KEY GUIDES

Data Protection

for voluntary organisations

4th edition

Paul Ticher

dsc
directory of social change

What they said about the book...

'Protecting personal data of vulnerable and disadvantaged people and ensuring their rights is the undeniable responsibility of every non-profit organisation that supports them. If you feel out of your depth and worried that your organisation doesn't meet the mark, this book is the perfect place to start.

'Written in clear language and set in a meaningful context, this is the best translation of the hundreds of pages of data protection legislation as it applies to charitable organisations. A prodigious achievement on one of the most important and challenging legal responsibilities for our sector.'
Sian Basker, Co-Chief Executive, Data Orchard

'A detailed and methodical approach to data protection. This comprehensive guide is an accessible source of information filled with valid and relevant examples. I found it a particularly great help in getting to grips with specific areas, such as consent and contracts.'
Kirsty Cunningham, Head of Fundraising, St Martin-in-the-Fields Charity

'There are not many people within the charity sector who are specialists in data protection. Paul uses simple, straightforward language to cover all key aspects of this complex but vitally important subject. Brilliantly practical!'
Peter Dean, Director of Finance, Riding for the Disabled Association

'I have worked with Paul for many years now and I have always appreciated his ability to share his enthusiasm for this complex subject and how it applies to our sector. Written in a very understandable and user-friendly way, this book is truly accessible.'
Jeni Woods, Quality Manager, Grace Eyre Foundation

KEY GUIDES

Data Protection

for voluntary organisations

4th edition

Paul Ticher

dsc
directory of social change

Published by the Directory of Social Change (Registered Charity no. 800517 in England and Wales)

Office: Suite 103, 1 Old Hall Street, Liverpool L3 9HG

Visit www.dsc.org.uk to find out more about our books, subscription funding websites and training events. You can also sign up for e-newsletters so that you're always the first to hear about what's new.

The publisher welcomes suggestions and comments that will help to inform and improve future versions of this and all of our titles. Please give us your feedback by emailing publications@dsc.org.uk.

First published 2000
Second edition 2002
Third edition 2009
Fourth editions (print and digital) 2021

ISBN 978 1 78482 049 7 (print edition)
ISBN 978 1 78482 050 3 (digital edition)

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Cover and text design by Kate Griffith
Typeset by Marlinzo Services, Frome
Printed and bound in the UK by Page Bros, Norwich

Contents

About the series vi
About the Directory of Social Change vii
About the author viii
Acknowledgements ix
Foreword by Jon Baines x
Preface xi
Who this book is for xii
Why data protection? xiv
1 The key elements of the GDPR 1
2 Processing personal data 7
3 Who is the controller? 13
4 Engaging a data processor 19
5 Managing data protection 23
6 Determining your lawful basis for processing personal data 31
7 Special category data 39
8 The six data protection principles 49
9 Data protection principles 1 and 2: lawfulness, fairness and transparency, and purpose limitation 55
10 Data protection principles 3, 4 and 5: data minimisation, accuracy and storage limitation 65
11 Data protection principle 6: integrity and confidentiality 73
12 Transferring personal data abroad 83
13 Data subjects and their rights 87
14 Right of access by data subjects 95
15 Confidentiality 101
16 Working in collaboration with other organisations 107
17 Data protection in service delivery 111
18 Data protection in direct marketing (including fundraising) 119
19 Data protection in HR and volunteer management 131
20 Data protection in IT 141
21 Archiving, research and statistics 147
22 Role and powers of the Information Commissioner's Office 151
Appendix 159
References and notes 165
Index 171

About the series

This series of key guides is designed for people involved with not-for-profit organisations of any size, no matter how you define your organisation – voluntary, community, non-governmental or social enterprise. All the titles offer practical, comprehensive, yet accessible advice to enable readers to get the most out of their roles and responsibilities.

There are several other titles available in this series, you can find details about the whole range at www.dsc.org.uk/publication/key-guides.

For further information, please contact the Directory of Social Change (see page vii for details).

About the Directory of Social Change

At the Directory of Social Change (DSC), we believe that the world is made better by people coming together to serve their communities and each other. For us, an independent voluntary sector is at the heart of that social change and we exist to support charities, voluntary organisations and community groups in the work they do. Our role is to:

- **provide practical information** on a range of topics from fundraising to project management in both our printed publications and e-books;
- **offer training** through public courses, events and in-house services;
- **research funders** and maintain a subscription database, *Funds Online*, with details on funding from grant-making charities, companies and government sources;
- **offer bespoke research** to voluntary sector organisations in order to evaluate projects, identify new opportunities and help make sense of existing data;
- **stimulate debate and campaign** on key issues that affect the voluntary sector, particularly to champion the concerns of smaller charities.

We are a registered charity ourselves but we self-fund most of our work. We charge for services, but cross-subsidise those which charities particularly need and cannot easily afford.

Visit our website **www.dsc.org.uk** to see how we can help you to help others and have a look at **www.fundsonline.org.uk** to see how DSC could improve your fundraising. Alternatively, drop us a line at **cs@dsc.org.uk**.

About the author

Paul Ticher's whole career has been in the voluntary sector, mostly as an independent consultant and trainer working with national and local organisations. After working for some years as a volunteer in Africa and then with the Campaign Against Arms Trade, his focus of interest became information management, including such areas as the use of information technology and the management of information services. This led to a considerable amount of work on the application of the Data Protection Act 1984 to voluntary organisations. He wrote the first edition of this book in 2000 to coincide with the Data Protection Act 1998 coming into force. Since then, Paul has been a leading trainer and writer on data protection throughout the UK, and he has provided bespoke advice to many voluntary organisations, large and small. For many years he has been recognised as one of the sector's go-to experts on data protection.

Paul's other books, published by the Directory of Social Change, include *Minute Taking* (with Lee Comer) and earlier editions of *Data Protection for voluntary organisations*. He also contributed the data protection appendix for *The Complete Fundraising Handbook* and published numerous articles and research reports into aspects of IT management in the voluntary sector.

Readers are invited to contact the author with comments, or to seek further help on the practical application of data protection in their organisation.

email: paul@paulticher.com

Acknowledgements

This book would not have been possible without the numerous challenging and stimulating discussions with my colleagues in voluntary organisations up and down the country over the last two decades and more. Only when they shared with me the issues they were facing did I really start to understand how data protection works – or should work – in practice, and I would like to thank every one of them for their contribution.

I am indebted to other professionals in the data protection field for providing insights, and often a second opinion, when I find myself struggling with an unfamiliar issue. In particular, I have benefitted immensely from contributions to the online JiscMail data protection discussion group.

For her thoughtful and assiduous attention to detail I am indebted to Hannah Lyons at the law firm Bates Wells who reviewed the text and provided helpful comments from a legal perspective. I would like to thank successive staff at Bates Wells and especially Lawrence Simanowitz for their support on previous editions of the book and also for work together on other projects.

The Directory of Social Change has not just given me the opportunity to get this book into print but also asked me to deliver face-to-face training on data protection for many years, which gave me insights into the issues facing a wide range of voluntary organisations, large and small.

Finally, of course, I want to thank my partner Gill Taylor for her personal and professional support. She has frequently been a valuable sounding board as well as posing the occasional challenging data protection question from her work as an HR consultant.

Every care has been taken to make sure that information in this book is as accurate and up to date as possible. Any mistakes or omissions are entirely my responsibility.

Foreword

Data protection is a fundamental right, and compliance is, therefore, not just a tick-box exercise. On the contrary, fair, accurate and transparent handling of personal data is essential to the functioning of society. As someone who has practiced in data protection matters for a number of years, I am continually impressed by the desire of most organisations to comply with the relevant regulations – to do the right thing. But I am also struck by the difficulties they face in finding sound advice (without incurring huge costs). The voluntary sector has been a prime example of this. When many in the sector were receiving criticism, and in some cases regulatory action, for data protection infringements around fundraising, it became clear that what seemed obvious to some practitioners was not widely known by many voluntary organisations.

The advent of the General Data Protection Regulation (GDPR) only intensified this imbalance between a desire to comply and the lack of support to do so. As much as one can rely on guidance from the Information Commissioner, it sometime lacks the detail and nuance that those working in specific sectors seek. And although the introduction of the GDPR led to any number of supposed experts appearing on the scene, that was not an unalloyed positive. Many of these 'experts' came from backgrounds ill-suited to the understanding of data protection law. Those of us, like Paul Ticher, who were around long before the GDPR and will remain around long after the hype (but not the impact) has faded away, are still having to help organisations overcome the effects of poor advice.

In this context, I am most reassured to see the latest edition of *Data Protection for voluntary organisations*. I know Paul as someone with a wealth of experience, both as an expert commentator and – crucially – as a practitioner. He knows the subject and he knows the specific challenges those working in voluntary organisations face. I particularly commend the book to those working in the sector but also recommend it more widely – it is a fine guide to data protection in general.

Jon Baines, Chair, National Association of Data Protection and Freedom of Information Officers and Senior Data Protection Specialist, Mishcon de Reya LLP

Preface

From what many would regard as rather shaky beginnings in 1984, data protection in the UK has gradually become a valuable and accepted consideration when data about individuals is collected and used. Voluntary organisations have generally been keen to accept the measures required by the legislation, recognising that the needs of the organisation have to be balanced against the interests of the people it engages with. At the same time, growing public awareness of individual rights and firmer expectations of how organisations are supposed to behave mean that organisations cannot afford – more than ever – to get data protection wrong.

When the General Data Protection Regulation (GDPR) was agreed in 2016, it heralded an exciting new era in the European Union's world-beating data protection regime. This regulation benefitted from substantial input from the UK, which had pioneered much of the thinking on the topic in the last few decades of the twentieth century.

The referendum decision for the UK to leave the European Union in 2017 raised questions which have not been fully resolved at the time of this book going to press. Although the UK's data protection legislation will continue with little practical change for most organisations in the short term, there is scope for greater change in the future, especially in the context of the UK's negotiation of trade deals around the world.

It is too soon to speculate how data protection regulations may develop and, as you read the book and apply it in your organisation, you should bear in mind that over time some of the details may well change. However, the GDPR brings the legislation up to date with current technology and practice, and provides a solid common basis for good practice. There is now so much international support for the underlying principles – both as law and as good practice – that it is highly likely that the current regulations will be the benchmark for recommended practice for the foreseeable future.

Who this book is for

Data protection is everyone's business. Whether we like it or not, data about us is captured almost every time we engage with an organisation, as customers, members, citizens or recipients of services, and most of us care about how our data is used and looked after.

The legal rules and obligations that apply to commercial organisations and public bodies also apply to voluntary organisations. This book uses the term 'voluntary organisations' to include charities, other not-for-profit organisations, clubs, societies and social enterprises. For these organisations, while the rules are the same, how they choose to comply and the issues they most often face can be somewhat different. For example:

- Voluntary organisations don't have the same powers and duties as public bodies but, unlike commercial organisations, they may have active members.
- Most will do fundraising.
- Their clients and beneficiaries may be particularly vulnerable.
- They may have loose collaborative arrangements with other voluntary organisations.
- They may have obligations towards their funders.

All these topics, along with the data protection basics, are covered in this book.

It goes without saying that voluntary organisations need to hold information about people. Almost everyone within an organisation is likely to handle this personal data in some way and therefore to have some responsibility for looking after it and using it appropriately. It is important to recognise that this includes not just paid staff but also volunteers, who, for example, may obtain information when they visit clients at home or handle Gift Aid declarations in the organisation's shop.

However, it is the organisation itself that carries the main legal responsibility, not any individual. For most people who handle personal data, it is enough to have a general understanding of what data protection involves and then to follow the policies and procedures of the organisation.

For others, data protection may be a significant proportion of their work – those in fundraising or marketing, for example, or those responsible for information security. And for many others, it will come into play as one element among many that affects their decision-making on policies, procedures and issues that arise from day to day. This includes the trustees, who are responsible for ensuring that their organisation complies with its legal obligations and may have to make key decisions about its approach to data protection compliance.

This book is especially relevant to you if you fall into any of these categories – in other words, if you are more deeply involved in making decisions about how your organisation discharges its data protection responsibilities.

As well as setting out the general principles behind data protection, this book therefore contains chapters that are particularly relevant to managers in the key areas where personal data is used in most voluntary organisations: service delivery (chapter 17), fundraising and marketing (chapter 18), HR (chapter 19) and IT (chapter 20).

The legislation discussed in this book is based substantially on the European Union's General Data Protection Regulation (GDPR), which applied directly in the UK from May 2018. The GDPR has now been adopted as domestic UK legislation, with slight modifications to reflect the UK's departure from the European Union. So, although the principles and much of the detail may well be relevant elsewhere, this book explicitly covers just the UK.

Why data protection?

Data protection is not about protecting *data* but about protecting *people*. It does, of course, involve protecting data, but only because of the potential harm we could cause to individuals if we did not handle their personal data properly.

Data protection can come over as terribly dry and procedural, but it goes to the heart of individual concerns, with potentially serious impacts on people's lives. If your GP transfers your records to a computer and the old paper files end up in a skip for anyone to see, that's a data protection issue. If your bank confuses you with someone else and your credit rating plummets, that's also a data protection issue. Data protection issues can adversely affect your life chances in many ways: inaccurate detrimental information provided in a job reference might prevent you getting a job; a faulty computer algorithm might deny you a loan that you need (see page 91 for more information). There have even been cases when people have suffered physical harm from a data protection breach, such as when their location was wrongly disclosed to someone who then assaulted or abducted them.

Fortunately, such extreme outcomes are rare. Your challenge in a voluntary organisation is to achieve the right balance: taking appropriate steps to prevent rare but potentially serious events, without imposing a regime which is so restrictive that it hampers the effective operation of the organisation.

The risks have increased significantly as computers have become ubiquitous, allowing large amounts of data to be stored, manipulated, shared and disclosed. Further opportunities for things to go seriously wrong arise from the growth of the internet, with its support for cloud computing, social media, online shopping and banking, and home automation systems. The spread of small, portable devices such as laptops, smartphones and memory sticks also increases risk.

As a result, the legislation has had to be progressively brought up to date. The UK's first data protection legislation was the Data Protection Act 1984, which was followed by a 1998 Act of the same name. The next development occurred when the European Union reached agreement in 2016 on the General Data Protection Regulation,[1] which is generally known as the GDPR and which came into force across the European Union (including the UK) in May 2018.

In the UK the GDPR is complemented by the Data Protection Act 2018 (DPA 2018), which also came into force in May 2018, and a number of other pieces of legislation. For more on the legal background, see the appendix. This book generally refers to the GDPR as shorthand for all of the relevant pieces of legislation. However, on occasion, it will draw your attention to specific provisions in the DPA 2018 or other UK legislation.

While the main concern of the GDPR is to prevent harm, close behind this comes the concept of 'fairness' – above all, being open and honest with people about how you are using data about them, and giving them choices about what you do with the data. For example, in some cases individuals can stop an organisation from using their data, or even require the organisation to erase it (sometimes known, in somewhat of an exaggeration, as 'the right to be forgotten').

The GDPR also offers genuine – and in some cases new – rights to 'data subjects' (the people about whom organisations hold data) and provides a framework for responsible behaviour by those using the data. It places great emphasis on accountability: your organisation must not just do the right thing, it must be able to show how it is doing so.

For voluntary organisations, openness and fairness are key to building relationships of trust with the wide range of people who are vital to the effective functioning of the organisation, including clients, beneficiaries, volunteers, donors and paid staff. This trust-building is not just desirable but essential. Good data protection practice can also demonstrate to funders and regulators that your organisation takes its responsibilities seriously.

Because of this, voluntary organisations have no reason to fear the GDPR. In many ways it gives legal backing to recognised good practice. Compliance with the GDPR can best be approached by understanding what it is trying to achieve, rather than seeing it as a series of legal hoops to be negotiated. You will find that compliance is very often a matter of judgement, not the application of detailed rules.

This book makes the assumption that you will be keen to follow best practice wherever possible. Indeed, it is often more onerous to make the effort to find technical loopholes. Grudging compliance is an option, of course, for those wishing to circumvent the spirit of the legislation. As with any law, there are grey areas and special cases that can be exploited to avoid giving people the maximum benefit of the law. Ignoring the legislation is increasingly not an option, however, as the Information Commissioner's Office (see chapter 22) has been given significantly increased enforcement

powers while individuals are coming to expect, and insist on, greater transparency and higher standards of compliance.

Note on legal terminology

EU legislation is structured as a set of 'recitals' which set out the intentions and rationale of the legislation, followed by numbered 'articles' that make the specific legal provisions. This book occasionally refers to the recitals in the General Data Protection Regulation (GDPR) where it is felt that they give insight into the meaning or purpose of the articles.

UK acts comprise numbered 'sections' (referred to as s.1, s.2 and so on in this book) supported by a series of 'schedules' that make additional provisions and go into specific matters in greater detail. The Data Protection Act 2018 (DPA 2018) is also divided into 'parts' and 'chapters'; however, you may find this confusing: the sections are numbered consecutively throughout, but the chapter numbering in each part restarts from Chapter 1. On those rare occasions when you might need to refer directly to the Act itself, it is essential to check that you are looking at the correct part of the legislation. (This is especially true in the cases of Parts 2, 3 and 4. Part 2 contains the rules that apply to most organisations (including voluntary ones), while Parts 3 and 4 apply very similar rules to law enforcement and the intelligence services respectively.) See page 161 in the appendix for further detail on the structure of the DPA 2018.

1 The key elements of the GDPR

The most important concepts in the General Data Protection Regulation (GDPR) relate to the two key pillars on which most of your data protection compliance rests: having a sound **lawful basis** for any processing that takes place and complying with the **six data protection principles** at all times. Before we look at these in detail, it is important to understand when data protection applies (and when it doesn't), and whose responsibility it is to ensure compliance. By covering these topics, this chapter therefore provides a guide to the main issues that will be addressed in more detail in the following chapters.

This chapter:

- briefly introduces key terminology and concepts;
- explains the obligation to have a lawful basis for all processing of personal data;
- outlines the six data protection principles;
- briefly lists some of the other key requirements;
- explains the role of the Information Commissioner's Office (ICO);
- indicates where in this book to find out more on each topic.

When does data protection apply?

Data protection applies whenever an organisation or its representatives 'process' 'personal data'. These are both technical terms that are explained below.

Personal data

The purpose of data protection is to protect people (or 'data subjects', as they are technically known). Information about a data subject is called 'personal data'. The individuals have to be 'identifiable' and the GDPR sets out a very broad definition of the factors that could make someone identifiable (see chapter 2).

Data protection only applies to information about living people. This is not stated in the GDPR, but it is made explicit in s.3(2) of the UK's Data Protection Act 2018.

Index

access *see also* data subject access requests (DSAR)
  authorised and unauthorised access to personal data 80–2, 115–16
  right of access by data subjects 88, 95–100
accountability 14–15, 26
accuracy principle 50–1, 65–9
advertising material 120–2 *see also* direct marketing
archiving, research and statistics
  anonymised or pseudonymised data 69, 116 148
  data retention special provision 69, 147
  data subject rights 149
  'in the public interest', meaning 149–50
  purpose limitation 62, 147
  special category data processing 47, 147–50

biometric data
  special category data processing 45, 135
breaches
  Charity Commission, reporting to 28
  data subjects, reporting to 28
  enforcement action by ICO 125–6
  ICO, reporting to 28, 144–5
  management procedures 144–5
  penalties 52, 74–5, 155
  reporting 27–9, 138–9, 144–5

charities
  annual fee to ICO 156
  ICO enforcement for fundraising failures 125–6
  trading companies linked to 128–9
Charity Commission
  reporting serious incident to 28
children
  age-appropriate code of practice 153
  authorisation on behalf of 113–15
  data subjects, as 87–8
  parental consent 88
  special category data processing 46
cloud providers 21–2
  security of applications 77–8
Code of Fundraising Practice 120, 124
compensation for data subjects 92, 155
complaints by data subjects 92

compliance
  breach 27–9
  data protection principles 52–3
  policies and procedures 26–7
  responsibility for 2–3
  role of manager 24–5
confidentiality 101–5 *see also* integrity and confidentiality principle
  data protection, interaction with 2, 101, 102
  duty to disclose overriding 102–3
  enforcement 105
  IT 142
  official requests for disclosure 103–4
  policy 104–5
  references 137
  service delivery 115–16
  volunteers 136
consent
  cookies 143–4
  data subjects 35–7, 125
  definition 35
  direct marketing 122
  explicit 40–1
  HR management 131–2
  processing personal data 32, 33, 35–7
  relationship with legitimate interests 37
  special category data 40–7, 147
contracts with processor 20–1
controllers 2–3, 13–17 *see also* joint controllers
  accountability 14–15
  contract with processors 20–1
  definition 13
  individuals as controllers 16–17
  reporting breaches to ICO 28
  responsibilities 14–15
cookies 143–4
copyright of database 82
counselling service
  parental consent 88
  special category data processing 46
criminal offence
  personal data breaches by individuals 154–5
  unauthorised access to personal data 81–2
criminal record data 40 *see also* special category data

criminal record data—*continued*
official requests for disclosure 104
Cyber Essentials 80

data minimisation principle 50–1, 65–9
data protection *see also* compliance; controllers; data protection principles; lawful bases; personal data; processing personal data
by design and by default 25–6
confidentiality, interaction with 2, 101, 102
history of the legislation xiv–xv, 159–63
management 23–9, 138–9
organisations working in collaboration 3, 15–16, 107–10
when applicable 1–2
Data Protection Act 1984 xiv, 159
Data Protection Act 1998 xiv, 159–60
Data Protection Act 2018 xv–xvi, 161–2
Data Protection (Charges and Information) Regulations 2018 156, 161
data protection officer 23–4
data protection principles 4–5, 49–82
accuracy 50–1, 65–9
data minimisation 50–1, 65–9
fairness 49–50, 55–61
integrity and confidentiality 51–2, 73–82, 102, 141–2
IT, application to 141–2
lawfulness 49–50, 55–61
purpose limitation 49–50, 62–3, 147
storage limitation 50–1, 69–71, 147
transparency 49–50, 51, 55–61
data quality 51, 66–9, 127
emails 67–8
HR management 133
service delivery 112
data retention 51, 69–71
archiving, research and statistics 69, 147
data subjects who have died 70–1
emails 69
HR management 133–4
legacies 70, 71
photographs 70
volunteers 136
data subject access requests (DSAR) 96–100, 139–40
exemptions 140
IT assistance 145
whether to redact information 99–100
data subjects 1, 7–8 *see also* children; right of access

data subjects—*continued*
authorisation by third party 113–15
automated decision-making, rights as to 91–2
compensation 92, 155
complaints 92
consent 35–7, 125
death of 70–1
exemptions to rights 92–3
more than one individual 10
opt-outs 34–5, 124–5, 127–8
portable format, right to receive data in 90–1
privacy notices 56–8, 60–1, 112
processing, rights on 90, 91
reasonable expectations 35, 63
rectification of information, right of 88–9
reporting breaches to 28
requests made on behalf of 92
rights for archiving, research and statistical purposes 149
secondary 10
special category data 39–47
vital interests 32, 42
database copyright 82
deletion *see* erasure of information
direct marketing 119–29
consent 122
definitions 120–2
draft ICO Code of Practice 119–21
ePrivacy Regulation (EU) 119, 122, 162
ethics 123
existing customers 127
Fundraising Preference Service (FPS) 119
lawful basis 122–4
opt out records 127–8
Privacy and Electronic Communications Regulations (PECR) 2003 119, 122, 151, 162
processing personal data 122–4
record-keeping 127–8
right to opt out 124–5
trading companies linked to charities 128–9
transparency 126–8
disability, persons with
special category data processing 45, 46–7
disclosure of information
confidentiality and duty to disclose 102–3
official requests 103–4

electronic data 9
emails
  data quality control 67–8
  marketing by 122–3
  response to data subject request for access 97–8, 139–40
  retention periods 69
  security 76
employees *see also* HR management
  data subject access requests (DSAR) 139–40
  privacy notices 138–9
  private use of employers' systems 138
  security checks and monitoring 79
  use of own equipment 137–8
ePrivacy Regulation (EU) 119, 122, 162
equal opportunities
  special category data processing 44, 135
equipment
  employees' use of own 137–8
erasure of information 10
  data subjects right to request 89
ethics
  direct marketing 123
ethnic diversity or origin
  special category data processing 44, 45
European Economic Area (EEA) 163
  transfers of personal data to 83–4
European Union (EU)
  Data Protection Directive 1995 159–60
  ePrivacy Regulation 119, 122, 162
  General Data Protection Regulation (GDPR) 2016 xi, xiii–xvi, 160–1
  leaving of UK xi, 163
  Privacy and Electronic Communications Regulations (PECR) 2003 119, 122, 151, 162
  transfers of personal data to 83–4
  transfers of personal data to US 86

fairness principle 49–50, 55–61
  right to opt out 124–5
fees to ICO 156
fundraising *see also* direct marketing
  Code of Fundraising Practice 120, 124
  enforcement action by ICO 125–6
  Fundraising Preference Service (FPS) 120

General Data Protection Regulation (GDPR) 2016 xi, xiii–xvi, 1–6, 160–1
  see also data protection principles; lawful bases
genetic data
  special category data processing 45

home-working *see* working from home
HR management 131–40
  confidentiality 135–6
  data quality 133
  data retention 133–4
  data subject access requests (DSAR) 139–40
  employees' use of own equipment 137–8
  equal opportunity monitoring 135
  lawful bases 131–2
  policies and procedures 138–9
  references 137
  reporting personal data breaches 138–9
  special category data 134–6
  third parties 136–7
  transparency 133
  volunteers 136

ICO *see* Information Commissioner's Office
identifiable individuals *see* data subjects
Information Commissioner 5, 151
  list of office holders 152
Information Commissioner's Office (ICO) 151–7
  assessment notices 154
  codes of practice 152–3
  contact details 157
  draft Direct Marketing Code of Practice 119–21
  enforcement action 125–6
  enforcement powers xv–xvi, 154
  fees and exemptions 156–7
  financial penalties 155
  guidance 153
  information notices 154
  reporting breaches to 28, 144–5
  warrants for entry and inspection 154
integrity and confidentiality principle 51–2, 73–82, 102
  IT, application to 141–2
intellectual property rights 82
international data transfers 83–6
  adequacy provision 83–4
  European Economic Area (EEA) 83–4
  European Union 83–4
  United States 86
international standards on security 79–80
IT *see also* online activity
  breach management 144–5
  confidentiality 142
  data protection principles applied to 141–2

IT—*continued*
external suppliers 142–3
integrity 141
monitoring and investigating usage 145
security 77–8, 141–3

joint controllers 3, 15–16, 107–10
data-sharing 128–9
statutory bodies, working with 110

lawful bases
contract 32
direct marketing 122–4
HR management 131–2
legal obligation 32
legitimate interests 33–5
processing personal data 3–4, 31–7, 55
public functions 33, 110
service delivery 111–12
vital interests 32
lawfulness principle 49–50, 55–61
legacies
data retention 70, 71
legitimate interests
lawful basis for processing 33–5
relationship with consent 37

marketing 120–2 *see also* direct marketing
email, by 122–3
fundraising failures by charities 125–6
meetings online 78
membership renewals 127
mental illness, persons with
special category data processing 46–7

online activity 7, 141–5 *see also* IT
age-appropriate code of practice 153
children 88
privacy notices 56, 60–1
security of meetings 78
security of service delivery 116
opt-outs 34–5, 124–5
record-keeping 127–8

paper records 9
security 76
parental consent 88
PECR *see* Privacy and Electronic Communications Regulations
penalties
fundraising failures by charities 125–6
ICO powers 155
security breach 52, 74–5
person, identifiable *see* data subjects
personal data *see also* controllers; data protection principles; data subjects; international data transfers; privacy notices; processing personal data; right of access; special category data
authorised and unauthorised access 80–2, 115–16
breaches 27–9, 138–9, 144–5
categories 7–8
definition 1–2, 7
domestic purposes exemption 10–11
identifiable person 1, 7–8
information-sharing 109–10
records about more than one individual 10
third parties, information from 60, 136–7
transparency 49–50, 51, 55–61, 133
photographs
retention period 70
policy document 26–7
confidentiality 104–5
retention policy and schedule 69
special category data 43–4
staff data protection 138–9
political parties
special category data processing 42
Privacy and Electronic Communications Regulations (PECR) 2003 119, 122, 151, 162
privacy notices 56–8
employees 138–9
fundraising transparency 126–8
notification of changes 61
providing the information 60–1
retention schedule appended to 69
service delivery 112
volunteers 136
processing personal data 7–11 *see also* data protection principles; lawful bases; special category data
automated 91–2
consent 32, 33, 35–7
contract lawful basis 32
data subject restricts or objects 90, 91
definition of processing 2, 9–10
direct marketing 122–4
lawful bases 3–4, 31–7, 55
legal obligation lawful basis 32
legitimate interests lawful basis 33–5
public functions lawful basis 33, 110
service delivery 111–12
vital interests lawful basis 32

processing personal data—*continued*
vital interests without data subject's consent 42
processors 3
cloud providers 21–2, 78
definition 19–20
IT suppliers 142–3
reporting breaches to controller 28
requirements in contracts for 20–1
profiling 126
promotional material 120–2 *see also* direct marketing
public bodies *see* statutory bodies
public interest *see also* substantial public interest
definition 150
purpose limitation principle 49–50, 62–3, 147
compatibility issue 62–3

quality of data *see* data quality

racial diversity or origin
special category data processing 44, 45
reasonable expectations 35, 63
record-keeping
data subject access requests (DSAR) 100
direct marketing 127–8
opt-outs 127–8
service delivery 115
records *see also* accountability; data retention; record-keeping
about more than one individual 10
paper 9
references
confidentiality 137
religious bodies
special category data processing 42
research *see* archiving, research and statistics
retention of data *see* data retention
right of access 88, 95–100 *see also* data subject access request (DSAR)

safeguards
archiving, research and statistics 47, 148
children 46
special categories of data 41–7, 148
security
authorised and unauthorised access to information 80–2, 115–16
breach 27, 52
cloud applications 77–8
data in transit, vulnerability of 52, 75–6
security—*continued*
emails 76
equipment 77
integrity and confidentiality principle 51–2, 73–82, 102, 141–2
IT 77–8, 141–3
paper documents 76
penalties for breaches 52, 74–5
physical 78–9
service delivery 115–16
staff checks and monitoring 79
standards 79–80
volunteers 116
website 77
working from home 77
self-employed people 17
sensitive data 4, 40 *see also* special category data
service delivery 111–17
authorisation on behalf of data subject 113–15
case studies and statistics, reporting of 116–17
confidentiality 115–16
data quality 112
lawful basis 111–12
privacy notices 112
records retention 115
security 115–16
special category data 112
third parties 112–15
transparency 112
sexual orientation
special category data processing 45
special category data 4, 39–47
archiving, research and statistics 47, 147–50
biometric data 45, 135
consent 40–7, 147
counselling service 46
disability or medical condition, persons with 45
equal opportunities 44, 135
ethnic diversity or origin 44
HR management 134–6
non-for-profit bodies 42
prevention or detection of unlawful acts 45
processing without consent 41–7
racial diversity or origin 44, 45
safeguarding of children 46
service delivery 112
substantial public interest 43–4, 110

special category data—*continued*
vital interests 42
statistics
data retention special provision 69, 147
purpose limitation 62, 147
service delivery 116–17
special category data processing 47, 147–50
statutory bodies
joint controllers with 110
public functions lawful basis for processing 33, 110
special category data processing 43–4, 110
storage limitation principle 50–1, 69–71, 147 *see also* data retention
subject access requests see data subject access requests (DSAR)
substantial public interest
special category data processing 43–4, 110

tax data
official requests for disclosure 104
telephone marketing 122
Telephone Preference Service (TPS) 122
telephone services 112
third parties
authorisation on behalf of data subject 113–15
personal data from 60, 136–7
service delivery 112–13
trade unions
special category data processing 42
trading companies
charities linked to 128–9
training on data protection 139
transparency
fundraising 126–8
HR management 133
principle 49–50, 51, 55–61
service delivery 112
third parties 60, 112–13

unincorporated organisations
compliance with the GDPR 13–14
United States (USA)
transfers of personal data to 86
unlawful acts, prevention or detection
special category data processing 45

vital interests
lawful basis for processing 32
special category data processing 42
voluntary organisations xii–xiii
annual fee to ICO 156
volunteers 17
agreements 136
security of personal data 116
training on data protection 139

websites 77
cookies 143–4
privacy notices 60–1
working from home 77

KEY GUIDES

Data Protection

Open, fair and well-managed data protection practice is not just desirable but essential if you want to ensure trust in your charity. Get it wrong and you risk reputational damage as well as financial penalties. This book will enable you to set a shining example of best practice by complying with UK data protection legislation and the General Data Protection Regulation (GDPR) in force since 2018. It will help you:

- Understand the key principles and elements of data protection
- Recognise your responsibilities as a data controller
- Distinguish when you need consent from individuals to hold and use their data (and when you don't)
- Ensure that your organisation's security measures are appropriate
- Appreciate what the rights of data subjects are

Invaluable to data managers or those who handle personal information such as IT, personnel, marketing and fundraising departments, this book is essential reading for anyone in the UK voluntary sector who wants to get beyond tick-box data management. For professional advisers and academics it also offers a valuable summary that draws out key data protection points by examining and interpreting the primary legislation.

'Written in accessible language and set in a meaningful context, this is the best translation of the hundreds of pages of data protection legislation as it applies to charitable organisations. A prodigious achievement on one of the most important and challenging legal responsibilities for our sector.'

Sian Basker, Co-Chief Executive, Data Orchard

'There are not many people within the charity sector who are specialists in data protection. Paul uses simple, straightforward language to cover all key aspects of this complex but vitally important subject. Brilliantly practical!'

Peter Dean, Director of Finance,
Riding for the Disabled Association

ISBN 978-1-78482-050-3

9 781784 820503

www.dsc.org.uk