



GDPR

How to Achieve and Maintain Compliance

Andrew Denley,
Mark Foulsham
and Brian Hitchen

GDPR – How to Achieve and Maintain Compliance

Following the implementation of the new General Data Protection Regulation on 25 May 2018, organizations should now be fully compliant with their national interpretation of this far-reaching data protection standard. The reality is that most are not; whether through their inappropriate use of online cookies or ineffective physical data security, businesses continue to struggle with the increasing pressure from regulators to apply the Regulation. Non-compliance is widely due to misinterpretation, lack of real-world thinking, and challenges in balancing costs against business practicalities.

This book provides insight into how to achieve effective compliance in a realistic, no-nonsense and efficient way. The authors have over 100 years' collective international experience in security, compliance and business disciplines and know what it takes to keep companies secure and in-line with regulators' demands. Whether your organization needs to swiftly adopt GDPR standards or apply them in "Business as Usual" this book provides a wide range of recommendations and explicit examples.

With the likelihood of high-profile penalties causing major reputational damage, this book explains how to reduce risk, run a remedial project, and take immediate steps towards mitigating gaps. Written in plain English, it provides an invaluable international reference for effective GDPR adoption.

Andrew Denley is a GDPR Compliance Consultant with 35 years' experience in the research, intelligence, government and commerce sectors in both technical and consultancy capacities. In recent years he has championed and implemented information security risk analysis and framework compliance for a number of commercial companies with considerable success. An ISO27001 Lead Auditor, he has been listed on the International Register for Certified Auditors.

Mark Foulsham is Chief Digital Officer at Scope, CEO of Surrey Innovations, and Director of CIO Connect, UK. He has experience spanning over 30 years in leading both business and technology disciplines within organizations and has supported businesses from the Financial Services, wider commercial sector, universities and social enterprises in achieving their GDPR compliance programmes.

Brian Hitchen is a GDPR Compliance Consultant and author with 30 years' experience working as an IT Security Manager for a number of financial services organizations. With an interest in cyber crime and the impact on small to medium businesses, Brian now writes to help companies better understand IT security, risks and issues, contingency planning and data analysis and plan what they need to do to counter the latest threats and deal with legislation.

GDPR – How to Achieve and Maintain Compliance

Andrew Denley, Mark Foulsham and
Brian Hitchen



First published 2019
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

© 2019 Andrew Denley, Mark Foulsham and Brian Hitchen

The right of Andrew Denley, Mark Foulsham and Brian Hitchen to be identified as authors of this work has been asserted by them in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data

A catalog record has been requested for this book

Visit the eResources: www.Routledge.com/9781138326170

ISBN: 978-1-138-32617-0 (hbk)

ISBN: 978-0-429-44997-0 (ebk)

Typeset in Bembo
by Integra Software Services Pvt. Ltd.



Printed in the United Kingdom
by Henry Ling Limited

Contents

<i>The Authors</i>	vi
<i>Acknowledgments</i>	viii
Introduction	1
Section 1: Does the GDPR apply to you?	7
Section 2: GDPR principles	15
Section 3: Key roles	19
Section 4: Rights of the data subject	26
Section 5: Your GDPR project	34
Section 6: Information security best practice	46
Section 7: Awareness	58
Section 8: Data handling and management	64
Section 9: Data breaches	83
Section 10: Your technology environment	90
Section 11: Assessing your suppliers	94
Section 12: Direct marketing	101
Section 13: Privacy Notice(s)	108
Section 14: The Regulation	117
Index	204

Following the implementation of the GDPR on 25 May 2018, organizations are facing a new interpretation of this far-reaching regulation. These are not; whether through technical challenges, physical data security, business continuity, or pressure from regulators to comply. The book is a response to misinterpretation, lack of real-world thinking, and a shortage of practical examples that address the challenges against business practicalities.

This book provides insight into how to achieve effective compliance in a no-nonsense and efficient way. The authors have over 100 years of combined experience in security, compliance and business disciplines. It is designed to keep companies secure and in-line with regulators' demands. Whether your organization needs to swiftly adopt GDPR standards or apply them in "Business as Usual" this book provides a wide range of recommendations and explicit examples.

With the likelihood of high-profile penalties causing major reputational damage, this book explains how to reduce risk, run a remedial project, and take immediate steps towards mitigating gaps. Written in plain English, it provides an invaluable international reference for effective GDPR adoption.

Andrew Denley is a GDPR Compliance Consultant with 35 years' experience in the research, intelligence, government and commerce sectors in both technical and consultancy capacities. In recent years he has championed and implemented information security risk analysis and framework compliance for a number of commercial companies with considerable success. An ISO27001 Lead Auditor, he has been listed on the International Register for Certified Auditors.

Mark Foulsham is Chief Digital Officer at Scope, CEO of Surrey Innovations, and Director of CIO Connect, UK. He has experience spanning over 30 years in leading both business and technology disciplines within organizations and has supported businesses from the Financial Services, wider commercial sector, universities and social enterprises in achieving their GDPR compliance programmes.

Brian Hitchen is a GDPR Compliance Consultant and author with 30 years' experience working as an IT Security Manager for a number of financial services organizations. With an interest in cyber crime and the impact on small to medium businesses, Brian now writes to help companies better understand IT security, risks and issues, contingency planning and data analysis and plan what they need to do to counter the latest threats and deal with legislation.

BUSINESS & MANAGEMENT

Cover image: © Shutterstock

 **Routledge**
Taylor & Francis Group
www.routledge.com

Routledge titles are available as eBook editions in a range of digital formats

Biblioteka Główna
Akademii Sztuki Wojennej

26721/III (CB)



03-026721-000-0

Czyt.
004.056

ISBN 978-1-138-32617-0

9 781138 326170