EU GENERAL DATA PROTECTION REGULATION (GDPR)

AN IMPLEMENTATION AND COMPLIANCE GUIDE

IT GOVERNANCE PRIVACY TEAM

EU General Data Protection Regulation (GDPR)

An Implementation and Compliance Guide

IT GOVERNANCE TEAM

EXTRACT

IT Governance Publishing

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher or, in the case of reprographic reproduction, in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at the following address:

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

© IT Governance Team 2016

The author has asserted the rights of the author under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

First published in the United Kingdom in 2016
by IT Governance Publishing.

ISBN 978-1-84928-836-1

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

ABOUT THE AUTHOR

IT Governance is a leading global provider of IT governance, risk management and compliance expertise, and we pride ourselves on our ability to deliver a broad range of integrated, high-quality solutions that meet the real-world needs of our international client base.

Our privacy team, led by Alan Calder, Richard Campo and Adrian Ross, has substantial experience in privacy, data protection, compliance and information security. This experience, and our understanding of the background and drivers for the GDPR, are combined in this manual to provide the world's first guide to implementing the new data protection regulation.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

CONTENTS

Introduction 11
The purpose of the GDPR 12
Structure of the Regulation 13
Impact on the EU 14
Implementing the GDPR 15
Key definitions 18
Chapter 1: Privacy Compliance Frameworks 23
Material scope 27
Territorial scope 28
Governance 29
Objectives 32
Key processes 33
Personal information management systems 37
ISO/IEC 27001:2013 40
Selecting and implementing a compliance framework 47
Implementing the framework 49
Chapter 2: Role of the Data Protection Officer 52
Specification of the DPO 54
Duties of the DPO 56
The DPO and the organisation 61
The DPO and the supervisory authority 62
Data protection impact assessments and risk management 63
In house or contract 64
Chapter 3: Common Data Security Failures 66
Personal data breaches 68
Anatomy of a data breach 69
Sites of attack 70
Securing your information 71
ISO 27001 72

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Ten Steps to Cyber Security 73
Cyber Essentials.....74
NIST standards.....75
The information security policy.....76
Assuring information security.....77
Governance of information security 78
Information security beyond the organisation's borders 79
Chapter 4: Six Privacy Principles 81
Principle 1: Lawfulness, fairness and transparency.....83
Principle 2: Purpose limitation.....89
Principle 3: Data minimisation 90
Principle 4: Accuracy.....92
Principle 5: Storage limitation 94
Principle 6: Integrity and confidentiality 95
Accountability and compliance.....97
Chapter 5: Requirements for Data Protection Impact Assessments 102
Privacy impact assessments 104
When to conduct a DPIA 112
Who needs to be involved.....117
Privacy by design and by default 118
Chapter 6: Risk Management and DPIAs 122
DPIAs as part of risk management 123
Risk management standards and methodologies 123
Risk responses.....134
Risk relationships.....137
Chapter 7: Data Mapping 139
Objectives and outcomes 140
Four elements of data flow 141
Data mapping, DPIAs and risk management.....142
Chapter 8: Conducting DPIAs.....149
When to conduct a DPIA 150
Objectives and outcomes 151

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Consultation 154
Five key stages of the DPIA 156
Integrating the DPIA into the project plan 165
Chapter 9: Data Subjects' Rights 168
The right to information 169
The right to access 171
The right to rectification 172
The right to be forgotten 173
The right to restriction of processing 176
The right to notification 178
The right to data portability 179
The right to object 181
The right to appropriate decision making 182
Chapter 10: Consent 184
Consent in a nutshell 185
Withdrawing consent 188
When consent isn't necessary 189
Practicalities of consent 190
Children 193
Special categories of personal data 196
Data relating to criminal convictions and offences 196
Chapter 11: Subject Access Requests 198
The information to provide 199
Data portability 201
Responsibilities of the data controller 202
Processes and procedures 203
Options for confirming the requester's identity 205
Records to examine 208
Time and money 209
Dealing with bulk subject access requests 210
Right to refusal 211
Chapter 12: Controllers and Processors 212
Data controllers 212

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Joint controllers 214
Data processors 215
Controllers that are processors 216
Controllers and processors outside the EU 217
Records of processing 219
Demonstrating compliance 223
Chapter 13: Managing Personal Data Internationally 226
Key requirements 227
Adequacy decisions 229
Safeguards 231
Binding corporate rules 233
The EU-US Privacy Shield 234
Privacy Shield Principles 236
Limited transfers 238
Cloud services 239
Chapter 14: Incident Response Management and Reporting 242
Notification 243
Events vs incidents 246
Types of incident 247
Cyber security incident response plans 248
Key roles in incident management 250
Prepare 251
Respond 252
Follow up 254
Chapter 15: GDPR Enforcement 257
The hierarchy of authorities 257
One-stop-shop mechanism 259
Duties of supervisory authorities 260
Powers of supervisory authorities 261
Duties and powers of the European Data Protection Board 262

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Data subjects' rights to redress 263
Administrative fines.....265
The Regulation's impact on other laws 268
Chapter 16: Transitioning and Demonstrating Compliance 271
Transition frameworks 271
Transition – understanding the changes from DPD to GDPR.....273
Using policies to demonstrate compliance 276
Codes of conduct and certification mechanisms.....281
Appendix 1: Index of the Regulation 283
Appendix 2: EU/EEA National Supervisory Authorities 290
ITG Resources.....291

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

INTRODUCTION

Due to be enforced from March 2018, the European Union's General Data Protection Regulation (GDPR) will require all data controllers and processors that handle the personal information of EU residents to "implement appropriate technical and organisational measures […] to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" or face fines of up to €20 million or 4% of annual global turnover – whichever is the greatest.

The GDPR is the latest step in the ongoing global recognition of the value and importance of personal information. Although the information economy has existed for some time, the real value of personal data has only become more recently evident. Cyber theft of personal data exposes EU citizens to significant personal risks. Big data analysis techniques enable organisations to track and predict individual behaviour, and can be deployed in automated decision-making. The combination of all these issues, together with the continuing advance of technology and concerns about the misuse of personal data by governments and corporations, has resulted in a new law passed by the EU to clarify the data rights of EU citizens and to ensure an appropriate level of EU-wide protection for personal data.

The GDPR applies across all the member states of the EU but its reach is far wider: any organisation anywhere in the world that provides services into the EU that involve processing the data of EU citizens will have to comply. This means that the GDPR is probably now the most significant data security law in the world. While it builds on the work of

EXTRACT

the EU's Data Protection Directive (DPD), the US's HIPAA and various other data protection regimes, the GDPR can be regarded as a distillation and comprehensive update of the EU's goals in protecting the rights and freedoms of the people who live within it.

The purpose of the GDPR

The DPD (Data Protection Directive) has been in place for twenty years; it sets a minimum standard for data protection law in EU member states. Many states have gone significantly further in terms of legislating to protect personally identifiable information (PII), and this has made it increasingly difficult for EU citizens to know how their rights are protected across the EU and for organisations to determine which set of laws they should comply with, particularly when trading across multiple member states.

The EU Commission therefore decided that a single, unified law would be a more effective way of achieving two key goals:

1. Protecting the rights, privacy and freedoms of natural persons in the EU.
2. Reducing barriers to business by facilitating the free movement of data throughout the EU.

In terms of EU legislation, a regulation is quite distinct from a directive, which is how data protection was previously handled under the DPD. While directives set minimum standards and then ask EU member states to provide their own legislation to meet those standards, regulations exist as laws themselves, superseding any relevant laws passed by member states.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

While member states are allowed to apply directives in whatever way suits each member, a regulation is applied consistently in all member states. If there is room for local variations, it is specifically identified in the text of the regulation. Regulations are, therefore, an effective mechanism for applying a consistent approach across 350 million people in 28 member states – and often beyond.

Structure of the Regulation

Appendix 1 of this manual provides a breakdown of the overall structure of the Regulation. The regulation itself can be downloaded, in all the official languages of the EU, from *http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf*. There is also a pocket guide to the EU GDPR, available from IT Governance Publishing[1], which gives an overview of the legislation.

The GDPR is divided into two broad sections, which is standard for EU directives and regulations. The first section comprises the recitals. The recitals essentially provide context, direction and oblique guidance so that the later explicit requirements can be better understood.

The second part of the Regulation comprises the articles. The articles set out the specific requirements with which those entities within the scope of the regulation have to comply. Not every article in the GDPR applies to every organisation – given that some articles are relevant only to the Commission, the Board or the supervisory authorities, it may

[1] *www.itgovernance.co.uk/shop/p-1830-eu-gdpr-a-pocket-guide.aspx*

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

actually be impossible for every article to apply to a single organisation. In many cases, only a few articles may be completely relevant.

In broad terms, Chapters VI, VII, X and XI of the GDPR talk primarily about the Commission and the supervisory authorities so, if you are using this manual to plan your GDPR compliance programme, you may not need to give extensive attention to those sections.

Impact on the EU

As an EU regulation, the GDPR operates above the level of other laws. It cannot be simply overturned or repealed by a single government or nation, nor can those governments or nations modify the legislated requirements to make compliance simpler or less effective. This is because it has already been agreed by representatives from all member states through the standard EU legislative process.

The GDPR asserts a number of rights for individuals in relation to their personal data, and these rights are set out in Chapter III of the Regulation. The protection of these rights naturally results in a number of obligations on the part of the organisations that collect, store and process that personal data. Data collectors and processors have to act in accordance with the GDPR in order to ensure that the fundamental data rights of individuals are protected. This is not a simple "if A then B" law, of course, and there are various conditions that protect businesses' rights to do business, as well as protecting public authorities' ability to serve the public.

On one hand, the Regulation appears to be disruptive. Every organisation in the EU has to comply with the law and that

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

means they will all need to review the impact of the Regulation on their operations to determine what changes have to be made and the extent to which spending on compliance needs to be increased; there will have to be significant changes to how most organisations collect, process and store personal data; and the GDPR is, of course, bolstered by the threat of punitive and "dissuasive" administrative fines. On the other hand, the Regulation is trying to tread a fine line between protecting the rights of the individual and removing barriers to the "free movement of personal data within the internal market". In other words, while the GDPR sets out specific restrictions on the use and storage of personal data, it does so in order to preserve the interests both of the EU's residents and the organisations that do business within it.

Organisations that act quickly to ensure compliance with the Regulation will be those that thrive in the evolving regulatory environment. Equally, some organisations will be able to make significant process improvements, as with standardised requirements for data protection, organisations can streamline their processes – particularly for pan-EU and Internet services operations – and significantly improve efficiency.

Implementing the GDPR

The prerequisites for implementing a complex compliance framework are knowledge and competence; the IBITGQ (*www.ibitgq.com*) EU GDPR Foundation and Practitioner qualifications are designed so that individuals can gain the skills and competence they need and this manual, the primary purpose of which is to help organisations tackle the GDPR,

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

is also the text book for the IBITGQ EU GDPR Practitioner qualification.

This manual explains how to achieve compliance with the Regulation and how to do so while minimising the impact of the necessary changes. In any compliance project, there are many instances where organisational processes must be structured to meet legal or regulatory requirements, and it is important to ensure that your organisation is able to do this cost-effectively and efficiently.

It is also important to understand that the GDPR will apply in varying measures to organisations *outside* the EU. Much as you are expected to abide by the laws of any country you live in, non-EU organisations that want to collect or process the personal data of European citizens will also need to abide by the Regulation. While compliance with the Regulation may be difficult for some organisations – typically smaller ones that have no other interest in the EU – simple supply-chain forces, and the explicit GDPR requirements around extra-territorial data processing will put compliance pressure on organisations that want to do business within the EU.

In fact, the only real way to avoid complying with the GDPR will be to avoid doing business with the EU entirely. Given that the EU is the largest trading bloc in the world, this would be impractical for any organisation that wants to take advantage of the Internet or works with modern global markets and supply chains.

This book does not lay out a one-size-fits-all framework for achieving GDPR compliance. Organisations operate in different ways, with different partners and suppliers, different business objectives and a variety of business models, and no single compliance framework is likely to work – or even be suitable as a general approach – for all

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

organisations in all parts of Europe or the world. Rather, this book provides information about the features of a compliance framework that are known to work in many organisations and which reflect the GDPR requirements. The manual identifies the specific requirements of the GDPR and provides analysis and recommendations for pragmatically and effectively achieving compliance.

Readers should, however, note that this manual does not cover every possible situation in which the GDPR might apply, nor does it deal with the compliance requirements in every sector and industry. It instead focuses on the core activities and issues that most GDPR compliance projects are going to have to face, and provides advice and guidance that is broadly applicable in most – but not all – circumstances.

Finally, it should be noted that this is a manual for implementing a GDPR compliance framework in an organisation; it is explicitly not a legal compliance manual and you will need specific legal advice on aspects of the GDPR, particularly in relation to contracts and other legal statements. Your legal advisers have an important role to play in your GDPR project, but most lawyers are not experts on cyber security, information assurance or business continuity, nor do they usually have expertise in organisational management. Direct their services to the maximum value of your GDPR compliance project and remember that GDPR compliance is much bigger and more important than legal documentation; the GDPR has to become part of the fabric of the organisation in much the same way as does Health and Safety, internal control or information security.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Key definitions

There are a number of key terms that are used throughout the manual, many of which have very specific definitions. These definitions all originate in the GDPR itself. There are four terms universally applied throughout the Regulation that need to be clearly understood from the outset.

Controller

> 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.[2]

The data controller is the organisation that determines the purpose for processing personal data and what processing will be done. Bear in mind that "processing", under the terms of the GDPR, includes collecting and storing information, so it's possible that an organisation may be accountable as a controller but not otherwise involved with the actual processing of personal data. A firm that hires a marketing agency to profile their customers, for instance, is unlikely to see any of the data other than the results, probably in some sort of opaque pie chart. Given that they determined the purpose for which the data was processed, however, they are

[2] GDPR, Article 4, Clause 7.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

the data controller and the marketing agency is the data processor[3].

Processor

> 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[4]

Data processors are organisations or entities that process personal information on behalf of a data controller. As noted above, "processing" is essentially anything done to the data, including storage. It is possible for an organisation to be both a controller and a processor.

Personal data

> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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.[5]

---

[3] This is true in the absence of any other factors. However, if the marketing agency is given leeway to determine the manner of processing, they may be joint controllers.

[4] GDPR, Article 4, Clause 8.

[5] GDPR, Article 4, Clause 1.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Personal data under the GDPR is a broad set of types of information about "an identified or identifiable natural person". This means that the information is *not* personal data if there is no way to link it to a person. Personal data is anything that could be linked in any way to the data subject, so organisations will need to be careful about how information is gathered and used, as it may be possible to accidentally gather sufficient information to remove the anonymity of the subject. Note that the definition now specifically includes biometric, genetic and health information, as well as online identifiers that can be used to identify a person. The GDPR does not extend any rights to deceased persons.

Supervisory authority

> 'Supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51.[6]

The supervisory authority is the governmental organisation in each member state that will be responsible for enforcement of the GDPR. Your organisation may need to interact with the supervisory authority on a number of occasions, so it's worth making sure you know who that will be (in the UK, for instance, it's the Information Commissioner's Office, while in France it is the Commission Nationale de l'Informatique et des Libertés, and so on). There

[6] GDPR, Article 4, Clause 21.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

is a full list of the current EU national supervisory authorities in Appendix 2.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

CHAPTER 1: PRIVACY COMPLIANCE FRAMEWORKS

The first few steps of your compliance project can be the most confusing. Where do you start? Who needs to be involved? How do you go about identifying and meeting all of your obligations? How will you prove that you're meeting all of the Regulation's requirements?

Such questions can distract you from the project's core requirements and make the entire process seem incredibly daunting.

For most organisations, a simple approach may be to ignore the specific, detailed requirements of the GDPR for now, and start instead by building a framework to ensure compliance both now and in the years ahead. The GDPR has a specific requirement that controllers should, "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, […] implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary"[7].

This clause is, in effect, saying that organisations should put in place a compliance framework which ensures they are implementing appropriate technical and organisational

[7] GDPR Article 24 (1).

EXTRACT

measures to ensure that data processing is performed in compliance with the GDPR.

A "compliance framework" is a structured set of guidelines and practices that bring together the regulatory compliance requirements that apply to an organisation, and the business processes, policies and controls that are necessary in order to meet these requirements. Technical measures include specific procedures, as well as staff training, audits and all the relevant technical and physical security controls that form part of an effective information security management system. These processes, policies and controls will generally outline how the organisation manages communication, risk and governance relevant to the compliance requirements. Because there will often be some overlap between different compliance requirements, the framework should identify this in order to eliminate redundancies and uncertainties.

All compliance frameworks have to include three categories of activity as illustrated in Figure 1: people, process and technology.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

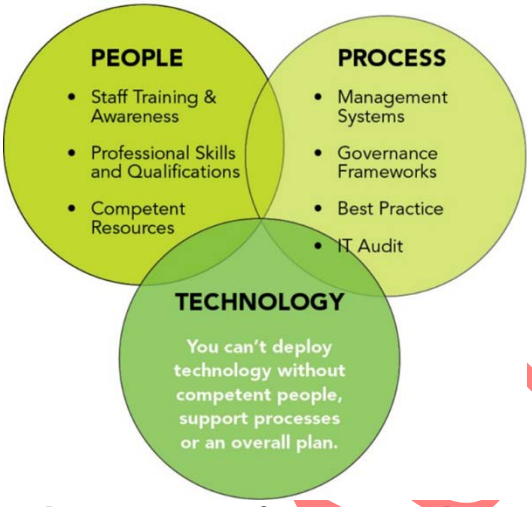

Figure 1: Three categories of activity: people, process and technology

A compliance framework could be developed for any set of legislative, regulatory or contractual requirements. For the GDPR, of course, it will be a privacy compliance framework.

The development of a privacy compliance framework is comparable to any other ongoing business project; you want to establish a set of practices and policies that make sure that certain processes are always followed. Assuming those processes are aligned with the legal requirements, the framework should ensure that the organisation remains on the right side of the law. Importantly, all the necessary processes don't need to be defined from the start: they can be built into the framework at appropriate stages in order to achieve compliance. The most important step is getting the initial framework in place.

There are two ways of approaching this task: work it all out for yourself, or deploy and adapt a publicly available

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

compliance framework. The first option relies on some combination of trial and error and (probably expensive) consultancy support; the second draws on established best practice and can be a faster and more cost-effective route to compliance than doing it all yourself.

There are several compliance frameworks and standards to choose from. The GDPR explicitly identifies the use of international standards and privacy marks as effective tools for demonstrating compliance with requirements and it makes practical and commercial sense for a privacy compliance project to start off by drawing on such established best practice.

A privacy compliance framework is useful primarily because it provides a structured way of managing confidential data in such a way that the organisation is able to comply with often complex laws and, perhaps, on a multi-jurisdictional basis. Organisations that do not already have a privacy compliance framework can use a standardised framework to make the leap from exposure to compliance; organisations that do already have a privacy compliance framework can use national and international standards to obtain certifications that will enhance credibility with customers and stakeholders while also demonstrating to regulators and, perhaps, judges the due diligence and compliance efforts that have been made. There are currently two recognised standards or frameworks that could be used: ISO/IEC 27001:2013 and BS 10012:2017. There is an internationally recognised, accredited certification programme for ISO 27001. The certification status for BS 10012 is not yet clear. Other standards and Trust Marks are also expected to emerge.

The three key areas of a privacy compliance framework are:

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

- governance, risk management and compliance objectives;
- the privacy principles;
- policies, procedures, controls and records.

In most management systems and frameworks, there is a sense that the various processes are related, and that they feed into and are informed by a common set of controlling processes. That is, like most business processes, these functions will have defined inputs and outputs, and the privacy-specific inputs will eventually result in privacy-specific outputs.

Material scope

Any framework applies to a specific scope, the area of the organisation and its operations that fall within it. For the purposes of compliance, the scope of the framework must be directly informed by the requirements of the Regulation, which is described in Article 2.

> This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[8]

That is, your framework must cover all activities that involve the collection, use or other processing (such as deletion or

[8] GDPR, Article 2, Clause 1.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

modification) of personal data. For many organisations, this will cover almost all of their activities. Remember that this does not specify that the personal data is that of customers: you must also include personal data of your employees, contractors, etc.

There are some exemptions, but these typically relate to either high-level Union activities (such as member states operating in the interests of national or Union security), in the pursuit of criminal justice by competent authorities, or to very low-level activities (such as handling personal data as a natural person exercising activities that are exclusively personal or domestic rather than as an organisation).

Territorial scope

The GDPR is explicit[9] in saying that it

> applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

In other words, any organisation in the world may be subject to the GDPR if it provides services to EU data subjects.

[9] GDPR, Article 2.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Furthermore, the GDPR requires[10] organisations that are based outside the EU to nominate in writing a representative organisation within the EU. This representative must be located in one of the member states where the target data subjects are based and must be mandated by the data controller or data processor to be addressed by supervisory authority or data subjects on all issues relating to the processing of personal data. The appointment of such a representative will not, however, enable the controller or processor to avoid legal action for breaches of the GDPR.

In terms of the compliance framework, there may be other considerations, such as local or sector-specific laws and regulations, that may also have to be taken into account.

Governance

All organisations have an obligation to comply with the law. One of the fiduciary duties of directors is to ensure that their organisation has taken appropriate steps to comply with all relevant laws. Directors also have a fiduciary – and in many cases also a legal and contractual duty – to ensure that risks to the organisation are appropriately managed. Cyber risk is an example of the type of risk of which directors have to be aware. Cyber attack exposes organisations to significant reputational and operational damage, as well as the possibility of legal action by those whose personal data has been compromised. The GDPR, with its specific requirements around data breach reporting and its significant

[10] GDPR, Article 27.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

administrative penalties (up to 4% of global revenue or 4 million euros, whichever is the higher) for compliance breaches, should be on the radar of all directors and on the agendas of all board meetings. Boards should ensure that the privacy compliance frameworks that are put in place are capable of ensuring GDPR compliance and that they contain mechanisms for providing regular reports and assurance to the board on the state of compliance across the organisation.

One way that boards can approach their governance responsibility in respect of information and privacy risk is through the appointment of a board-level senior information risk owner (or 'SIRO'). The UK Government originated the idea of this role as part of its extended strategy to tackle information risk across the public sector and described the role of SIRO to be managing information risk from a business not a technical perspective, focusing on the strategic information risks related to the delivery of corporate objectives. This means taking a holistic approach to information risk across the supply chain and managing it in line with the organisation's risk appetite. This is a useful role for a board to put in place. This role is expected to work with board colleagues to:

1. establish an information risk strategy which allows assets to be exploited and risks to be managed effectively;
2. identify business-critical information assets and set objectives, priorities and plans to maximise the use of information as a business asset; and
3. establish and maintain an appropriate risk appetite with proportionate risk boundaries and tolerances.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Clearly this role has a broader responsibility than simply managing privacy risk. The reality, however, is that any framework you build to manage privacy risk must, perforce, be part of your wider framework for managing information risk. It therefore makes sense to tackle GDPR compliance as part of your wider strategy for managing information risk.

This governance element should manifest itself in appropriate resource commitment – in terms of personnel, financing and systems – to the GDPR compliance project, in demonstrable top management leadership and commitment, and in the corporate privacy policy and throughout internal communications.

All international management system standards published after 2013 contain, in clause 5 and its sub-clauses, a number of specific requirements covering top management commitment; these provide a good starting point for any organisation in determining the leadership of a corporate governance framework. The clause 5 requirements are detailed below.

Top management demonstrates leadership and commitment to the management system by:

a. ensuring policy and objectives are established and are compatible with strategic direction;
b. ensuring integration of the management system into the organisation's processes;
c. ensuring resources needed for the management system are available;
d. communicating importance of effective management and of conforming to the management system requirements;

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

e. ensuring the management system achieves its intended outcome(s);
f. directing and supporting persons to contribute to the effectiveness of the management system;
g. promoting continual improvement, and;
h. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

ISO/IEC 38500 is a standard that deals specifically with the corporate governance of information and communications technologies. It, too, is useful guidance for creating an effective technology governance framework.

Objectives

Your privacy framework will have a number of objectives. Obviously, the overall objective should be to comply with the Regulation and to avoid the "dissuasive" fines and other punitive measures. Your framework should also identify specific subsidiary objectives relating to the rights of data subjects and the protection of personal data.

Objectives should be determined in a way that enables performance against them to be tracked and measured. An objective is only useful, after all, if you can determine how you stack up against it. The normal acronym used in relation to objectives is that they should be SMART:

- Specific
- Measurable
- Actionable (or achievable)
- Realistic

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

- Time-bound

The performance of information security controls should be capable of measurement and improvement and ISO/IEC 27004 provides specific guidance on control measurement. While this standard is a useful starting point for tackling control performance, it does not contain specific guidance on measuring performance against specific data privacy objectives.

Key objectives could include:

- the capability of responding to subject access requests within the allowed time frame;
- the capability of reporting data breaches to supervisory authorities within 72 hours;
- retention periods of personal data;
- staff awareness training.

Key processes

A privacy framework should have a number of key processes, some of which your organisation may already have, and others that may be new. These could include processes for incident management, change management, corrective action, risk management and continual improvement.

Incident management processes – which will be discussed in Chapter 14 of this manual – are all about what you do when there is a data breach or some other information security incident.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

Fundamentally, the incident management process will comprise several stages: realising that something has happened and reporting it, understanding what has happened, containing the event to minimise damage, repairing the damage, making sure that the event cannot recur, and reviewing the organisation's response. The outputs of the incident management process will inform how the organisation's framework evolves to meet its current and future challenges.

The organisation will also need **change management** processes. All organisations have to change and adapt to risks and events, and to changes in customer and market requirements. When changes are rolled out to an organisation in an unstructured manner, new and unforeseen risks can be introduced. This is particularly true of ICT-related processes. Inadequate management of changes to business processes (or to departments or reporting structures) can create risks to personal information and possible breaches in existing privacy protection mechanisms. A change management process is an essential step in ensuring that rolling out a change is completely thought through, that possible deviations, problems and consequences have been identified and mitigated, and that roll-back options are in place.

A **corrective action** process is also necessary so that an organisation can make amends when something doesn't work as intended. This might be as obvious as a control being inadequate and failing to suitably protect an asset, or it might be a larger, systemic fault that prevents a whole process from functioning. In either case, the organisation will need a systematic method of identifying and remediating the fault.

You'll see the obvious connection here with the incident management and change management processes. Once an

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

incident has been dealt with, there should be an analysis of the cause of the incident, which should lead to the identification of amendments to or changes in existing controls or processes. These changes should be dealt with through the corrective action process, ensuring that corrections are reviewed and approved, that they're correctly implemented, and that they're reviewed for effectiveness. This last point is worthy of note: a corrective action needs to correct the problem, so your process will need to include a review stage. This review might be a one-off confirmation or it might require ongoing attention – that's something the process will need to identify.

One of the more critical processes is **risk management**, which is dealt with in much greater depth in Chapter 6 of this manual. All organisations face risks and, in the case of GDPR compliance, the focus will be on risks to personal data and to the systems and processes that interact with that data.

Risk management is very much at the core of any privacy compliance framework because the organisation needs to understand exactly what risks it needs to protect itself from. Just as a person might put on a suit of armour to save themselves from injury, that suit will be completely useless against poisonous gas, or might only have limited effectiveness against a bear. The organisation should ensure it invests its money and resources in the right areas, so having an effective risk management regime in place is a good way of ensuring that the return on investment is worthwhile.

A framework or management system should also have an underlying continual improvement process. A continual improvement process assesses existing processes and their outputs for conformity with laws, regulations or other requirements, determines any necessary adjustments, and

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

then feeds these into the originating processes that determine the framework or management system's inputs. In simpler terms, you might like to refer to the Plan-Do-Check-Act cycle (PDCA, also called the Deming Cycle), which is a popular management tool for ensuring ongoing improvement.

Other continual improvement cycles, such as the COBIT® Continual Improvement Life Cycle or the ITIL® Continual Service Improvement process, could be applied instead of the PDCA cycle.

The PDCA cycle divides the standard processes and practices for a management system or development process into four distinct stages: planning, doing, checking and acting. As a cyclical process, each stage feeds into the one that follows and enables continual improvement.

In brief:

- the organisation plans what it is going to do;
- does what it has planned to do;
- checks whether what it has done has achieved what it planned, and;
- acts on those findings to improve how it achieves its objectives.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

The PDCA cycle is illustrated in Figure 2, below.

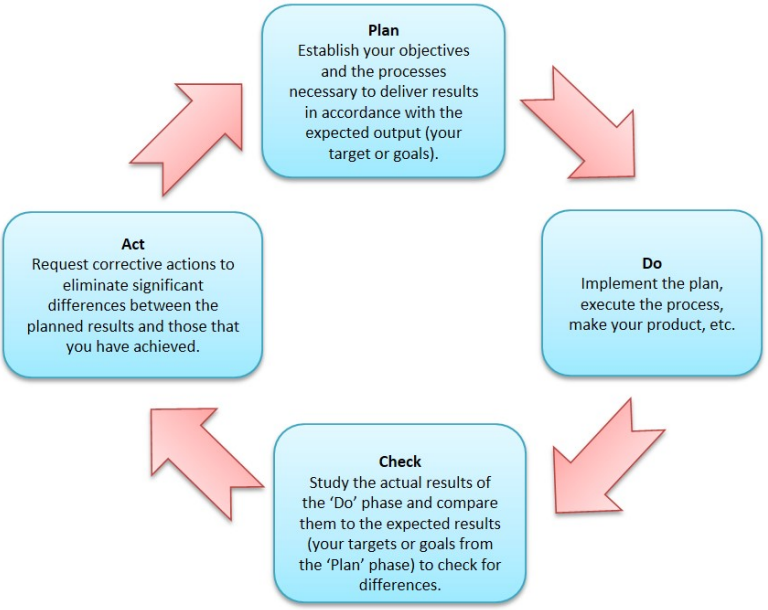

Figure 2: The PDCA cycle

Understanding how the processes and continual improvement of those processes all fit together is a critical feature of any effective compliance framework. Under the assumption that all of your processes are adequate and that they are being followed, such a framework provides assurance that you are continuing to adapt and improve your processes so as to continue meeting your compliance requirements.

Personal information management systems

Personal information management systems (PIMS) are a form of management system dedicated to the management of

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

personal information. As such, they can form a good basis for a compliance framework.

It is important to note that, while a PIMS and a compliance framework are broadly similar, there are distinctions. For instance, a compliance framework is not necessarily a "single object" but may be comprised of two or more management systems working in concert (a PIMS and an information security management system, or ISMS, for example). A PIMS may also be focused on simply managing personal information rather than necessarily protecting it in line with legal or regulatory requirements. In this sense, the PIMS may only provide some of the processes necessary to ensure overall compliance.

While a PIMS is not necessarily designed to ensure compliance with the GDPR specifically – or even with current laws such as the UK's Data Protection Act (DPA) or Germany's Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) – standardised models will usually include a requirement to identify legislative, regulatory and contractual requirements relating to personal information, and to include those requirements in the PIMS.

There are several possible ways to achieve this and BS 10012:2017 – *Data protection – Specification for a personal information management system* – provides one such framework for doing so. It provides a well-defined, well-understood structure for managing data protection, and it is designed to follow the PDCA cycle to ensure continual improvement. While the earlier version of the standard was specific to the UK's DPA, it has been re-drafted and updated to reflect the requirements of the GDPR and, as such, BS 10012: 2017 should be generally suitable as the core of a compliance framework.

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

BS 10012 includes a requirement to "define the scope of the PIMS and set personal information management objectives, with due regard to the […] applicable statutory, regulatory, contractual and/or professional duties"[11]. Properly applied, this means that the processes described in BS 10012 should take the appropriate legal requirements into account.

However, BS 10012 may not on its own be an adequate framework, depending on how your organisation collects, stores and uses personal data. BS 10012 is narrowly focused on privacy protection, and if PII is more widely used across your business processes, then a more comprehensive security framework would be appropriate. In this circumstance, you may need to define additional processes in order to comply with the Regulation. This is where an additional management system may be useful, such as ISO/IEC 27001, which is the international standard that describes best practice requirements for an information security management system (ISMS).

Regardless of the standard or business process model employed, a PIMS is likely to be a useful core for your privacy compliance framework. Figure 3 provides an overview of the typical components of a PIMS.

EXTRACT

[11] BS 10012:2009, Clause 3.2 d).

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

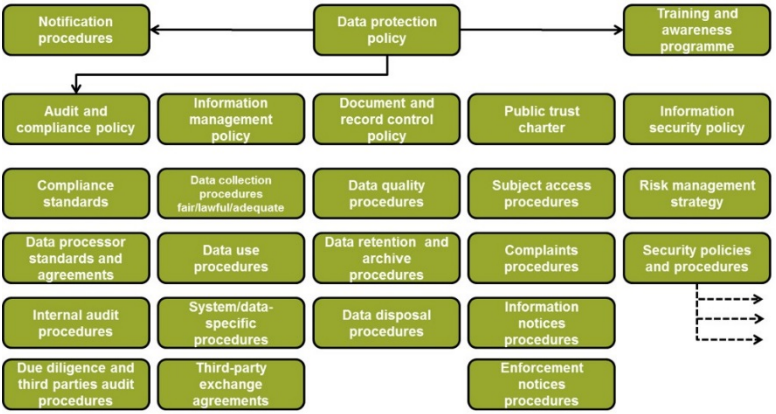

Figure 3: An overview of the typical components of a PIMS

<<< END OF EXTRACT >>>

EXTRACT

This extract and the original text it is taken from are both subject to ITGP copyright and may not be reproduced without prior written consent

New to the market, this must-have guide details what you need to do to comply with the GDPR. It covers:

- the GDPR in terms you can understand;
- how to set out the obligations of data controllers and processors;
- what to do with international data transfers;
- understanding data subjects' rights and consent;
- and much more.

The GDPR will have a significant impact on organisational data protection regimes around the world. *EU GDPR: An implementation and Compliance Guide* shows you exactly what you need to do to comply with the new law. Order your copy today:

www.itgovernance.co.uk/shop/p-1829.aspx

www.itgovernance.eu/p-1190.aspx

www.itgovernanceusa.com/shop/p-1542.aspx