 5 7, 11, 13
– Big Data 5 23, 28, 43, 68, 80, 88, 99, 102, 120, 125, 129, 131, 150
– central general principle 5 45
– certificate 5 143
– certification mechanisms 5 37
– CFR 5 1, 19, 22, 24, 29, 33, 49, 95, 122
– change of purpose 5 75, 78, 80, 82
– codes of conduct 5 31, 143
– Convention 108+ 5 3

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

- Proactive accountability 24 9
- Processing 5 8, 10 15
- in the public sector 6 47
- means 4(7) 14
- of photographs 9 30
- purpose 4(7) 14, 6 42
- Processing in the context of employment 88 1 et seq.
- collective agreement(s) 88 1, 6 et seq., 10, 24, 26 et seq., 32, 37, 41 et seq.
- declaratory effect 88 29
- derogations (or derogating) 88 22, 32
- duty of compensation 88 33
- duty to notify 88 1, 9, 42 et seq.
- employment contract 88 8, 16, 20
- group data protection officer 88 37
- group of undertakings 88 9, 28, 34 et seq.
- groups of enterprises engaged in a joint economic activity 88 34, 36
- human dignity, legitimate interests and fundamental rights 88 28
- human resource allocation 88 14
- Intergovernmental Negotiations 88 11
- joint economic activity 88 28, 34, 36 et seq.
- Justice and Home Affairs Council 88 10
- monitoring systems at the workplace 88 20, 38
- national rules 88 2, 6, 21, 23 et seq., 26, 28, 31 et seq., 37, 40, 43 et seq.
- notification 88 6, 25, 42 et seq.
- primacy of Union law 88 41
- proportionality 88 8, 30
- public authority(ies) 88 15
- recruitment 88 17, 20, 40
- representatives 88 26 et seq., 37, 39
- safeguards 88 1, 6
- sanctions 88 8, 39, 41
- self-employed worker(s) 88 18
- sources of law 88 24
- subsequent amendments 88 44
- suitable and specific measures 88 28, 31, 33 et seq., 37 et seq.
- transparency 88 28, 31 et seq., 41
- Processing of personal data 4(2) 1 et seq., 15 8
- automated means 4(2) 32
- collection (of personal data) 4(2) 3, 6, 8, 16 et seq., 31, 35, 37
- disclosure (of personal data) by transmission 4(2) 21
- dissemination (of personal data) 4(2) 17
- erasure or destruction (of personal data) 4(2) 37
- filing system 4(2) 4, 6, 28 et seq.
- means of the processing 4(2) 32 et seq.
- organisation (of personal data) 4(2) 16, 21, 35, 38
- processing operation 4(2) 4, 7, 10, 20 et seq., 31, 34 et seq.
- recording (of personal data) 4(2) 16, 37
- restriction (of personal data) 4(2) 10, 38
- retrieval (of personal data) 4(2) 31
- set of operations 4(2) 16, 21, 24 et seq.
- sets of personal data 4(2) 10 et seq., 24, 26, 30 et seq.
- structuring (of personal data) 4(2) 10 et seq., 16, 21, 38
- Processing of personal data relating to criminal convictions and offences 10 1 et seq.
- anti-money laundering 10 11, 19
- authorised by Union or Member State law (processing) 10 9, 15, 19
- background checks 10 19
- comprehensive register 10 1, 22
- connected vehicles and mobility related applications 10 9
- criminal convictions and offences 10 1 et seq., 5 et seq., 10 et seq.
- criminal records 10 7
- discrimination 10 1
- forensic laboratories 10 11, 19
- registers of criminal convictions 10 2, 21
- security measures 10 1 et seq., 9 et seq., 19
- under the control of an official authority (processing) 10 9, 15
- Processing of the national identification number 87 1 et seq.
- de facto NIN 87 5
- direct identifiers 87 6
- functionality creep 87 5
- identifiers of general application 87 1 et seq., 5 et seq.
- safeguards 87 9 et seq.
- sensitive data 87 2, 6
- single unique global identifiers 87 3
- Processing under the authority of the controller or processor 29 1 et seq.
- access to the personal data 29 11
- anti-money laundering 29 12
- confidentiality 29 2, 9 et seq.
- employees of the controller or the processor 29 1
- instructions of the controller 29 1, 4 et seq.
- obligation of the processor to immediately inform the controller 29 4
- person acting under the authority of the controller or the processor 29 1, 8 et seq.
- sub-processor(s) 29 1, 8, 12
- whistleblowing 29 12
- Processing which does not require identification 11 1 et seq.
- ability to demonstrate 11 14
- data minimisation 11 1, 5, 13, 19
- disproportionate effort 11 3, 8
- documentation of internal policies 11 15
- documentation of measures 11 16

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Receive and transmit data, right to 20 3 et seq.

Recipients 4(9) 1 et seq., 13 6, 14 4, 15 14 et seq., 16 4, 19 3, 19 et seq.

acting under the authority of the controller or processor 4(9) 6
disclosed (data) 4(9) 1 et seq., 6, 9, 12

individual investigation 4(9) 10

natural or legal person, public authority, agency or body 4(9) 5

particular inquiry 4(9) 2, 8 et seq.

public authorities which may receive personal data in the framework of a particular inquiry 4(9) 8

records of data processing activities 4(9) 1

requests for disclosure 4(9) 12

scope of the right to information and the right to access 4(9) 1

third party 4(9) 2, 7, 11

Records of processing 5 142, 24 32, 30 1 et seq.

Records of processing activities 30 1 et seq.

accountability 30 1, 11

audit trail 30 9

data governance responsibilities 30 1

investigative powers 30 13

living document 30 7

micro, small and medium-sized enterprises 30 15 et seq.

Rectification 18 2, 5

Rectification management 5 114

Rectification measures 5 113

Rectification or erasure 58 18

Rectification, right to 16 1 et seq.; see also Rights of the data subject

accuracy 16 1 et seq., 8, 12 et seq.
allegations by third parties 16 9

arbitrary complement 16 13

completion 16 4, 13
correction 16 4, 6, 10, 12, 14
data quality (principle of) 16 8
diagnoses 16 6
estimates 16 11
ex post empowerment measures 16 2

facial recognition 16 7

freedom of expression; freedom of information 16 14

inaccurate 16 1 et seq., 7 et seq., 13

misinformation 16 1

opinions and value judgments 16 10

optional extension 16 12

over-accuracy 16 8

partial deletion 16 4

precision 16 8

right to directly control 16 2

scientific or historical research purposes; statistical purposes; archiving purposes in the public interest 16 14

sensitive data 16 7

supplementary statement 16 6, 13

trivial inaccuracies 16 8

without undue delay 16 3, 12 et seq.
Index

Refusal 11 19
Register 42 29, 43 14
– of criminal convictions 10 2 et seq.
– publication 40 51
Regulated self-regulation
– codes of conduct 64 17
Regulatory competence
– for Member States 67 77
Relevance 5 92
Religious or philosophical beliefs 9 23
Remedies
– urgency procedure 66 21
Remedies, liability and penalties 77 1 et seq., 78 1 et seq., 79 1 et seq., 80 1 et seq., 81 1 et seq., 82 1 et seq., 83 1 et seq., 84 1 et seq.
– action de groupe 80 15
– alternative remedy 79 6 et seq.
– behaviour of controller/processor 77 15, 82 3, 83 22 et seq.
– choice between the judge or the SA 79 6 et seq.
– choice of the competent SA 77 4, 9 et seq.
– collective redress 80 3 et seq., 8, 10 et seq., 13 et seq., 82 3
– consistency mechanism 77 2, 78 21, 79 3, 81 3, 11
– contact between courts 81 2, 7 et seq.
– damage 77 15, 80 9, 15, 82 1 et seq., 9 et seq., 14 et seq., 20, 23 et seq., 27 et seq., 30, 32 et seq., 83 21, 23
– data protection agreement 82 32
– EDPB opinion 78 4, 20 et seq.
– effective, proportionate and dissuasive 83 13, 36, 43, 84 12, 15
– establishment 79 21 et seq., 26 et seq., 29, 80 7, 16, 82 33 et seq., 83 11, 30
– form of the complaint 77 24 et seq.
– free of charge 77 28
– general conditions for imposing administrative fines 83 1 et seq.
– graduation of the amount of administrative fines 83 26
– gravity of the infringement 83 20 et seq.
– handling of the complaint 77 2, 29 et seq., 78 4, 14, 83 31
– inform the complainant/data subject (duty to) 77 12, 15, 29, 35 et seq., 78 4, 14, 83 23
– joint liability 82 5, 24 et seq.
– jurisdiction 78 5, 7, 12, 19, 79 1, 8, 21, 26, 28 et seq., 81 1 et seq., 4 et seq., 7, 9, 11, 13, 16, 18 et seq., 82 5, 33, 35
– legally binding decision 78 8
– liability 77 1, 82 1 et seq., 14, 18, 21 et seq., 27 et seq., 32, 83 2, 42
– mandate 80 4 et seq., 7, 9 et seq., 13
– Model for Collective Redress 80 8
– not-for-profit body, organisation or association 79 1, 80 7
– notification 83 29, 84 18 et seq.
– object of the complaint 77 21 et seq.
– opening clause 80 4, 11, 14 et seq., 83 42
– penalties 77 1, 82 3, 83 2, 5, 8, 37, 84 1 et seq.
– place of the alleged infringement 77 9 et seq.
– place of work 77 9 et seq.
– preliminary steps before the complaint 77 17 et seq.
– public authority 77 11, 78 16, 79 23, 80 15, 81 4, 82 34, 83 9, 18, 42
– public interest 77 11, 78 16, 79 23, 80 7, 82 34
– representation of data subjects 77 3, 80 1 et seq.
– residence 77 9 et seq., 79 21, 24 et seq., 29, 81 1, 82 33
– right to an effective judicial remedy against a controller or processor 79 1 et seq.
– right to an effective judicial remedy against a supervisory authority 78 1 et seq., 82 12
– right to compensation and liability 80 9, 17, 82 3 et seq., 83 2
– right to lodge a complaint with a supervisory authority 77 1 et seq.
– safeguards 80 12, 83 6, 40 et seq.
– suspension of proceedings 79 3, 81 1 et seq.
– temporal requirements 77 26 et seq.
Reporting template 33 13
Representatives of controllers and processors from third countries 3 7
– Administrative fine 27 17, 32 et seq.
– Admissibility of further tasks 27 10
– Branch as representative 27 12
– Children 27 16
– Conflict of interests 27 11
– Definition 27 5
– DPD 27 2 et seq.
– Effects on the territorial scope 3 17
– Establishment inside of the EU 27 19 et seq.
– Exceptions to the obligation of designation 27 13 et seq.
– Extent of the representation 27 22 et seq.
– Function 27 1
– Incompatibility with being appointed as external DPO 27 11
– Lawyers 27 12
– Legal person as representative 27 10
– Legal status 27 21 et seq.
– Liability of the represented entity 27 29
– Market place principle 3 57
– multiple 27 7
– No lead supervisory authority 3 57, 27 22
– Obligation of designation 27 6 et seq.
– Obligation to act according to instructions 27 25
– Own liability 27 26 et seq.
– Profiling 27 15
– Public authorities in third countries 27 18
– Qualifications 27 11
– Risk-based approach 27 13 et seq.
– Termination 27 8
– Time limit 27 8
### Index

- Written designation 278
- Representatives of controllers or processors not established in the Union 4(17) 1 et seq., 271 et seq.
- administrative coercion 2733
- application and enforcement (of GDPR) in third countries 271
- behaviour 2714, 19 et seq., 31
- branch as representative 4(17) 5, 2712
- breaches of contract 2726
- cases of doubt 2717
- coercive measures 2730
- communicative character 2722
- conflict(s) of interest 4(17) 5, 2710 et seq.
- cooperate with the SA 275, 26
- corrective powers 2728, 31
- designate a representative (obligation to) 4(17) 2 et seq., 5, 2772, 6 et seq., 17, 33
- electronic signature 278
- enforcement mechanism 2728
- establishment 4(17) 4, 273, 3, 12, 20, 22
- external DPO 2711
- factual requirement 276, 6, 13 et seq.
- fines 2711, 17, 26 et seq., 32 et seq.
- grounds for termination 279
- in writing 278
- infringements of the representative 2723
- large scale 2713, 15
- legal enforcement 2730
- legally effective declaration 2723
- legally regulated power of representation 4(17) 6, 2723
- legislative process 273
- limit the term of the designation 279
- mandate 4(17) 6, 278, 8, 12, 23, 25, 30
- material responsibilities 2727
- messenger 4(17) 6, 2723
- minimum degree of personal qualification 2711
- nature, context, scope and purposes (of processing) 2716
- need for control 2717
- occasionally 2713 et seq.
- procedural law 2729
- professional agent(s) 2712
- prohibiting the offering of goods or services 2731
- public authority/ies and body/ies 2718
- ratio of the market place 2719
- record of processing activities 275, 26
- risk assessment 2716
- risk to the rights and freedoms 2713
- several controllers or processors 4(17) 5, 2710
- specific duties of the representative 4(17) 6, 2733
- substantive law 2729
- territorial scope 271, 4, 26, 30
- third country 4(17) 3, 5, 2716, 22 et seq., 30 et seq.
- unlawfulness of the data processing 2732
- vagueness 2713

Research, academic and scientific 12, 23, 14, 13, 15, 29, 16, 14, 20, 13, 85, 17
- historic 14, 13, 15, 29, 16, 14, 20, 13
- public interest 14, 13
- Research consortium 26, 41

Research purposes 18, 17
Responsibility (of the controller) 5, 138, 241 et seq., 41 et seq.
- accountability (principle of) 242 et seq., 18, 30 et seq., 38, 45, 47 et seq.
- accountability mechanisms 246, 47
- appropriate and effective measures 241, 5, 48
- arrangement(s) 2418, 32, 41
- certification mechanism 246, 10, 47
- clear and transparent allocation 2654
- codes of conduct 246, 10, 27, 47
- complaints-handling mechanism 2432
- compliance evidence 243
- contractual arrangements 2432
- data breach reporting and handling procedures 2432
- data protection management and strategy 2444
- data protection policies 2410, 32, 42, 44 et seq.
- demonstrate compliance 241, 3, 7, 9 et seq., 47
- documentation 249, 32, 47
- DPO 249, 27, 31 et seq., 37, 42
- external oversight 2432
- fine(s) 244 et seq., 12, 48 et seq.
- impact (of processing on data subject) 2423, 26, 32
- joint control 2411, 15 et seq., 32, 36
- liability 245, 12, 28, 49
- necessity 2438, 45
- new accountability 248
- objective assessment 2423
- proactive accountability 246, 8 et seq.
- proportionality 249, 28 et seq., 44 et seq.
- records of processing activities 2432
- Regulation 2018/1725 246
- review and update of technical and organizational measures 2438 et seq.
- risk 2410, 19 et seq., 31 et seq., 39, 43, 45
- risk-based approach 2410, 23, 26
- sanctions 245, 48 et seq.
- scalability 2410, 19 et seq., 34
- scalable 2426, 31, 35, 46
- security measures 243, 9, 20, 26, 32 et seq., 36 et seq.
- technical and operational measures 2426, 30, 33, 36
- technical and organizational measures 247, 19 et seq., 22 et seq., 27 et seq., 32 et seq., 38 et seq., 42 et seq., 47, 50
- training (or education) 2421, 32, 35, 37, 42
- transfers (of data) 2432, 36, 42
- transparency 2432, 36

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

Restriction of processing 4(3) 1 et seq.
- blocking 4(3) 2 et seq.
- definition 4(3) 1 et seq., 6 et seq.
- marking 4(3) 5 et seq.
- measures to prevent 4(3) 6
- novelty 4(3) 1
- operations to communicate 4(3) 6
- Regulation 45/2001 4(3) 3
- right to reality of processing 4(3) 2, 4
- security measure(s) 4(3) 2, 6
- signalling and highlighting 4(3) 5
- technical measure(s) 4(3) 6
Restriction of the investigative powers 90 21
Restriction or prohibition of data processing 58 17
Restrictions of the rights of the data subject 5 9, 23 1 et seq.
- blanket restrictions 23 33
- breaches of professional ethics 23 24
- defence 23 4, 7, 19
- enforcement of civil law claims 23 30
- ethics for regulated professions 23 24
Restrictions of the rights of the data subject, execution of sentences 23 21
- abuse or unlawful access or transfer 23 34
- accountability 23 6
- additional restrictions 23 1, 22, 25
- automated decision-making including profiling 23 29
- chilling effect 23 9
- civil law claims 23 30
- confidentiality of deliberations 23 23
- Convention 108 23 3, 12
- data minimization 23 31
- disproportionate effort 23 26
- DPD 23 3 et seq., 14 et seq., 20, 22 et seq., 26, 30
- European Charter of Fundamental Rights 23 3, 9
- European Convention on Human Rights 23 3 et seq., 12, 34
- European Essential Guarantees 23 11
- execution of sentences 23 21
- foreseeability 23 7
- Guidelines by the European Data Protection Board 23 2, 6 et seq., 10 et seq., 20, 26, 37 et seq.
- human dignity 23 10
- immigration control 23 10, 22
- information about the logic involved 23 29
- inspection 23 25
- intellectual property 23 29
- judicial independence and proceedings 23 23
- judicial review 23 10
- law enforcement 23 5, 21, 24, 38
- LED 23 5, 21, 23, 38
- legislative powers 23 1
- less intrusive measures 23 13
- minimum requirements for restrictive legislative measures 23 31 et seq.
- monitoring 23 25
- national security 23 4 et seq., 7, 10, 15 et seq.
- necessity 23 4, 10, 12 et seq., 31 et seq.
- pressing social need 23 12
- professional ethics 23 24
- professional secrets 23 28
- proportionality 23 2, 7, 10, 13, 31 et seq.
- prosecution of criminal offences 23 21
- protection of the data subject and other persons 23 26 et seq.
- pseudonymisation 23 37
- public health 23 4, 7, 13, 22
- public interest 23 3 et seq., 7, 18, 22
- public security 23 6, 16, 20 et seq.
- Regulation (EU) 2018/1725 23 5
- regulatory functions 23 25
- restrictive interpretation 23 1
- right to be informed about restrictions 23 38
- rights and freedoms of other persons 23 26
- storage limitation 23 31
- storage period 23 36
- suitability (of restrictions) 23 13
- supremacy (principle of) 23 8
- technical procedures 23 34
- therapeutical privilege 23 27
- time limitation 23 7
- trade secrets 23 29
- transparency 23 7, 31
- Union institutions 23 5
Retargeting 37 21
Retina 4(14) 8
Return of the data by the processor to the controller 28 46
Re-use of public sector information 86 12
Review of issued certifications 58 8
Review of other Union legal act on data protection 97 7 et seq.
- amendment proposals 97 1 et seq.
- legislative proposals 97 6 et seq.
- scope 97 8
Review of other Union legal act on data protection 98 1 et seq.
- Cookies 98 14
- Discretion 98 1
- electronic communications 98 13
- free movement (of personal data) 98 4, 10
- legislative proposals 98 1, 8 et seq.
- review clause 98 3, 6, 11
- timeframe 98 9
- uniform and consistent protection 98 1 et seq., 6, 11
Revocation 41 19, 43 15
Right of access 45 9
Right to a detailed explanation 15 19
Right to access
- Standard contractual clauses (SCC) 46 36
Index

Right to be forgotten (to erasure) 17 1 et seq., 12, 14 et seq., 20, 21 3, 85 21 et seq., 25
- blocking (right to) 17 19
- censorship 17 11, 21
- child 17 20, 26, 29
- compliance with a legal obligation 17 21, 30
- control over data 17 3 et seq., 9
- court records 17 4
- data portability 17 4, 22
- data quality (principle of) 17 19
- deadlines (fixed; expiration) 17 27
- delete (duty/right to) 17 3 et seq., 6, 10 et seq., 18 et seq.
- detailed profile 17 16
- dissemination 17 9, 13, 20, 26, 31
- economic interests 17 11, 16, 18
- effectiveness 17 2
- enforceability 17 10
- expiration dates 17 4
- feasibility 17 5, 9, 12
- freedom of expression (and information) 17 11, 13, 17, 21, 30, 32
- historical, statistical and scientific research purposes 17 21
- inadequate, not relevant or excessive 17 19
- indexing 17 15
- inform third parties (duty to) 17 10, 24, 28
- information society (or societies) 17 13, 30 et seq.
- Internet users 17 6, 13, 15, 18
- journalistic, artistic, academic purposes or literary expression 17 32
- legal basis 17 30
- legal status 17 5
- limits (of the right to erasure) 17 32 et seq.
- no longer necessary 17 4, 19 et seq., 27, 30
- no longer needed 17 3
- object (right to) 17 4, 18, 20, 30
- proportionality 17 18
- public figure 17 17, 19
- public health 17 21
- publishers of websites 17 16, 18
- rectification (right to) 17 19, 22
- remove data 17 29, 34
- restrict (duty to restrict processing) 17 22 et seq.
- retention 17 21
- search engines 17 1, 15 et seq.
- storage 17 4, 9, 20, 23, 27, 34
- tech firms 17 9
- technical measures 17 10
- third-party advertisement 17 10
- withdraw consent 17 20, 30

Right to information
- scope 4(9) 1

Right to object 18 2, 15, 21 1 et seq.
- automated means 21 7, 20
- burden of proof 21 5
- compelling legitimate interest 21 5
- derogation 21 23
- direct marketing 21 1 et seq., 4, 6, 16 et seq., 20, 22
- exemptions 21 2, 10, 16
- grounds relating to the data subjects’ particular situation 21 5, 11
- information society service(s) 21 7, 20 et seq.
- obligation to inform 21 6, 18 et seq.
- right to erasure 21 3, 12
- scientific or historical research and statistical purposes 21 1, 8, 19, 22 et seq.

Right to privacy 90 18

Right to rectification 18 7

Right to request
- supervising authority, consistency mechanism 64 24

Right to restriction of processing 18 1 et seq., 9
- accuracy 18 8 et seq.
- allow or negotiate the processing 18 12
- consent 18 12, 20 et seq.
- enforcement 18 26
- erasure (right to) 18 1, 4 et seq., 11, 13, 23
- exceptions 18 20, 25
- inaccuracy (claim of) 18 8
- legal claims 18 13 et seq., 16, 20 et seq., 23
- legal consequences 18 18 et seq.
- legitimate grounds 18 16, 23
- object (right to) 18 1, 15 et seq.
- provide information (duty to) 18 23 et seq.
- public interest 18 15, 17, 20 et seq., 24
- rectification (right to) 18 1, 4 et seq.
- safeguard(s) 18 6 et seq., 12
- storage 18 18, 20
- unlawful processing 18 10 et seq.
- verification 18 7, 16

Rights of data subjects 5 40, 115, 40 28

Rights of the data subject 12 et seq.: see also Access, right of; Complement, right to; Correction, right to; Object, right to; Portability, right to; Receive and transmit data, right to; Rectification, right to; Restrictions
- burden of proof for exemptions 14 10
- denial of request 12 20, 24
- duty to facilitate the exercise 12 9 et seq., 16
- excessive exercise 12 22 et seq.
- exemptions 13 14, 14 10 et seq., 15 29 et seq., 16 14, 19 11, 20 11 et seq., 21 2, 10, 16, 23 1 et seq.
- gratuitousness to exercise 12 21
- identification of the controller 15 6
- identification of the data subject 12 25 et seq.
- motivation for exercising 12 23
- non-EEA-citizens 15 6, 34 5
- non-negotiable rights and obligations 12 5
- research 12 23, 20 11, 15, 21 1, 8, 19, 22 et seq.
- restrictions 20 11 et seq., 23 1 et seq.; see also exemptions
- right to copy of personal data 15 22 et seq.
- right to negative information 15 7
- time limits 12 18 et seq., 16 12

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

Risk adequacy
– big data 5 150
– ubiquitous computing 5 150
Risk and harm 32 13
Risk assessment 6 72, 28 10, 30 16, 32 14
Risk likelihood and severity 32 16 et seq.
Risk neutrality
– legal certainty 40 14
Risk prevention 25 5, 18
Risk reduction 11 1
Risk-based approach 5 140, 24 23, 26, 25 16,
32 11 et seq., 37 6, 39 25 et seq.
– Representatives of controllers and processors
from third countries 27 13 et seq.
Risky operations 32 18
Safe Harbour Intro 135
Safeguard of secrecy obligations 90 2
Safeguards 6(1)(f) 19, 22, 25 30, 39, 40 41,
41 23
Safeguards and derogations relating to
processing for archiving purposes in the
public interest, scientific or historical research
purposes or statistical purposes 89 1 et seq.
– advancement of knowledge 89 4
– appropriate safeguards 89 6, 14 et seq.
– archiving purposes in the public interest
89 1, 6, 8 et seq., 12, 16 et seq., 24
– concurrent purposes 89 24
– data minimisation 89 14
– derogations 89 3 et seq., 8, 11, 14, 16 et seq.,
21 et seq.
– European Research Area (ERA) 89 2, 11, 19
– fundamental rights 89 4
– historical research purposes 89 1, 6, 12, 16,
24
– Member State implementations 89 5
– pseudonymisation 89 15
– risk-based approach 89 15
– scientific research purposes 89 11, 24
– statistical purposes 89 1, 6 et seq., 13, 16, 24
– technical and organisational measures 89 14
Sanctions 24 5, 88 41; see Enforcement
Scalable 24 26, 31, 46
Schrems II 24 41
Scientific purposes
– International data flows 49 47
Scientific research 4(11) 35, 6(1)(f) 2;
see Research, academic and scientific
Social Plug-Ins
– Territorial scope 3 51 et seqq.
Scope of application
– opinion procedure 64 9
Scoring 13 11, 15 10
Screening tests 4(15) 6
Search engines 85 15, 22
Secondary legislation 89 18
Secrecy (obligation of) 90 1 et seq.
– confidentiality 90 4 et seq., 16, 22
– investigative powers 90 8, 16, 21
– national law specifications 90 12
– notify (duty to) 90 23 et seq.
– supervisory authority/ies (SA/SAs)
90 1 et seq., 7 et seq., 16, 18, 21 et seq.
Security breach notification see Personal data
breach
Security company 4(7) 40
Security incident see Personal data breach
Security measures 10 5, 24, 32, 89 15
– appropriate technical and organisational
measures 32 9 et seq.
Security of processing 32 1 et seq.
– accountability 32 14, 35, 37
– availability and access to personal data
32 30
– confidentiality, integrity and availability of
personal data 32 3, 33
– cyber-resilience approach 32 32
– divergences of national laws 32 6
– encryption 32 5, 10, 26
– legal and financial consequences 32 38
– likelihood and severity of the risk
32 16 et seq.
– network and information security
32 2 et seq.
– potential threats 32 17, 19
– pseudonymisation 32 5, 10, 21 et seq.
– regularly testing, assessing and evaluating
the effectiveness of technical and
organisational measures 32 31
– risk and harm 32 13
– risk-based approach 32 6, 11, 14, 24
– risks to the rights and freedoms of the data
subject 32 14
– risky operations 32 18
– security of personal data 32 1
– security principle 32 2 et seq., 11, 27, 32
– special group of security risks 32 33
– technical and organisational measures 32 4,
9 et seq., 35
– technology neutral approach 32 4, 6
– trilogue 32 5
– types of harm 32 20
Security principle 32 2
– availability 32 3
– confidentiality 32 3
– integrity 32 3
Security risks
– special category of risks 32 33
Self-help and support groups 4(15) 5
Self-monitoring 41 1
Self-protection 15 1, 34 1
Self-regulation 85 10

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

Sensitive data 6 17, 9 1 et seq., 7, 16 7, 34 4, 37 20
– archiving, scientific and historical research 9 75 et seq.
– biometric data 9 6, 29 et seq., 84, 64 28
– conclusive action 9 41
– COVID-19 9 9, 36, 49, 78
– data concerning a natural person’s sex life or sexual orientation 9 6, 10, 38
– data concerning health 9 9 et seq., 34 et seq., 73, 78, 84
– data revealing political opinions, religious or philosophical beliefs 9 10, 16, 21 et seq.
– data revealing racial or ethnic origin 9 18 et seq.
– data that are manifestly made public 9 14, 56 et seq.
– derogations 9 11 et seq., 15, 39 et seq.
– employment, social security and social protection law 9 47
– establishment, exercise or defence of legal claims 9 59 et seq.
– explicit consent 9 13, 40 et seq.
– foundations, associations, not-for-profit bodies 9 52 et seq.
– genetic data 9 26 et seq., 34, 84
– legal grounds 9 12 et seq., 16, 39
– photographs (processing of) 9 30, 32
– physically or legally incapable (of giving consent) 9 13, 48, 51
– preventive or occupational medicine 9 68 et seq.
– professional secrecy 9 68, 70 et seq., 83
– public health 9 71 et seq., 78
– public interest 9 65, 71 et seq.
– Representatives of controllers and processors from third countries 27 13 et seqq.
– right to be forgotten 9 60
– right to object 9 60
– right to restriction of processing 9 60
– Second Payment Services Directive 9 43
– secrets (legal regulation of); banking secrets; insurance secrets 9 1, 4
– social media 9 57
– substantial public interest 9 65 et seq.
– third country data transfers 9 60
– trade union membership 9 10, 24 et seq.
– vital interests 9 13, 48, 51
Sex life, sexual orientation 9 38, 16 7
Signature 4(14) 8
Single unique global identifier 87 3
Skin 4(13) 5
Sleep diary 4(15) 14
Small and medium-sized enterprises 40 15
Smart city 12 13
Smart data 37 17
Smart devices 5 85, 87
Smoking and drinking habits 4(15) 5
Social media and networks 6(1)(f) 18, 46, 9 57, 14 3, 20 2, 5, 12, 64 28

Sole interlocutor 56 16
Sources by law
– collective agreements 88 24 et seq.
Sources of law
– specific national rules 88 24 et seq.
Sovereignty
– urgency procedure 66 13
Special categories of data 4(14) 1, 9 1, 7, 37 22, 87 2; see Sensitive data
Special provisions 89 3
Specific authorisation 28 16
Specific rules 88 20 et seq.
Specific technical processing 4(14) 4
Stakeholders 40 45
– consultation 40 21 et seq.
Standard contractual clauses (SCC) 4(7) 13, 28 74, 46 31 et seq.
– breach of contract 46 45 et seq.
– choice of jurisdiction 46 44
– choice of law 46 44
– consistency mechanism 64 19
– data breaches 46 34
– data protection principles 46 34
– data subject rights 46 36
– governmental data access 46 42
– joint liability 46 37
– legal obligations in the third country 46 42
– legal remedies 46 41
– liability 46 37
– monitoring of domestic legislation 46 43
– onward transfers 46 35
– opinion procedure 64 19
– purpose limitation 46 34
– right to access 46 36
– safeguards 46 34 et seq.
– scope of application 46 32
– Sub-processing 46 46 et seq.
– supervision 46 39
– surveillance laws 46 42
– termination 46 45 et seq.
– third-party beneficiaries 46 36
– Transfer Impact Assessment (TIA) 46 42
– transfer third country 64 19
Standard data protection clauses 46 26 et seq., 58 29
– adoption 46 28
– approval 46 27
– intra-group agreement 46 30
– parties 46 30
– scope of application 46 29
– Standard contractual clauses (SCC 2021) 46 31 et seq.
Statistical purposes 14 13, 15 29, 16 14, 18 17
– international data flows 49 47
Steps counting 4(15) 14
Stock option plans 49 23
Storage limitation 5 62, 122 et seq.
– exceptions 5 128
– necessity 5 121

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-8487-3372-9

1203
Index

- personal data  5 124
- Storage of data  18
- safe  18
- "Streisand effect"  19 11

Subject access  see Access, right of
Subject-matter and objectives (of GDPR)  1 1 et seq.
- anti-discrimination  1 31, 40
- automated (data processing)  1 12
- autonomy  1 29
- balancing  1 1, 20, 28 et seq., 34
- barrier to trade  1 42
- chilling effect  1 29
- citizen score  1 29
- competence  1 21, 23, 29, 33
- competition  1 21, 41, 43, 47
- competitive advantage  1 21
- conflict-of-laws rule  1 35
- conflicts of objectives  1 21, 25
- constitutional law  1 23
- controller(s)  1 3, 10, 30, 42, 46
- cultural diversity  1 40
- danger  1 12
- Data Protection Directive for Police and
  Criminal Justice Authorities  1 24
- data protection law  1 2 et seq., 6 et seq., 12,
  21 et seq., 24, 26 et seq., 30 et seq., 36, 39,
  42 et seq., 47
- data subject(s)  1 3 et seq., 10, 27, 33, 35
- deceased persons  1 39
- democracy  1 34
- digitization  1 4, 8 et seq.
- discretionary power  1 1
- ECHR  1 24, 38
- economic commodity  1 41, 47
- economy  1 6, 28, 40, 47
- enforcement  1 9, 11, 17
- ePrivacy Directive  1 6, 10
- ePrivacy Regulation  1 10, 24
- external effects  1 30
- fair trial  1 32, 34
- forum shopping  1 35
- free movement of data  1 5, 27, 32, 41, 45,
  47 et seq.
- freedom of assembly  1 32
- freedom of communication  1 40
- freedom of expression  1 32, 34, 40
- freedom of information  1 40
- freedom of religion and conscience  1 32
- fundamental principle  1 1 et seq., 16
- fundamental rights  1 15, 19, 28 et seq., 32,
  34 et seq., 49
- human being  1 12, 27
- implementation  1 15, 17, 33, 35, 43
- indeterminate legal term  1 1
- individual  1 3, 7, 21, 25, 27 et seq., 34, 40,
  42, 44, 48
- Information Law  1 8
- internal market  1 5, 17, 19 et seq., 25, 28, 33,
  35, 41 et seq., 44 et seq., 49
- interpretation aid  1 1
- legal persons  1 39
- level playing-field  1 21, 43
- margins of assessment  1 1 et seq.
- market freedom  1 41
- Member State(s)  1 1, 7, 11, 15 et seq., 23,
  33 et seq., 39, 42, 46, 48 et seq.
- nasciturus  1 39
- non-EU citizens  1 39
- object of protection  1 3, 5
- opening clause  1 1, 6 et seq., 10 et seq., 13,
  16, 18, 33, 48
- overall assessment  1 11
- precautionary interpretation  1 2
- precautionary principle  1 34
- priority of data protection  1 30
- privacy  1 3, 8, 15, 23, 28 et seq., 39 et seq.
- processor(s)  1 10, 34 et seq.
- profiling  1 6, 31
- public good  1 4, 35
- right to physical integrity  1 32
- right to respect for family and private life
  1 38
- risk  1 2, 4, 6, 12
- risk-based approach  1 2
- rivalry  1 4
- scope of application  1 6, 8, 10, 23
- sector-specific  1 6
- self-determination  1 30
- standard of protection  1 6
- supervisory authority/ies  1 25, 33
- technological neutrality  1 6
- technology  1 2, 4, 9 et seq., 12, 21, 34, 41
- technology law  1 2, 4, 12, 34
- telecommunications  1 6
- third countries  1 6, 45 et seq.
- transfer of data  1 6, 42, 45 et seq.

Submission  57 17, 58 24

Subordination
- situations  4(11) 26

Sub-processing  28 3

Sub-processors  4(8) 8, 28 14 et seq., 29 1

Substantial public interest  9 65

Sufficient guarantees provided by the processor
  28 12

Supervisory authorities  4(21) 1 et seq., 39 21,
  41 4 et seq., 51 1 et seq., 52 1 et seq.,
  53 1 et seq., 54 1 et seq., 55 1 et seq.,
  56 1 et seq., 14, 57 1 et seq., 58 1 et seq.,
  59 1 et seq.
- access to the premises  58 4, 11
- activities of the SA  53 10, 13, 59 6
- activity reports  59 1 et seq.
- addressees (of the activity report)  59 9
- adequacy decisions  45 53 et seq.
- administrative agreement  58 31
- administrative assistance  55 10, 57 9
- advisory activities  57 8, 11
- annual report  59 4, 6, 8
- another independent body  53 7
- appointment mechanism  53 5

1204

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

- appointment of the member or members
  53 2, 5 et seq., 54 10, 12
- authorisation and advisory powers
  58 1, 22 et seq.
- awareness raising
  57 13
- binding corporate rules
  58 32
- blocking period
  65 31
- catch-all clause
  57 16
- certification bodies
  57 15, 58 19, 27
- coherence procedure
  51 8, 55 12
- competence
  51 18, 53 12, 55 1 et seq., 56 3 et seq., 12, 57 1, 66 17
- competence and the judiciary
  55 13 et seq.
- competence for public tasks
  55 9 et seq.
- competent
  64 10
- competent authority
  64 4
- complete independence
  51 1, 17, 52 1, 3 et seq., 7 et seq., 26 et seq., 53 6, 54 5, 57 6, 59 1
- compliance with the GDPR
  4(21) 4, 51 17, 19, 58 5, 15
- confidentiality
  54 2, 4, 7, 17 et seq., 58 11
- conflicts of interest
  52 18 et seq.
- consistency mechanism
  51 7, 23, 52 2, 21, 56 18
- consistent application
  51 20 et seq.
- contractual clause
  57 15, 58 29 et seq.
- contrarius actus appointment
  53 12
- control/monitor mechanism
  51 4
- controller
  51 3, 22, 26, 52 20, 54 17, 55 4, 7, 9, 11 et seq., 56 1, 3, 5 et seq., 12 et seq., 16, 18, 57 11 et seq., 58 4, 6 et seq., 9 et seq., 13 et seq., 20, 23, 25 9 et seq.
- controller without an establishment in the EU
  55 11
- cooperation
  66 1 et seq.
- cooperation principle
  66 1
- corrective powers
  58 1, 12
- criminal judicial activities
  55 15
- cross-border processing
  55 1 et seq., 5, 7, 12, 56 1 et seq., 4 et seq., 7
- data protection audit
  58 7
- data protection board
  40 10
- data protection impact assessment
  57 13, 58 23
- decision, legal protection
  64 7
- decision, remedies
  64 7
- decision, unlawful
  64 7
- democratic legitimation
  53 7
- direct influence
  51 6, 52 12 et seq.
- discretion, urgency procedure
  66 16
- draft codes of conduct
  58 26
- duties of the members and employees
  52 20, 54 13
- effective supervision
  51 6
- enforcement
  51 20, 52 16, 21 et seq., 25, 54 1, 55 1, 56 13, 57 3, 8 et seq., 58 1, 6, 11
- erasure
  58 18
- establishment
  51 1, 5, 10, 13, 17, 22, 54 1 et seq., 55 4, 8, 11, 56 1, 3, 5 et seq., 10 et seq., 13, 18
- Europeanised SA
  51 19
- examination (of complaints)
  57 10
- excessive requests
  57 19
- exchange of information
  51 8, 57 9
- exclusive direction
  52 29, 31, 53 7
- external influence
  52 1, 6, 9 et seq., 25, 54 12
- extraordinary termination
  53 12
- final decision
  64 2
- financial independence
  52 21 et seq.
- financial oversight
  52 13, 16, 21 et seq.
- financial resources
  52 14, 21 et seq., 54 5, 59 10
- fines
  58 12, 20
- free flow of personal data
  4(21) 1, 51 18
- free to design the content (of activity report)
  59 7
- function (of activity report)
  59 1
- functional independence
  52 7 et seq.
- fundamental rights and freedoms
  4(21) 1, 51 18
- general conditions for the members of the supervisory authority
  52 7, 53 1 et seq.
- government
  52 8 et seq., 15, 19, 25, 30, 53 7, 11, 58 24, 59 9
- group of undertakings
  56 11
- head of state
  53 4, 7
- human resources
  52 23
- incompatibilities with other activities of the members and employees
  54 13
- incompatible occupations
  52 20, 53 7
- independence
  4(21) 4, 51 1, 4, 12, 15, 17, 21, 26, 52 1 et seq., 53 1 et seq., 6 et seq., 54 1 et seq., 5, 12, 14 et seq., 55 13 et seq., 57 5 et seq., 59 1, 10, 64 55, 65 1, 66 16
- independence, consistency mechanism
  64 24
- independency
  45 18 et seq.
- independent authority
  4(21) 1 et seq., 51 5, 57 5, 62
- independent public authorities
  51 17 et seq.
- independent state supervision
  51 11
- indirect influence
  51 6, 52 12 et seq., 17, 28
- interim measures
  45 34 et seq.
- International transfers
  45 33 et seq.
- investigation
  52 22, 55 4, 56 4, 57 8 et seq., 58 7, 10
- investigative powers
  58 1, 3, 5, 11
- issuing certification
  58 28
- job advertisement
  53 8
- joint controllership
  56 10
- judicial administration
  55 16
- judicial decision-making
  55 14
- judicial independence
  55 14
- judicial review
  51 4, 15, 52 2, 13, 16, 58 33
- Kooperationsprinzip
  66 17
- lead SA
  51 8, 14, 55 6, 9, 12, 56 1 et seq.
- legal basis
  57 2
- Legal enforcement in third countries
  27 30 et seq.
- legislative process
  4(21) 1, 53 4, 54 6, 55 6, 57 7, 59 5
- main establishment
  56 1, 3, 6, 8, 10 et seq.
- manifestly unfounded requests
  57 19
Index

- market location principle 55 11
- measures 64 10
- members (of the SA) 52 7, 10, 12 et seq., 29 et seq., 53 1 et seq., 5 et seq., 10 et seq., 54 1 et seq., 4, 6 et seq., 10 et seq., 17, 55 5, 17
- minimum list 57 3
- monitoring 4(21) 1, 4, 51 4, 11, 18, 52 4, 9, 54 8, 55 5, 57 3, 8 et seq., 58 1, 6
- national government 59 9
- national parliament 58 24, 59 9
- notice of an infringement 58 9
- obligation to cooperate 51 8, 20 et seq.
- one shop stop 51 4, 55 2, 6, 12, 56 1, 3, 10, 13, 18
- opening clause 57 4, 58 2, 4, 11, 24, 34 et seq.
- ordinary termination 53 11
- organisational independence 52 10, 27 et seq.
- parliament 52 25, 30, 53 7, 11, 58 24, 59 3, 9
- personal data breach 58 16
- personal independence 52 1, 7, 11, 14
- powers (of the SA) 58 1 et seq.
- principle of sincere cooperation 51 21
- prior consultation 58 23
- processing activities 55 10 et seq., 56 4, 6, 14
- processing by authorities or private bodies that act in the public interest 55 9
- processing carried out by courts 55 13
- processor 51 3, 52 20, 54 17, 55 4, 7, 11 et seq., 56 5 et seq., 12 et seq., 16, 57 11 et seq., 58 4, 6 et seq., 9 et seq., 13 et seq., 17, 20, 29 et seq.
- processor without an establishment in the EU 55 11
- professional secrecy 54 2, 4, 58 11
- prohibition of data processing 58 17
- provision of information 58 6
- public awareness 55 4, 59 2
- purpose (of activity report) 59 2
- qualifications 54 9
- qualifications, experience and skills 53 2, 10
- re-appointment 53 7, 54 12
- reasons for dismissal 53 2
- rectification 58 18
- register 64 53
- Regulation 45/2001 52 5 et seq., 53 3, 54 5, 55 5, 59 4
- removal from office 53 11
- reprimand 58 12 et seq.
- requirements for the appointment 53 3, 54 9
- requirements for the members of the SA 53 5
- resource allocation 59 2
- restriction of data processing 58 17
- review of issued certification 58 8
- safety guard 58 33
- sectoral differentiation 51 7
- separate, public, annual budget 52 24
- serious misconduct 53 12
- sole interlocutor 56 1, 16 et seq.
- sovereignty 55 7, 10, 56 3
- staff of the authority 52 29 et seq.
- standard data protection clause 58 29
- submission of complaints 57 17
- submission of opinion 58 24
- supervisory authority concerned 52 5, 56 14
- suspension of data flows 58 12, 21
- tasks (of SA) 57 1 et seq.
- technical resources 52 23
- term of office of the member or members 53 4 et seq., 11 et seq., 54 11
- termination of the employment relationship 53 9, 54 13, 16
- termination of the SA membership 53 2, 5, 11 et seq.
- termination of the term of office 53 5, 11
- territorial competence 55 6 et seq.
- territoriality 55 3, 7, 56 1
- third country 45 18 et seq.
- transparency 52 25, 53 8, 59 1 et seq., 6
- uniform application and enforcement 51 2, 8, 15, 55 1
- warning 58 9, 12 et seq.
- withdrawal of certification 58 19

Supervisory authority

- Competence when applying the market place principle 3 57

Supervisory authority concerned

- complaint 4(22) 1, 9 et seq.
- consistency mechanism 4(22) 1
- cooperation between the supervisory authorities 4(22) 1
- damage, loss or distress 4(22) 6
- dispute settlement procedure 65 26, 31
- established on the territory of the Member State of the supervisory authority 4(22) 1
- establishment of the controller or processor on the territory of the Member State of that supervisory authority 4(22) 3 et seq.
- habitual residence 4(22) 7
- lead supervisory authority 4(22) 1, 4
- main or single establishment 4(22) 4
- special categories of personal data 4(22) 6
- substantial impact on data subjects residing in the Member State of the supervisory authority 4(22) 5 et seq.
- substantially affected or likely to be substantially affected 4(22) 1
- urgency procedure 66 5, 13

Surveillance measures 45 15

Sweat pore patterns 4(14) 8

SWIFT 4(7) 42, 45 31

System design 5 134

System presets 25 41

Systematic monitoring 37 19

Tattoos 4(14) 9

Taxi service 4(8) 9

Technical and operational measures 24 33
Index

Technical and organisational measures  5 133, 20 9, 24 19, 25 24, 27, 29, 33, 44, 32 28 et seq.
   review and update  24 38
Technical resources  52 23
Technology neutral approach  32 4
Term of office of the member  54 11
Termination of the employment relationship  54 13, 16
Termination of the term of office  53 11
Territorial competence  55 7
Territorial scope
   – Authorities of third countries  3 2
   – Browser fingerprinting  3 51 et seqq.
   – Choice of law  3 62
   – Cloud computing  3 38
   – Convention 108  3 8
   – Cookies  3 51 et seqq.
   – Data subjects in third countries  3 15
   – Diplomatic missions and consular posts  3 58 et seqq.
   – DPD  3 5 et seq.
   – EEA states  3 61
   – Forum shopping  3 31
   – Health data  3 48
   – JHA Directive  3 8
   – Letterbox corporation  3 17
   – Market place principle  3 3 et seq., 32 et seqq.
   – Natural persons as a representative  3 19
   – Opening clauses  3 29
   – Principle of establishment  3 13 et seqq.
   – Problems of competence  3 30
   – Public authorities  3 2
   – Regulatory principles  3 1
   – Representatives of controllers and processors from third countries  3 17
   – Social Plug-Ins  3 51 et seqq.
   – Targeted advertising  3 52
   – Tracking  3 51 et seqq.
   – Transit of data  3 39
   – Websites  3 18
Territorial scope (of GDPR)  3 1 et seq., 55 3
   – authorities of third countries  3 2, 8
   – choice of law clauses  3 62
   – cloud computing  3 21, 46, 54
   – concept of behaviour  3 48
   – concept of establishment  3 2, 14, 19, 23
   – context of the activities of an establishment 3 4, 20 et seq.
   – contract  3 27, 47, 52, 54 et seqq., 62
   – controllers and processors in third countries 3 3 et seq., 32
   – cookies, social plug-ins, browser fingerprinting  3 52
   – data subjects who are in the Union 3 33 et seq.
   – diplomatic missions and consular posts  3 58
   – effective and real exercise of activity through stable arrangements  3 17, 19
   – existence of an establishment  3 13, 16 et seq.
   – forum shopping  3 31
   – free movement of goods  3 40
   – goods or services  3 6, 9, 42, 54
   – internal market  3 1, 4, 40 et seq.
   – Internet circumstances  3 43
   – length of stay  3 35
   – market place  3 1, 4 et seq., 14, 23, 32 et seq., 56
   – mobile stalls or trade fair stands  3 17, 43
   – monitoring of behaviour  3 26, 47 et seq.
   – national law  3 1, 5, 9, 31, 56
   – natural person(s)  3 14, 19, 51
   – no establishment in the Union  3 36 et seq.
   – offline context  3 50
   – parent company  3 22 et seq., 28 et seq.
   – payment  3 6, 41
   – physiological state  3 48
   – processing by public authorities  3 2
   – provider in the third country  3 44
   – public international law  3 1, 58 et seq.
   – representative  3 2, 7, 17, 23, 30, 43, 57
   – residence or the permanent address  3 19
   – small market place principle  3 56
   – substantive law  3 29, 31
   – supervisory authority  3 16, 28 et seq., 56 et seq.
   – technical processing  3 22
   – tracking  3 6, 51 et seq.
   – transfer to third countries  3 25, 27
   – transit of data  3 39
   – website  3 18 et seq., 44 et seq., 49, 51 et seq.
Terrorism financing  45 31, 90 6
   “Therapeutical privilege”  15 9, 23 27
Third countries
   – Enforcement  3 3
   – Market place principle  3 3 et seq.
Third country
   – Designation of a representative inside of the EU  27 7 et seqq.
   – Legal enforcement  27 30 et seq.
   – Market place principle  3 32 et seqq.
   – Territorial scope  3 32 et seqq.
Third country transfer  40 32
   – definition  44 21
   – Important reason of public interest  49 25
   – judicial proceedings  49 33
   – necessity  49 7
   – pre-contractual measures  49 20
   – public registers  49 41 et seq.
   – third-party beneficiary contracts  49 21
Third parties  4(1) 27, 4(10) 1 et seq., 10, 4(9) 7, 6(1)(f) 10, 53, 28 32
   – direct authority  4(10) 6 et seq.
   – disclosure  4(10) 4
   – legitimate interest  4(10) 1 et seq., 5, 8 et seq.
   – natural or legal person, public authority, agency or body  4(10) 5
   – other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data  4(10) 6 et seq.

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

- recipient 4(10) 2, 4, 9
- under the authority 4(10) 6
Threshold for joint controllership 24 16
Time limit 5 126 et seq., 41 12
- dispute settlement procedure 65 31
- opinion procedure 64 31
Timing of consent 4(11) 4
Tobacco consumption 4(15) 13
Tracking
- Territorial scope 3 51 et seq.
Trade secrets 13 10, 15 27, 20 12, 23 29, 33 10
Trade union membership 9 24
Traditional role 4(7) 41
Transatlantic data flows 45 37 et seq., 44
- Privacy Shield 45 39
Transfer
- definition 44 11
Transfer impact assessment 46 14
Transfer third countries 64 19 et seq.
Transfer to third countries 3 24 et seq., 54 et seq.
- cloud computing 44 11
- definition of transfer 44 11
- direct transfer by the data subject 44 15 et seq.
- employees 44 12
- encryption 44 11
- group of undertakings 44 12
- If GDPR applies according to Art. 3 para 2 3 7
- International agreements 48 9
- Internet 44 18 et seq.
- LED 44 3
- Lindqvist judgement 44 18 et seq.
- onward transfer 44 8, 27 et seq.
- pre-trial discovery 48 4
- processors 44 13
- production order 48 4
- rationale 44 4 et seq.
- rationale persons 44 21
- relation to Art. 3 GDPR 44 13 et seq.
- remote access 44 11
- Representatives of controllers and processors from third countries 27 4
- Transit 44 11
- transparency 44 26
Transfer to third country
- recipient subject to GDPR 44 13
Transfer tools 24 42
Transfers of personal data to third countries or international organisations 44 1 et seq., 18 et seq., 45 1 et seq., 46 1 et seq., 47 1 et seq., 48 1 et seq., 49 1 et seq., 50 1 et seq.
- accredited certification body 46 62
- action against the EU data exporter 46 20
- action of annulment 45 36
- additional requirements 44 1, 25
- alternative liability models 47 26
- anti-FISA clause 48 3
- approval 45 41, 46 15, 25, 27, 68, 47 2, 8 et seq., 13 et seq., 35, 48, 3, 49 35
- audit(e) 46 13, 42, 54, 47 3, 30
- automated individual decision-making 45 11
- balancing 44 7, 49 4, 6 et seq., 31, 45, 50
- balancing exception 49 4, 45
- balancing test 49 31
- binding corporate rules 46 25, 47 1 et seq.
- blanket consent 49 12
- breaches of contract 46 39
- Brexit 44 21, 45 3
- Brussels effect 44 8
- Canada 45 4, 29, 31
- civil law claims 49 35
- commercial interests 44 5
- company law 47 1, 13
- compensating the specific risks of the transfer 49 48
- compliance measures 49 28
- consent 44 17, 45 10, 46 11, 35, 55 et seq., 49 3, 8 et seq., 39
- constitutional underpinning 45 38
- continuing protection of personal data 44 8
- continuity of the level of data protection 44 6 et seq.
- contractual obligation 44 28, 46 41, 45, 58
- controller/processor in another third country 44 27, 48 6
- controller/processor in the EU 44 14, 16, 20, 45 26, 46 31, 57, 47 17, 26, 48 6
- convergence between the public interests of the third country and those of the EU or the Member State 49 29
- cooperation credits 49 28
- criminal proceedings 49 35
- data backup 46 8, 14, 39, 42, 45 et seq., 49
- data linked to data transferred from the EU 47 6
- data protection rules of the third country 45 8
- data transferred from the EU or the EEA 47 6
- derogations for specific situations 44 3, 49 1 et seq.
- diplomatic missions 44 21
- direct transfer 44 14, 29, 45 42, 47 5
- disclosure 44 11, 46 18, 54, 48 2, 4 et seq., 7
- EDPB 45 21, 46 18, 21, 28, 60, 62 et seq., 67 et seq., 49 16, 29
- effective judicial review 45 11, 40, 42, 46 46
- employee(s) 44 12, 45 11, 46 33, 47 11, 13 et seq., 23, 49 13, 18, 22
- essentially equivalent 44 2 et seq., 6 et seq., 45 6, 49 32
- establishment 44 12 et seq., 16, 46 4, 47 7, 48 10, 49 18, 33, 35
- exceptional character 49 45
- exceptions 44 3, 10, 45 15, 46 1, 48 9, 49 1 et seq., 6 et seq., 51

1208

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

explicit (consent) 46, 35, 49, 3, 9 et seq.
FISA 45, 41, 48, 3
follow-up marketing 49, 16
Fourth Amendment 45, 38, 42 et seq.
functional comparison 45, 6
general principle (for transfers) 44, 1 et seq.
governmental access 45, 14, 46, 9, 47, 7, 47
ground for transfer 46, 4, 60, 48, 1
group of undertakings 44, 12, 46, 4, 7, 30, 52, 47, 1, 3, 5 et seq., 13, 16 et seq., 19, 25 et seq., 28 et seq., 48, 6, 49, 17 et seq., 36
hierarchically organized groups of undertakings 47, 4
humanitarian organization 49, 40
implementing act 45, 3 et seq., 7, 21, 24, 28, 46, 60, 47, 35
independent sources and expert advice 45, 7
inform (SA or data subject) 45, 9, 46, 34 et seq., 63, 47, 27, 33, 48, 3, 49, 4, 11, 19, 49
information about specific risks 49, 11, 19
inspection(s) 46, 11, 54
instruments of international cooperation 48, 2
international agreements 44, 23 et seq., 46, 23, 48, 7, 9 et seq., 49, 29
international data transfers 46, 26
international organisations 44, 11, 21 et seq., 45, 3
International treaties 44, 23 et seq.
 intra-group agreement 46, 30, 47, 13
Japan 45, 3 et seq., 29 et seq.
joint economic activity 47, 3 et seq., 19, 26, 30
joint liability 46, 40
judicial review 44, 15, 45, 11, 16, 40, 42 et seq., 45, 44, 47, 11
jurisdiction 44, 21, 45, 42, 46, 9, 44, 59, 47, 25, 33, 48, 6
law enforcement 45, 32, 40, 42 et seq., 46, 54
law in action 45, 7
law in the books 45, 7
legal claim 48, 10, 49, 33 et seq.
legitimate interest 49, 4, 41 et seq., 47
level of data protection in the third country 44, 2, 45, 23, 46, 5, 49, 52, 47
level playing field 44, 5
liability 46, 33, 40 et seq., 53, 47, 25 et seq.
limited or repetitive (number of transfers) 49, 6
material content 46, 5
medical emergency 49, 40
merger 49, 35
monitoring 45, 1, 22 et seq., 30, 46, 42, 45, 65, 47, 28
multinational corporation 49, 18
Mutual Legal Assistance Treaties (MLAT) 48, 2, 9, 49, 30
national court(s) 45, 5, 33, 36, 46, 19
national security 45, 3, 17, 40, 48, 5, 49, 27
necessary for the performance of the contract 49, 16 et seq.
necessity test 49, 7, 16, 21, 31, 37
negotiation(s) 45, 6, 47, 3, 49, 4
notice (to SA) 46, 27
obligation to inform the competent SA 46, 63, 47, 33, 49, 4, 49
Ombudsman 45, 12
onward transfers 44, 11, 8, 27 et seq., 45, 12, 46, 5, 35, 47, 5, 22, 31, 49, 7, 48
outsourcing contracts 49, 23
PNR 44, 6, 23, 45, 31, 49, 13, 16
point of contact 46, 38, 47, 4, 17
power to suspend a transfer 45, 35
PPD-28 45, 40 et seq.
pre-formulated declaration of consent 49, 10
pre-trial discovery 48, 4, 49, 34, 38
primary responsibility of the data exporter 47, 33
PRISM program 45, 41
Privacy Shield 45, 4, 7, 37, 39 et seq.
private entity(ies) 44, 3, 49, 26, 30
processors located in a third country 44, 13
prohibit the transfer of certain categories of data to third countries 49, 5, 51
public authority(ies) 44, 3, 45, 15, 46, 3, 23, 69, 49, 3, 13, 15, 26, 35
public interest 46, 23, 48, 10, 49, 5, 25 et seq., 28 et seq., 51
purpose limitation 45, 10, 46, 34, 49, 48
real choice 49, 13
reasonable expectation of privacy 45, 38
recognizable and specific connection 49, 10
record of processing activities 49, 50
refuse an approval 46, 18
regulated self-regulation 47, 1
representation (of data subject) 46, 37
request for disclosure 48, 5
request for transfer 49, 30
responsibility 44, 9, 45, 1, 46, 45, 53, 47, 24, 30, 33, 49, 1
revision 46, 26
right of access 44, 26, 45, 9, 46, 36
risk of a transfer 44, 4
rule of law 45, 8, 14
SCC I 46, 31, 34 et seq., 37 et seq., 40, 42 et seq., 48 et seq., 51, 53
SCC II 46, 31, 33 et seq., 41 et seq., 48 et seq., 53
SCC Processor 46, 31, 50 et seq.
scientific or historical research or statistical purposes 49, 47
sectoral adequacy decisions 45, 37
sectoral legislation 45, 13, 38
self-certified 45, 37, 39
self-determination 49, 39
self-executing 46, 24
special categories of personal data 45, 11, 47, 22, 49, 9
Standard Contractual Clauses (SCC) 46, 9, 13, 26, 31, 33 et seq., 68, 47, 23
Index

- standing (to bring claim)  45 16, 36, 38, 42 et seq.
- state legislation  45 38
- strictly necessary  45 15, 41
- subprocessor  46 52, 55 et seq., 68
- subsidiary  47 24, 29, 49 6, 46
- suitable safeguards  49 48
- supervisory authority(ies)  44 4, 9, 15 et seq., 26, 28, 45 5, 18 et seq., 30, 33 et seq., 38, 46 3, 7, 10 et seq., 13, 15 et seq., 21 et seq., 24 et seq., 27 et seq., 31 et seq., 42 et seq., 47, 54, 59 et seq., 62 et seq., 68, 47 1 et seq., 6 et seq., 12, 16, 19, 26, 29 et seq., 48 3, 49 4, 28, 36, 49 et seq.
- supervisory body  46 59
- surveillance measures  44 11, 15, 45 15, 40 et seq., 46 14, 46, 47 33
- suspend or prohibit a transfer  46 18, 43, 47
- termination  46 16, 49
- territorial link  44 8, 47 17
- third countries  44 3 et seq., 8 et seq., 11 et seq., 20 et seq., 26, 45 1, 6, 15, 17, 26, 30, 46 4, 10, 26, 45, 40, 47 9 et seq., 17, 20, 22, 30 et seq., 48 5, 49 5, 41, 45, 51 et seq.
- third parties beneficiary rights  47 15, 49 22
- transfer within a company  46 29
- transferring data back to a controller in a third country  44 13
- transfers on the basis of an adequacy decision  45 1 et seq.
- transfers or disclosures not authorised by Union law  48 1 et seq.
- transfers subject to appropriate safeguards  46 1 et seq.
- transfers to other recipients  47 5
- transit  44 11, 13, 21, 45 41
- types of data  46 33, 47 31
- Umbrella Agreement  45 32, 42
- uniform data protection  46 4, 47 6
- unilateral assessment  45 6
- unilaterally constitutionalising international data flows  44 9
- unlawful access  45 11, 15
- update description of transfer  46 48
- US courts  45 42, 49 38
- validity of adequacy decision  45 5
- weak spot  45 40, 46 63
- website  44 14, 17 et seq., 45 28
- without detriment  49 13

Transfers to the EU  44 20

Transit of data
- Territorial scope  3 39

Transparency  53, 6(1)(f) 51, 12 1 et seq., 14 6, 16, 15 2, 20 1, 23 31, 38, 24 32, 33 1, 34 1, 43 14, 45 9, 89 15
- lawful processing  88 31 et seq.

Transparency interests  86 3

Transparent information, communication and modalities for the exercise of the rights of the data subject  12 1 et seq.
- accessibility  12 10

- artificial intelligence  12 9
- blind data subject  12 10
- by electronic means  12 15
- case of faulty drafting  12 17, 25
- children  12 12, 29
- clear and plain language  12 7, 9, 12
- cognitive overload  12 9
- comprehensibility  12 27
- concise, transparent, intelligible and easily accessible form  12 9
- conditions for the lawful processing
  - (information and transparency)  12 4
- costs of transparency  12 21
- DPD  12 7, 18, 26
- duties of the controller  12 2, 9 et seq.
- excessive (request)  12 8, 22 et seq.
- exemptions  12 22
- gratuitousness (principle of)  12 21 et seq.
- guidance and simple means of information  12 16
- identity theft  12 26
- in writing  12 14 et seq.
- inform the data subject (duty to)  12 9, 18, 20, 24
- informational self-determination  12 1, 3
- language  12 7, 9, 11 et seq., 27
- layered approach  12 9
- layered notices  12 15
- LED  12 6
- machine-readable  12 28
- manifestly unfounded (request)  12 8, 22 et seq.
- motivation  12 23
- orally  12 15
- profiling  12 9, 17, 19, 21, 25
- reasonable doubts  12 25 et seq.
- reasonable fee  12 22, 24
- refuse to act (on request)  12 17, 22, 24
- rights of the data subject  12 1 et seq., 5, 11, 18, 21, 23
- sanctions  12 26, 28
- sensor-based Smart City infrastructures  12 13
- standardization of symbols  12 30
- standardized icons  12 29 et seq.
- time-limit  12 18 et seq.
- transparency (principle of)  12 1
- video surveillance  12 27
- videoclips  12 28
- visualisation  12 27

Triad process  32 5, 88 11
- consistency mechanism  64 37
- dispute settlement procedure  65 22
- Trust  5 48
- disadvantage  5 31
- Two side markets  6 29

Umbrella agreement  45 32

Unambiguous consent  4(11) 59

Unborn life  4(1) 16

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.
Index

Undue delay 12 19, 16 3, 12 et seq., 19 5, 33 11
Uniform application and enforcement 55 1
United States 45 37 et seq.
  – adequacy 45 40
  – differences to the EU 45 38
  – judicial review 45 42 et seq.
  – Privacy Shield 45 39
  – right to privacy 45 38
  – surveillance laws 45 40 et seq.
  – Trans-Atlantic Data Privacy Framework 45 44
  – Umbrella Agreement 45 32
Unlawful access 45 11
Unlawful processing 18 12
Unlinkability
  – intervenability 5 135
Urgency procedure 66 1 et seq.
  – action for annulment 66 21
  – Anticipation of the main case 66 10
  – circumstance, exceptional 66 6
  – competence 66 5
  – deadline 66 18
  – decisions 66 18
  – discretion 66 11–16 et seq.
  – duration 66 12
  – duty to inform 66 14–19
  – EDPB 66 15
  – examples 66 8
  – history 66 2
  – legal consequence 66 9 et seq.
  – majority principle 66 18
  – measure, definitive 66 15
  – measures, interim 66 4 et seq., 9 et seq.
  – Non-active supervisory authorities 66 17
  – obligation to state reasons 66 15
  – opinion procedure 66 15, 18
  – preconditions 66 3 et seq.

– principle of territoriality 66 13
– proceeding(s) 66 18
– purposes 66 1
– remedies 66 21
– remedies, interim 66 21
– systematic 66 3
– the public 66 19
Urine and blood analysis 4(15) 7
Value judgments 16 10
Vein patterns 4(14) 8
Verification 4(14) 10
Video surveillance 6(1)(f) 3, 9 58, 12 27, 13 4,
  18 13, 15
  – intelligent 64 28
Violations 5 10
Virtual assistant 13 4
Vital interests 6 43 et seq., 9 48 et seq., 49 39
Voice samples 4(14) 8
Voluntarily appoint
  – DPO 37 30
Warning and reprimand 58 13
Way of walking 4(14) 8
Wearable device 13 4
Web archives 85 25
Websites
  – Territorial scope of the GDPR 3 18
Weight 4(15) 14
Whistleblower 14 7, 15, 15 18, 28, 23 26, 29 12
WiFi 12 14, 27
Wirtschaftsakademie case 4(7) 29, 26 36
Withdrawal of certification 58 19
Written and binding instrument 26 48

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.