

River Publishers Series in Security and Digital Forensics

# GDPR and Cyber Security for Business Information Systems

ANTONI GOBEO  
CONNOR FOWLER  
WILLIAM J. BUCHANAN



River Publishers







---

# GDPR and Cyber Security for Business Information Systems

---

# **RIVER PUBLISHERS SERIES IN SECURITY AND DIGITAL FORENSICS**

---

*Series Editors:*

**WILLIAM J. BUCHANAN**

*Edinburgh Napier University, UK*

**ANAND R. PRASAD**

*NEC, Japan*

Indexing: all books published in this series are submitted to the Web of Science Book Citation Index (BkCI), to CrossRef and to Google Scholar.

The “River Publishers Series in Security and Digital Forensics” is a series of comprehensive academic and professional books which focus on the theory and applications of Cyber Security, including Data Security, Mobile and Network Security, Cryptography and Digital Forensics. Topics in Prevention and Threat Management are also included in the scope of the book series, as are general business Standards in this domain.

Books published in the series include research monographs, edited volumes, handbooks and textbooks. The books provide professionals, researchers, educators, and advanced students in the field with an invaluable insight into the latest research and developments.

Topics covered in the series include, but are by no means restricted to the following:

- Cyber Security
- Digital Forensics
- Cryptography
- Blockchain
- IoT Security
- Network Security
- Mobile Security
- Data and App Security
- Threat Management
- Standardization
- Privacy
- Software Security
- Hardware Security

For a list of other books in this series, visit [www.riverpublishers.com](http://www.riverpublishers.com)

---

# GDPR and Cyber Security for Business Information Systems

---

**Antoni Gobeo**

Edinburgh Napier University, UK

**Connor Fowler**

Edinburgh Napier University, UK

**William J. Buchanan**

Edinburgh Napier University, UK



**River Publishers**

*Published, sold and distributed by:*

River Publishers  
Alsbjergvej 10  
9260 Gistrup  
Denmark

River Publishers  
Lange Geer 44  
2611 PW Delft  
The Netherlands

Tel.: +45369953197  
[www.riverpublishers.com](http://www.riverpublishers.com)

ISBN: 978-87-93609-13-6 (Hardback)  
978-87-93609-12-9 (Ebook)

© 2018 River Publishers

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

---

# Contents

---

<b>Preface</b>	<b>xi</b>
<b>Acknowledgements</b>	<b>xiii</b>
<b>List of Figures</b>	<b>xv</b>
<b>List of Abbreviations</b>	<b>xvii</b>

## **PART ONE: INTRODUCTION**

<b>1</b>	<b>The GDPR Fundamentals</b>	<b>3</b>
	A Brief History of Data Collection and Data Protection.....	4
	The GDPR .....	5
	To Whom Does It Apply? .....	6
	Who Is Exempt?.....	6
	Personal Data: Why it's Worth Protecting .....	7
	The Privacy Argument .....	8
	The Economic Argument.....	11
	Consequences to Individuals of Data Misuse .....	12
	The Heart of the GDPR; The Six Principles.....	13
	The Six Lawful Bases .....	14
	The Rights of Natural Persons in the GDPR.....	22
	The Three Exceptions.....	28
	Chapter Review .....	30
	References .....	30
	Appendix .....	33
<b>2</b>	<b>Organisations, Institutions, and Roles</b>	<b>37</b>
	Introduction .....	38
	Quis Custodiet Ipsos Custodes?.....	38
	European Union .....	38

Duties of the EDPB .....	40
Supervisory Authorities .....	41
The ICO in Action .....	44
Organisations Under the GDPR .....	44
Public Authorities .....	44
Types of Public Authorities.....	45
NGO's and Charities.....	45
NGO's and Charities as Data Controllers.....	46
Institutions and Agencies.....	47
Court of Justice of the European Union .....	48
European Union Agency for Network and Information Security: ENISA .....	49
The United Kingdom.....	50
Government Communications Headquarters .....	50
The National Cyber Security Centre.....	53
The GCHQ Bude: GCHQ Composite Signals Organisation Morwenstow .....	53
Investigatory Powers Commissioner's Office.....	54
Investigatory Powers Tribunal .....	56
Chapter Review .....	58
References .....	58
Appendix .....	60
<b>3 Information Systems Management and the GDPR</b> .....	<b>69</b>
Introduction .....	70
Information Systems in Organisations .....	71
Processes and Essential Systems .....	72
Types of Information Systems .....	73
Information Management .....	75
What is IM .....	75
Stakeholders .....	75
Data Management through the Ages.....	76
Functions of Information Management .....	78
Information Systems Theory .....	79
Data Flow Mapping .....	82
Data Flow Mapping Techniques .....	84
Data Controller and Data Processor .....	86
Data Controller .....	87
Data Processor .....	87

Distinguishing the Difference Between the Data Controller and the Data Processor.....	88
Chapter Review .....	91
References .....	91
<b>4 Cyber Security and the GDPR</b>	<b>93</b>
Introduction .....	94
Cyber Security as a Function of Compliance .....	95
Privacy .....	95
Protection.....	96
Process .....	98
Cyber Attacks .....	99
Malware .....	100
Social Engineering.....	103
Phishing .....	108
Countermeasures .....	110
Encryption.....	110
Chapter Review .....	114
References .....	114

**PART TWO: PREPARATORY STEPS**

<b>5 Data Protection by Design and Default</b>	<b>119</b>
Introduction .....	120
Data Protection is a Program; not a Project.....	120
What is Privacy? .....	121
Privacy and Protection by Design and Default.....	122
The Security Principle: Appropriate Technical and Organisational Measures .....	125
Organisational: A Corporate Culture of Data Protection.....	126
Staff Awareness of Security .....	127
Organisational Responsibility for Security.....	129
Technical Measures.....	129
Physical Security .....	129
Hardware Security .....	131
Computer Security: Design.....	132
Computer Security: Measures.....	133

Open Web Application Security Project (OWASP).....	135
Assessing Information Assets: Value and Risk.....	136
Information Classification and Labelling .....	137
Special Category Data: Sensitive and Very Sensitive	
Personal Data .....	138
Criminal Offence Data.....	138
Labelling of Data .....	138
Chapter Review .....	140
References .....	140
Appendix .....	143
<b>6 Protection Policies and Privacy Notices</b>	<b>145</b>
Introduction .....	146
Policy Framework: COBIT 5.....	147
COBIT 5: Principles, Policies and Frameworks in Depth .....	151
The Data Protection Policy .....	154
Policy Document Structure .....	155
Data Protection Privacy Notice.....	157
Types of Privacy Notices .....	159
Chapter Review .....	160
References .....	161
<b>7 DPO, DPIA, and DSAR</b>	<b>163</b>
Introduction .....	164
Data Protection Officer .....	164
Appointing a DPO .....	165
What Makes a good DPO?.....	167
Tasks of the DPO .....	168
Data Protection Impact Assessment .....	170
Legal Requirements .....	171
Defining Article 35 .....	173
Prior Consultation .....	175
Conducting a DPIA .....	176
Data Subject Access Request.....	178
How to access the data.....	179
The Organisations Role .....	180
Chapter Review .....	181
References .....	182
Appendix .....	183

**PART THREE: IMPLEMENTATION**

<b>8</b>	<b>International Standards; ISO's</b>	<b>189</b>
	The ISO.....	190
	4 Key Principles .....	190
	5 Year Review Process .....	191
	ISO as a Function of Compliance.....	191
	ISO 31000: Risk Management .....	191
	The Eight Principles .....	192
	Five Component Framework .....	193
	Six Stage Process.....	194
	ISO 27005: A Brief Visit.....	196
	ISO 8601: Representation of Dates and Times.....	196
	ISO 27000 Family – Information Security Management Systems... 198	
	ISMS: Information Security Management Systems .....	198
	ISO 27018: Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors .....	200
	ISO 27032: Guidelines for Cybersecurity .....	201
	ISO 9001 – Quality Management System.....	202
	Plan-Do-Check-Act Cycle .....	204
	Chapter Review .....	206
	References .....	206
<b>9</b>	<b>Security Incident Management</b>	<b>209</b>
	Introduction .....	210
	The GDPR Articles.....	210
	Computer Security Incident Response Team (CSIRT).....	211
	Incidence Response Plan (IRP) .....	213
	Incident Response Cycle.....	213
	Notification for a Personal Data Breach .....	224
	Data Breach Severity .....	225
	Breach Severity Rating and Risk .....	227
	ENISA Methodology .....	229
	Chapter Review .....	231
	References .....	232
	Appendix .....	233

<b>10 Valuing Security</b>	<b>235</b>
Valuing Security: Making the Business Case .....	236
Budgeting for IT and C-Suite .....	237
Budgeting .....	239
Mapping Out the Budget .....	242
Money Talks .....	244
Calculating the Annualised Loss Expectancy .....	244
Calculating the Return on Investment.....	245
Effective Communication .....	247
Email.....	249
Preparing a Presentation .....	251
Chapter Review .....	256
References .....	257
<b>Index</b>	<b>259</b>
<b>About the Authors</b>	<b>263</b>

# GDPR and Cyber Security Business Information Systems

Biblioteka Główna  
Akademii Sztuki Wojennej  
26777/III (CB)



00-026777-000-0

The General Data Protection

most stringent, regulations regarding Data Protection to be passed into law by the European Union. Fundamentally, it aims to protect the Rights and Freedoms of all the individuals included under its terms; ultimately the privacy and security of all our personal data. This requirement for protection extends globally, to all organisations, public and private, wherever personal data is held, processed, or transmitted within the EU.

Cyber Security is at the core of data protection and there is a heavy emphasis on the application of encryption and state of the art technology within the articles of the GDPR. This is considered to be a primary method in achieving compliance with the law. Understanding the overall use and scope of Cyber Security principles and tools allows for greater efficiency and more cost effective management of Information systems.

*GDPR and Cyber Security for Business Information Systems* is designed to present specific and practical information on the key areas of compliance with the GDPR relevant to Business Information Systems in a global context.

Key areas covered include:

- Principles and Rights within the GDPR
- Information Security
- Data Protection by Design and Default
- Policies and Procedures
- Encryption Methods
- Incident Response and Management
- Data Breaches

ISBN 978-87-93609-13-6



9 788793 609136



**River Publishers**