

# The EU General Data Protection Regulation (GDPR): A Commentary

Lukas Feiler  
Nikolaus Forgó  
Michaela Weigl



**German Law Publishers**



# The EU General Data Protection Regulation (GDPR): A Commentary

Lukas Feiler  
Nikolaus Forgó  
Michaela Weigl



Globe Law  
and Business



**German Law Publishers**

## Authors

Lukas Feiler  
Nikolaus Forgó  
Michaela Weigl

## Managing director

Sian O'Neill

*The EU General Data Protection Regulation (GDPR): A Commentary*  
is published by

Globe Law and Business Ltd  
3 Mylor Close  
Horsell  
Woking  
Surrey GU21 4DD  
United Kingdom  
Tel: +44 20 3745 4770  
[www.globelawandbusiness.com](http://www.globelawandbusiness.com)

Printed by CPI Group (UK) Ltd, Croydon CR0 4YY

*The EU General Data Protection Regulation (GDPR): A Commentary*

ISBN 9781787421363  
EPUB ISBN 9781787421370  
Adobe PDF ISBN 9781787421387  
Mobi ISBN 9781787421394

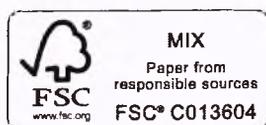
© 2018 Globe Law and Business Ltd except where otherwise indicated.

Text of the EU General Data Protection Regulations © European Union, 1998–2017,  
<http://eur-lex.europa.eu>.

All rights reserved. No part of this publication may be reproduced in any material form (including photocopying, storing in any medium by electronic means or transmitting) without the written permission of the copyright owner, except in accordance with the provisions of the Copyright, Designs and Patents Act 1988 or under terms of a licence issued by the Copyright Licensing Agency Ltd, 6–10 Kirby Street, London EC1N 8TS, United Kingdom ([www.cla.co.uk](http://www.cla.co.uk), email: [licence@cla.co.uk](mailto:licence@cla.co.uk)). Applications for the copyright owner's written permission to reproduce any part of this publication should be addressed to the publisher.

## DISCLAIMER

This publication is intended as a general guide only. The information and opinions which it contains are not intended to be a comprehensive study, nor to provide legal advice, and should not be treated as a substitute for legal advice concerning particular situations. Legal advice should always be sought before taking any action based on the information provided. The publishers bear no responsibility for any errors or omissions contained herein.



# Contents

---

<b>List of abbreviations</b> _____	9	<b>8. Information obligations and</b> _____	22
<b>List of Recitals of the General</b> _____	11	<b>privacy notices</b>	
<b>Data Protection Regulation</b>		<b>9. Rights of the data subject</b> _____	24
<b>Introduction to the General</b> _____	13	<b>10. Profiling and automated</b> _____	25
<b>Data Protection Regulation</b>		<b>individual decision-making</b>	
<b>1. Introduction</b> _____	13	<b>11. Data protection compliance</b> _____	26
<b>2. The most important</b> _____	13	<b>programme</b>	
<b>compliance steps until the</b>		11.1 <b>Organisational</b> _____	26
<b>GDPR applies from 25 May 2018</b>		<b>measures including data</b>	
<b>3. Basic terms of the GDPR</b> _____	14	<b>protection strategies</b>	
<b>4. The scope of the GDPR</b> _____	15	11.2 <b>Technical measures</b> _____	26
4.1 <b>Material scope – what</b> _____	15	<b>including privacy by</b>	
<b>processing activities are covered?</b>		<b>design and by default</b>	
4.2 <b>Personal scope – who</b> _____	15	<b>12. Maintaining a record of</b> _____	27
<b>does the GDPR apply to?</b>		<b>processing activities</b>	
4.3 <b>Territorial scope – where</b> _____	16	<b>13. Data protection impact</b> _____	28
<b>does the GDPR apply?</b>		<b>assessment and consultation</b>	
<b>5. The relationship with</b> _____	16	<b>obligation with supervisory</b>	
<b>national data protection laws</b>		<b>authority</b>	
<b>6. The principles relating to</b> _____	18	<b>14. Data protection officer</b> _____	29
<b>the processing of personal data</b>		<b>15. Data security</b> _____	30
<b>7. Legal basis requirement for</b> _____	19	15.1 <b>Mandatory data</b> _____	30
<b>any data processing activity</b>		<b>security measures</b>	
7.1 <b>Available legal bases</b> _____	19	15.2 <b>Obligation to notify</b> _____	31
7.2 <b>Requirements for valid</b> _____	20	<b>personal data breaches</b>	
<b>consent</b>		<b>16. Mandatory arrangements</b> _____	33
		<b>between joint controllers</b>	

17. Obligations in case of \_\_\_\_\_ 33  
outsourcing

18. International data transfers \_\_\_\_\_ 34

18.1 Transfers not subject \_\_\_\_\_ 35  
to notification or approval

18.2 Transfers subject to \_\_\_\_\_ 36  
notification

18.3 Transfers subject to \_\_\_\_\_ 36  
approval

19. International jurisdiction of \_\_\_\_\_ 36  
supervisory authorities

20. Administrative fines and \_\_\_\_\_ 38  
other sanctions

21. Civil liability and private \_\_\_\_\_ 40  
enforcement

**Text of the General Data \_\_\_\_\_ 41  
Protection Regulation and  
commentary**

**Chapter I – General provisions — 43**

Article 1 Subject-matter \_\_\_\_\_ 43  
and objectives

Article 2 Material scope \_\_\_\_\_ 47

Article 3 Territorial scope \_\_\_\_\_ 51

Article 4 Definitions \_\_\_\_\_ 55

**Chapter II – Principles \_\_\_\_\_ 73**

Article 5 Principles relating \_\_\_\_\_ 73  
to processing of personal  
data

Article 6 Lawfulness of \_\_\_\_\_ 79  
processing

Article 7 Conditions for \_\_\_\_\_ 87  
consent

Article 8 Conditions \_\_\_\_\_ 90  
applicable to child's  
consent in relation to  
information society  
services

Article 9 Processing of \_\_\_\_\_ 92  
special categories of  
personal data

Article 10 Processing of \_\_\_\_\_ 98  
personal data relating  
to criminal convictions  
and offences

Article 11 Processing which \_\_\_\_\_ 99  
does not require  
identification

**Chapter III – Rights of the \_\_\_\_\_ 101  
data subject**

**Section 1 – Transparency \_\_\_\_\_ 101  
and modalities**

Article 12 Transparent \_\_\_\_\_ 101  
information,  
communication and  
modalities for the  
exercise of the rights of  
the data subject

**Section 2 – Information and \_\_\_\_\_ 105  
access to personal data**

Article 13 Information to be \_\_\_\_\_ 105  
provided where personal  
data are collected from the  
data subject

Article 14 Information to be \_\_\_\_\_ 110  
provided where personal  
data have not been  
obtained from the  
data subject

Article 15 Right of access by \_\_\_\_\_ 115  
the data subject

**Section 3 – Rectification and \_\_\_\_\_ 118  
erasure**

Article 16 Right to \_\_\_\_\_ 118  
rectification

Article 17 Right to erasure \_\_\_\_\_ 119  
(‘right to be forgotten’)

Article 18 Right to restriction \_\_\_\_\_ 123  
of processing

Article 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	126	Article 33	Notification of a personal data breach to the supervisory authority	163
Article 20	Right to data portability	127	Article 34	Communication of a personal data breach to the data subject	166
<b>Section 4 – Right to object and automated individual decision-making</b>			<b>Section 3 – Data protection impact assessment and prior consultation</b>		
Article 21	Right to object	131	Article 35	Data protection impact assessment	169
Article 22	Automated individual decision-making, including profiling	134	Article 36	Prior consultation	177
<b>Section 5 – Restrictions</b>			<b>Section 4 – Data protection officer</b>		
Article 23	Restrictions	138	Article 37	Designation of the data protection officer	181
<b>Chapter IV – Controller and processor</b>			Article 38	Position of the data protection officer	187
<b>Section 1 General obligations</b>			Article 39	Tasks of the data protection officer	190
Article 24	Responsibility of the controller	141	<b>Section 5 – Codes of conduct and certification</b>		
Article 25	Data protection by design and by default	145	Article 40	Codes of conduct	192
Article 26	Joint controllers	147	Article 41	Monitoring of approved codes of conduct	196
Article 27	Representatives of controllers or processors not established in the Union	148	Article 42	Certification	198
Article 28	Processor	150	Article 43	Certification bodies	200
Article 29	Processing under the authority of the controller or processor	154	<b>Chapter V – Transfers of personal data to third countries or international organisations</b>		
Article 30	Records of processing activities	155	Article 44	General principle for transfers	203
Article 31	Cooperation with the supervisory authority	158	Article 45	Transfers on the basis of an adequacy decision	205
<b>Section 2 – Security of personal data</b>			Article 46	Transfers subject to appropriate safeguards	210
Article 32	Security of processing	159	Article 47	Binding corporate rules	214

Article 48	Transfers or disclosures not authorised by Union law	217	Article 62	Joint operations of supervisory authorities	254
Article 49	Derogations for specific situations	218	<b>Section 2 – Consistency</b>		<b>256</b>
Article 50	International cooperation for the protection of personal data	223	Article 63	Consistency mechanism	256
<b>Chapter VI – Independent supervisory authorities</b>		<b>225</b>	Article 64	Opinion of the Board	257
<b>Section 1 – Independent status</b>		<b>225</b>	Article 65	Dispute resolution by the Board	260
Article 51	Supervisory authority	225	Article 66	Urgency procedure	264
Article 52	Independence	227	Article 67	Exchange of information	266
Article 53	General conditions for the members of the supervisory authority	229	<b>Section 3 – European data protection board</b>		<b>267</b>
Article 54	Rules on the establishment of the supervisory authority	231	Article 68	European Data Protection Board	267
<b>Section 2 – Competence, tasks and powers</b>		<b>232</b>	Article 69	Independence	268
Article 55	Competence	232	Article 70	Tasks of the Board	269
Article 56	Competence of the lead supervisory authority	234	Article 71	Reports	272
Article 57	Tasks	241	Article 72	Procedure	273
Article 58	Powers	244	Article 73	Chair	274
Article 59	Activity reports	247	Article 74	Tasks of the Chair	275
<b>Chapter VII – Cooperation and consistency</b>		<b>249</b>	Article 75	Secretariat	276
<b>Section 1 – Cooperation</b>		<b>249</b>	Article 76	Confidentiality	278
Article 60	Cooperation between the lead supervisory authority and the other supervisory authorities concerned	249	<b>Chapter VIII – Remedies, liability and penalties</b>		<b>279</b>
Article 61	Mutual assistance	252	Article 77	Right to lodge a complaint with a supervisory authority	279
			Article 78	Right to an effective judicial remedy against a supervisory authority	281
			Article 79	Right to an effective judicial remedy against a controller or processor	283
			Article 80	Representation of data subjects	285
			Article 81	Suspension of proceedings	287

Article 82	Right to compensation and liability	289	<b>Chapter XI – Final provisions</b>	319
Article 83	General conditions for imposing administrative fines	292	Article 94	Repeal of Directive 95/46/EC
Article 84	Penalties	298	Article 95	Relationship with Directive 2002/58/EC
<b>Chapter IX – Provisions relating to specific processing situations</b>		299	Article 96	Relationship with previously concluded Agreements
Article 85	Processing and freedom of expression and information	299	Article 97	Commission reports
Article 86	Processing and public access to official documents	301	Article 98	Review of other Union legal acts on data protection
Article 87	Processing of the national identification number	303	Article 99	Entry into force and application
Article 88	Processing in the context of employment	304	<b>Keyword index</b>	327
Article 89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	306	<b>About the authors</b>	333
Article 90	Obligations of secrecy	311		
Article 91	Existing data protection rules of churches and religious associations	312		
<b>Chapter X – Delegated acts and implementing acts</b>		313		
Article 92	Exercise of the delegation	313		
Article 93	Committee procedure	318		

Biblioteka Główna  
Akademii Sztuki Wojennej

26673/III (CB)



03-026673-000-0

# The EU General Data Protection Regulation (GDPR): A Commentary

Lukas Feiler, Nikolaus Forgó and Michaela Weigl

From May 2018, the General Data Protection Regulation 2016/679 (GDPR) replaces the Data Protection Directive 95/46/EC, representing a significant overhaul of data protection law in the European Union. Applicable to all EU Member States, the GDPR's relevance spans not only organisations operating within the EU, but also those operating outside the EU.

This commentary, published in association with German Law Publishers, provides a detailed look at the individual articles of the GDPR and is an essential resource aimed at helping legal practitioners prepare for compliance.

Content includes:

- full text of the GDPR's articles and recitals;
- article-by-article commentary explaining the individual provisions and elements of each article;
- a general introduction to data protection law with a focus on issues such as:
  - how to adapt a compliance management programme;
  - whether or not to appoint a data protection officer;
  - 'privacy by design' and 'privacy by default';
  - the consequences of non-compliance with the GDPR;
  - data portability; and
  - the need for data protection impact assessments
- a detailed index.

In addition to lawyers and in-house counsel, this book is also suitable for law professors and students, and offers comprehensive coverage of this increasingly important area of data protection legislation.



German Law Publishers

ISBN 978-1-787421-36-3

9 781787 421363 >