Making Everything Easier!™

MetaCompliance Special Edition

GDPR FOR DUMMIES®

A Wiley Brand

Brought to you by

MetaCompliance®

Chad Russell
Data Privacy Expert

Shane Fuller
CIPP/E, CIPM

About MetaCompliance

MetaCompliance has over 12 years' experience working with clients across all industries to protect their data, educate staff and manage reputational and regulatory risks. In that time, the regulatory challenge for organisations has increased along with the threat landscape associated with their digital assets.

The company is a global leader in the 'human aspect' of cyber security and privacy compliance. Its integrated cloud platform incorporates Simulated Phishing, Cyber Security and Compliance eLearning, Policy Management, Privacy Management and Incident Management. This 'one stop shop' for managing privacy, compliance and cyber projects is graphically engaging, making it easier for staff to undertake their compliance obligations.

MetaCompliance's innovative MyCompliance cloud architecture is built upon the Microsoft Azure platform, which, like MetaCompliance, is fully ISO 27001 accredited. MetaCompliance is based in London, UK, Dublin, Ireland and Atlanta, GA, with a growing customer base in both the public and private sector.

GDPR

FOR DUMMIES®

A Wiley Brand

MetaCompliance Special Edition

by Chad Russell,

Data Privacy Expert

Shane Fuller,

CIPP/E, CIPM

FOR DUMMIES®

A Wiley Brand

GDPR For Dummies®, MetaCompliance Special Edition

Published by:
John Wiley & Sons, Ltd.,
The Atrium, Southern Gate Chichester, West Sussex,
www.wiley.com

ISBN 978-1-119-41925-9 (pbk); ISBN 978-1-119-41926-6 (ebk)

Printed in Bell & Bain Ltd, Glasgow

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Claire Ruston

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Frazer Hossack

MetaCompliance review team: Robert O'Brien and Ellen Mackay

Production Editor: Selvakumaran Rajendiran

Contents at a Glance

Introduction

As a line of business leader within your organisation, you're focused on your core area of responsibility. That could be marketing, human resources, operations or a number of other functions within the company.

You may have heard rumblings around the office about a new data privacy regulation coming from the EU called GDPR. If you're wondering what GDPR is and how it might impact your area of responsibility, *GDPR For Dummies* is for you.

About This Book

In the pages of this book, we explain to you what GDPR is and its potential impact across the various departments and divisions of your business.

GDPR is the General Data Protection Regulation. It's a new EU mandate designed to ensure data privacy and enhance control of personal data for EU citizens.

If your organisation interacts with EU citizens or businesses in any way, then you're subject to the obligations defined in this mandate.

Icons Used in This Book

What are icons? They're those little pictures you find in the margins of this book. They're there to make a special point. Here are the icons you'll come across:

This icon identifies useful bits of information that will help you understand the impact of GDPR and get handy tips on how to manage this.

Even if you don't read every word in this book, you'll want to take in the key points about GDPR that are marked with these icons.

There are lots of technical details around data privacy and GDPR. This icon indicates particularly technical information that might interest you.

This icon points out situations that just could get you and your organisation into trouble, so heed the advice.

Where to Go from Here

It's important that you gain an understanding of how your organisation as a whole will need to address GDPR so you can understand your place and part in addressing what needs to be done. Reading this book cover to cover will help you do just that.

However, if your time is tight and you're not able to read every word at this very minute, feel free to skip around to whichever section of the book addresses your particular needs. Pick what you want, and you'll find that you have the basic facts you need to evaluate the areas that might be relevant to your area of responsibility.

Chapter 1

Introducing the GDPR and the Data Privacy Challenge

In This Chapter

- An overview of GDPR
- Understanding the relevance of GDPR for your organisation

The General Data Protection Regulation (GDPR) is an iteration of the existing data protection law defined and enforced by the EU. The purpose of GDPR is to safeguard EU citizens along with their corresponding private information.

GDPR is a substantial overhaul of the data protection laws that have evolved over the past three decades, bringing it in line with the new digital world of Google, Facebook, Twitter and the like.

GDPR allows for EU Data Subjects (EU citizens whose data is being processed) to be granted certain rights and protections relative to their personal information. As you'll see in this book, personal information can include a myriad of data types, including but not limited to:

- First and last name
- Bank account information
- Address
- Medical records
- Passport information
- Personal email addresses

- Credit card information
- Photos and videos
- Usernames and passwords

An Overview of the GDPR

The GDPR replaces the EU's Data Protection Directive and unifies a patchwork of 28 differing privacy laws that currently exist across the EU into a consolidated and enforceable Regulation.

Looking at the history of GDPR

As shown in Figure 1-1, GDPR is an evolution of European data privacy laws that began in 1970 with the first Data Protection Law, which was legislated in Hessen, Germany during the mainframe era.

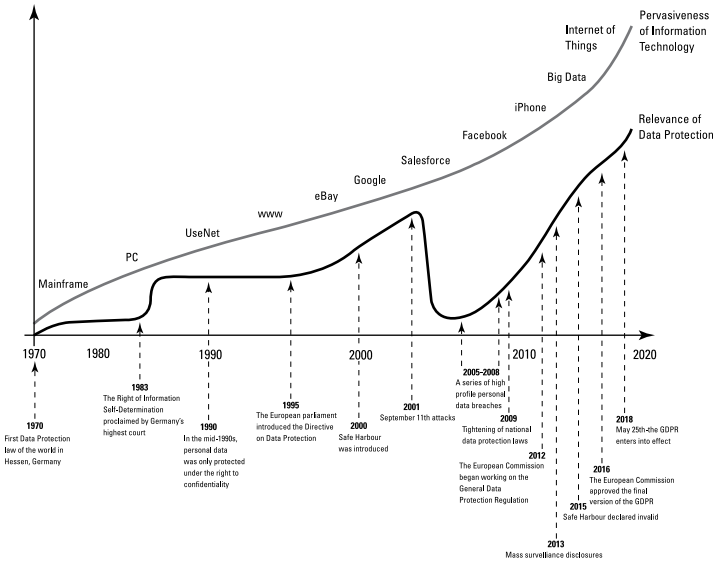

Figure 1-1: GDPR timeline.

In 1983, the Right of Information Self-Determination was proclaimed by Germany's highest court, and in 1995, the EU Directive on Data Protection was formally established, placing restrictions on the processing of personal data and the movement of this data.

The 'Safe Harbour' framework

Implementation of the EU Directive proved to be cumbersome considering the technology boom of the early 2000s and the increased electronic communications and commerce taking place between US- and European-based corporations and citizens.

In order to ensure adequate protections while reducing compliance-related friction, the US Department of Commerce and the European Commission developed the 'Safe Harbour' Framework.

In short, the 'Safe Harbour' framework ensured minimal business interruptions between US and EU organisations.

Numerous breaches in the latter 2000s

While the initial idea with 'Safe Harbour' was to streamline business interactions between EU and US organisations, it arguably relaxed definitions and enforcement relative to EU citizens' data privacy.

Numerous US companies that processed EU citizens' data were breached in the latter 2000s, which caused great concern for the EU.

Mass surveillance disclosures

In addition to the numerous breaches of US companies, there were revelations and disclosures that brought to light the existence of various mass surveillance programmes that collected data of EU citizens. This brought the issue right to the forefront for EU regulators, politicians and citizens.

One example of these mass surveillance programmes came from Edward Snowden's revelations regarding the 'Five Eyes' network, which comprises the US, Britain, Australia, New Zealand and Canada.

Another revelation regarding mass surveillance was PRISM, an electronic data mining program operated by the NSA.

The PRISM program purportedly collects internet communications from at least nine major US internet companies. These companies are required to turn over this data to the government pursuant to Section 702 of the US FISA Amendments Act of 2008.

GDPR key changes

Some of the key changes outlined by GDPR include:

- Increased territorial scope
- Enhanced data inventory requirements
- Increased penalties
- Appointment of a Data Protection Officer (DPO)
- Broader obligations for Data Controllers (organisations that collect and manage EU citizen data)
- Direct obligations for Data Processors (any company that processes personal data on behalf of a Data Controller)
- More timely data breach reporting
- Right to data portability
- Right to erasure ('right to be forgotten')
- Stronger Data Subject consent

Timeline for compliance

Any project plan starts with the end date in mind. Therefore, it's important to understand the timelines associated with GDPR compliance.

As at May 2018, GDPR will need to be fully implemented within your organisation. By this point, your team members should be fully versed in their roles and responsibilities as they relate to GDPR-compliant personal data handling and compliance.

To prepare for this, it's recommended that by Q1 of 2017 your organisation should have started preparations for GDPR compliance, including management education and buy-in. Also, it is recommended that your organisation should have considered appointing a DPO by this point. In addition, company policies and procedures should have been reviewed to ensure that they are up to date with compliance requirements as set out in the GDPR.

By Q2 of 2017 you should have started the gap analysis and risk assessment process. This phase involves analysing existing compliance levels. Organisations should have a clear understanding of the gaps between current compliance levels and compliance required once GDPR comes into full effect.

The third phase of GDPR preparation involves the prioritisation of risks and resource allocation. Items that have been deemed as high priority should receive immediate attention. Organisations should have completed this phase by the end of Q3 of 2017.

In Q4 of 2017 you should be executing remediation efforts focused on the high-priority risks identified in phase three. You can find more on GDPR preparation in Chapter 4.

GDPR comes into full effect on 25 May 2018. By this point, as a minimum, you should have remediated your high-priority risks and have all necessary personal data policies and controls in place.

Beyond May 2018, you're in the procedural and maintenance phase, which involves the ongoing management of personal data in line with the GDPR obligations. Head to Chapter 5 for more information on this phase.

Penalties for non-compliance

GDPR will be enforced from 25 May 2018. Companies who are in breach after this point will see a significant increase in fines as a result of the newly implemented Regulation.

GDPR states that 'The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the Supervisory Authority in order to remedy the breach.'

In the case of a breach, fines could be as high as €20 million or 4 per cent of annual global turnover, whichever is the highest of the two.

Understanding the Relevance of GDPR for your Organisation

The relevance of GDPR to your organisation will depend on several factors. Obviously, if you handle data for European citizens then it is in scope for you. In this book, we assume that you do handle data for European citizens.

GDPR relates to personal data. This is any information relating to an individual, whether it's in connection to his or her private, professional or public life. According to the European Commission, this can include but isn't limited to a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address (the unique number that identifies any computer using the internet). As you can see, it's a very broad definition. Thus, there is a high likelihood that any data you process for EU citizens is in scope.

With this in mind, it's important that your initial discovery exercise identifies the nationality of individuals associated with the personal data that you process across your business systems.

Scope and reach

The scope of GDPR in comparison to the initial EU directives is defined as being 'extra-territorial'.

GDPR determines whether processing falls within its geographical reach by taking the following factors into consideration:

- The location in which the personal data is being processed
- The location of the individual whose personal data is being processed

The intent is to make the Regulation equally applicable for organisations both inside and outside the EU where the personal data of an EU citizen is in scope.

If Data Controllers or Data Processors outside of the EU process personal EU citizen data in order to sell goods and services to EU citizens or monitor their behaviour, then it's deemed as being in scope.

This should be interpreted very carefully. For example, in several cases the simple use of web browser cookies is defined as a monitoring activity, therefore bringing the respective processing into the scope of GDPR. Web cookies are bits of information that are stored on your computer that track your activities when you browse websites.

Specifically, any non-EU company that tracks EU citizens using cookies is exercising behavioural monitoring as per GDPR guidelines.

The use of web cookies is just one example of behavioural monitoring. For example, tracking the IP addresses of EU citizens can also be interpreted as monitoring personal data.

Exceptions

GDPR does not apply directly to law enforcement agencies. GDPR exceptions also are afforded in other particular cases.

For instance, if a company outside of the EU (a US-based company, for example) has a website that is in English but only collects currency in US dollars and only accepts payment from US residents, then this would likely be out of scope for GDPR, even though an EU citizen still might be able to find a way to make a purchase on the site.

The GDPR allows member states to introduce exemptions on issues including national and public security, judicial independence and the enforcement of civil law as deemed necessary and appropriate.

Chapter 2

Summarising GDPR Best Practices

In This Chapter

- Getting to grips with the data privacy lifecycle
- The 'Prepare' phase – scoping and assessment
- The 'Operate' phase – data management
- The 'Maintain' phase – reporting and accountability

First and foremost, data privacy is a process that involves the incorporation of people, processes and technology. There are various best practices that can be incorporated covering people, processes and technology, which are covered throughout this chapter.

As you study this content, be sure to take into account your line of business and who might be impacted and how. This will allow you to thoughtfully interact with your respective team(s), which will need to be tasked with managing GDPR compliance for your area of responsibility.

Getting to Grips with the Data Privacy Lifecycle

The lifecycle can be broken down into three phases. In the first phase, stakeholders should be engaged to ensure organisational readiness. Next, the operational teams will implement procedures that are GDPR compliant. In the last phase, assurance criteria are reviewed and updated, then the entire lifecycle repeats itself.

Ensuring ongoing data privacy is a journey rather than a destination. It's an ongoing process of discovery, implementation and refinement.

Looking at the 'Prepare' Phase

The first phase involves several distinct activity sets in order to get the process of GDPR compliance underway. Along with ensuring stakeholder engagement, a GDPR readiness team should be assembled.

Relevant business function and third-party data processing activities need to be identified and a Personal Data Register should be created. Privacy policies and notices should be updated and internal personnel should be educated regarding GDPR as it relates to their specific job role. You can find more on this in Chapter 4.

Ensuring business engagement and stakeholder education

As with any major organisational project, the buy-in and sponsorship of senior management and executive teams is essential when putting a GDPR programme into place.

They should be educated as to the context of the regulation and the specific financial impacts associated with non-compliance.

Additionally, there should be representation from all lines of business within the organisation, such as:

- Human resources
- Procurement
- Sales and marketing
- Information technology
- Information security
- Development teams
- Legal, risk and compliance
- Customer services

Depending on the scope of your company, you might have a regional or global business presence. In smaller companies, it would be recommended to engage directly with senior managers and relevant peers to discuss the potential impact of GDPR on your organisation. If your company is larger or global in nature, then online training sessions may be a more practical way to initiate awareness and readiness across your organisation.

After the initial engagement process has been undertaken, a GDPR readiness team should be organised. If you're a business unit manager, you'll likely serve as a representative on the readiness team. The team should also consist of board-level sponsors, the Data Protection Officer (DPO), representatives from legal, risk and compliance and a programme manager who will be managing the overall GDPR compliance programme.

Once the team is in place, it's a matter of planning goals, objectives, milestones and resources, and ensuring adequate funding for the programme. Remember that there are costs associated with the initiation of the programme, but there will also be ongoing costs associated with GDPR compliance operations and maintenance.

Identifying personal data repositories

A Personal Data Register will need to be established by your company that tracks personal data associated with business processes, both internally and across third parties. As part of this, your organisation will need to begin ascertaining the relevance and reasoning behind storing and processing personal data.

Here is some of the information your organisation will need to know regarding personal data-related datasets:

- What data is being collected?
- Where is the data being sourced?
- Why is the data being collected?
- How is it processed?

- Who has access?
- How long is the data retained?
- Where is the data being transferred to?

Gathering this information into a common repository will provide your organisation with a central Personal Data Register, containing a common set of documentation regarding your personal data datasets, where they're sourced from, how they're processed and why.

The GDPR states that all organisations must implement appropriate data protection policies outlining the technical and organisational measures needed to ensure that personal data processing is performed in accordance with the Regulation. In addition, you must provide privacy notices as a means of being transparent with your customers, ensuring that they know how their information will be used.

Understanding your information lifecycle

It's important to understand your personal data-impacting business processes and the information life cycle (collection, processing, storage and transfer) associated with these processes. Once understood, these business processes will need to be risk assessed and a set of remediation actions defined where compliance gaps are uncovered.

Looking at the 'Operate' Phase

When instituting a compliance programme, guiding principles can help show the strategy and direction of an organisation's efforts.

Understanding the six guiding principles of GDPR

GDPR can be broken down into six overall guiding principles:

1. Lawfulness, transparency and fairness
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Confidentiality and integrity

Adhering to these guiding principles during design, implementation and operations will help to ensure that individuals and departments are following both the spirit and letter of the law.

In addition to adhering to the six guiding principles outlined above, the Data Controller must be able to demonstrate compliance with these principles. This relates to accountability, which could be considered a seventh principle.

Embedding compliant operational behaviours

Deep organisational incorporation of compliant behaviours ensures that employees at all levels operate in compliance with policies and procedures according to their respective roles in the organisation.

For example, the marketing department likely processes different personal data-related datasets than the corporate HR department, and in a different context. As such, there should be operational procedures in place for each line of business, and these should be contextual in nature.

Managing Data Subject requests

Clear instructions for handling Data Subject requests need to be defined and implemented in order to ensure consistency, predictability and accountability of these requests.

Data Subjects have certain defined rights according to GDPR that include:

- The right to information and transparency
- The right of access and rectification
- The right to erasure ('right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object

As such, it's important that your staff and those of any third party acting on your behalf can quickly recognise circumstances that engage a Data Subject's defined rights as outlined by the GDPR.

Handling privacy breaches

Handling privacy breaches is a critical operational pillar of GDPR compliance. GDPR defines a data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

If a breach is identified, GDPR dictates that documentation must be provided 'comprising the facts relating to the data breach, its effects and the remedial action taken'.

Having an incident response programme in place and modifying it to incorporate procedures specific to GDPR breach identification and notification allows organisations to leverage existing processes and procedures when managing relevant privacy incidents. You can read more about this phase in Chapter 5.

Looking at the 'Maintain' Phase

This phase operates broadly in parallel to the Operations phase. The Maintenance phase involves periodic analysis of all personal data operational practices. As part of this, you must also consider potential changes in the both the organisation and global compliance landscape. There's more on this in Chapter 6.

Establishing organisational accountability

Accountability in GDPR terms requires that you can demonstrate how you fulfil your obligations in relation to:

- Processing personal data lawfully and accurately in a transparent manner
- Having specific and legitimate reason to process the personal data
- Keeping personal data for no longer than is necessary
- Securing personal data against unauthorised use or accidental loss

A chain of accountability should be established at a department, company and organisation level in order to maintain consistent handling of incidents, operational processes and reporting activities.

Reporting on ongoing compliance efforts

GDPR requires that you evaluate the effectiveness of your personal data-related operational practices. Carrying out regular evaluations of your compliance efforts and reporting on such allows you to evidence accountability to your senior management team, board-level stakeholders and Supervisory Authorities whenever the need arises.

The effectiveness of the ongoing compliance programme requires tracking measurable metrics and adjusting processes accordingly when deviations are identified.

Understanding business changes and their privacy impacts

Most businesses find themselves in an almost constant state of change. As such, changes in the business need to be accounted for as to how they impact GDPR compliance activities.

It's good to stay close to major projects and initiatives within an organisation and incorporate representation by the DPO where relevant – especially when it comes to large projects or projects that clearly will involve the manipulation of personal data.

Examples of key business changes include the deployment of a new application, a business process re-engineering initiative, the acquisition of a new company, or even a divestiture. Or perhaps your company will move into an altogether new market. These are the types of changes, among many others, that can necessitate further review of compliance policies and processes.

The GDPR mandates that organisations have procedures in place that define when Data Protection Impact Assessments (DPIAs) need to be initiated in relation to business change events. The DPIA process must consider the impact of the new or altered processing operations on the protection of personal data.

Managing third-party data processing activities

In addition to instructing and educating third parties when initially engaged as to how to handle personal data, there should also be periodic reviews in order to ensure up-to-date handling in accordance with regulatory changes or changes in processing procedures.

GDPR-compliant obligations should be captured contractually at the outset of engaging a third party, and then reviewed periodically on an agreed schedule.

A third-party Data Processor should be periodically audited to measure effectiveness and adherence to GDPR personal data handling requirements.

Chapter 3

Putting in Place a Privacy Management Programme

In This Chapter

- Defining a Privacy Management Programme
- Embedding corporate privacy behaviours
- What line of business leaders need to know

A Privacy Management Programme (PMP) is not directly required under the GDPR, but it does simplify and streamline the process. It can also drive efficiency and improve accuracy, thereby enhancing compliance. In this chapter we look at why PMPs are important and how they relate to business unit leaders.

Defining a Privacy Management Programme

A PMP promotes transparency and accountability, and it should involve thorough planning and consideration of customers, employees and stakeholders. All employees will play a role in implementing the plan, some more so than others.

Having a PMP in place demonstrates a strong commitment to privacy and corporate governance practices. Having such a programme promotes a culture that respects privacy. Customers, regulators and business partners will take notice and interact accordingly. In addition, a PMP promotes an attitude of prevention as opposed to detection. If a breach or mishandling of personal data can be prevented, that can save your organisation money and protect its reputation.

A PMP is not a one-size-fits-all endeavour. Each company is unique and will therefore need to implement a programme that fits its needs.

Embedding Corporate Privacy Behaviours

One of the fundamental aspects of a PMP involves appointing someone to be a Programme Manager. A PMP Manager oversees the development, planning, implementation and ongoing maintenance of the programme. Ideally, having a PMP in place will not only be of benefit for GDPR purposes, but will serve as an enabling mechanism for future privacy-related compliance mandates that may come into effect in the future.

Implementing a PMP begins the process of embedding a privacy mindset into the DNA of a corporation. Employees should be trained during the induction process as to how to recognise and handle personal information as per the company's defined policies and procedures.

Those within your organisation who are identified as determining how personal data is managed or are authorised to handle and process personal data will require special training and serve key roles as part of an ongoing PMP.

Because technology is a driving force, it's crucial that line of business managers and the PMP Manager have a direct line to IT to look for opportunities to automate the PMP where possible.

What Line of Business Leaders Need to Know

As a line of business leader or business unit manager, you'll need to assess the personal data that you're responsible for, the personal data your team processes and the personal data your team ingests and forwards to other entities.

You therefore need to think through how your team interacts with customers or employees and how this might potentially change moving forward as a result of GDPR.

Customer service and marketing departments are typically on the front lines of Data Subject interaction and personal data handling.

Understanding the key roles defined by the GDPR

If your organisation determines the purposes and manner in which personal data is processed, it's considered to be a Data Controller.

Data Controllers play a key role in GDPR compliance, because of the customer and employee personal data that they retain and collect.

Data Controller duties include:

- Facilitating increased transparency of privacy data handling relative to Data Subject requests
- Ensuring that Data Subject requests are handled within the timelines defined by GDPR
- Carrying out privacy assessments and appointing DPOs
- Notifying Supervisory Authorities of data breaches within 72 hours of breach discovery
- Monitoring and responding to changes in compliance mandates
- Implementing pseudonymisation (replacing identifying data fields with pseudonyms) and encryption of personal data
- Maintaining records of personal data processing via a Personal Data Register
- Managing and governing third-party interaction relative to the processing and handling of personal data

If a person, organisation, agency or other body acts on behalf of a Data Controller, then they are considered to be a Data Processor.

Common examples of a Data Processor include:

- An outside agency (e.g. a company responsible for disposing of client information)
- A cloud provider that stores personal data
- Any service provider acting on your behalf with access to personal data of a customer or employee

Data Processors are subject to several direct new obligations within the scope of the GDPR, which include maintaining measures that allocate adequate levels of security for personal data relative to the potential risk.

Data Processors are required to abide by the instructions of Data Controllers unless such instructions conflict with the GDPR itself. Think of the Data Controller as the responsible party for the data and the Data Processors as those that process said data per a Data Controller's request and in line with the manner prescribed.

Although not mandatory in all cases under GDPR, most organisations will designate a Data Protection Officer (DPO). The DPO should be an expert in GDPR and privacy practices, as they are responsible for monitoring and reporting of GDPR compliance. DPOs are expected to help guide Data Controllers and Data Processors by auditing internal compliance and suggesting suitable corrective recommendations where necessary. DPOs are also expected to operate in an independent manner within an organisation. Arguably, this role is best suited to an internal audit and compliance manager or a member of your legal team, although there is still much debate on this topic.

Understanding your role in data privacy management

Your role in a PMP will differ based upon your role within the company. If you're the Chief Information Security Officer or Head of Legal for example, you'll likely play a larger, more

comprehensive role than an employee who works on the manufacturing floor who doesn't interact with personal data.

Responsibilities are often assigned on a departmental basis. Ideally, each line of business will have a Data Privacy Champion, who is someone in a management role that understands personal data handling, processing and privacy practices. If such a person doesn't exist, consider finding someone who is the most qualified and fill the gaps with training where needed.

A Data Privacy Champion will typically serve as part of an overall PMP committee and help to fashion and enact privacy controls within their respective lines of business.

Establishing the personal data elements under your control

In order to establish the personal data elements under your control, each line of business should conduct a business process review and analyse these processes to see whether they involve any interaction with personal data.

If this sounds like a daunting task, it is. Don't, however, let it overwhelm you. Start with some of the obvious high-level processes and work your way down into the details. This may involve several iterations of discovery in the form of employee interviews and group discussions.

Keep in mind that it's not just customer data that's affected – it could very well be employee data. Think of HR departments that manage data for employees who are EU citizens, for instance.

To conduct surveillance of employees lawfully, employers must demonstrate that such monitoring is required, transparent and legitimate.

There can be some interesting considerations when it comes to employee rights, privacy and freedoms and how they relate to GDPR. For instance, many companies will block employee access to certain websites or track employees' web browsing activities. These activities aren't necessarily non-compliant,

but they do require careful consideration regarding the context in which they're being done and the awareness and consent of the employee.

Cataloguing and recording your personal data processing activities

Cataloguing personal data processing should involve the establishment of a Personal Data Register. While you may not be responsible for establishing the Personal Data Register in your company, you may be required to contribute to it.

Each line of business will not only need to catalogue their personal data processing and implement controls that comply with GDPR, they must also be able to clearly document and evidence them.

For instance, if a customer service representative receives a request from a Data Subject to erase their data, then that request will need to be recorded, tracked and managed to completion.

An interesting and often overlooked area of personal data processing involves CCTV footage. While GDPR grants exceptions for law-enforcement purposes, if this data is used for other purposes, such as profiling, then these activities can be constituted as a breach of the GDPR mandate.

Managing customer and employee rights requests

Data Subject requests need to be managed in accordance with the timeframes and request parameters defined in the GDPR.

Customers and employees have a broad range of rights under GDPR, such as the right to request erasure of their personal data, also known as the right to be forgotten. In addition, customers can request exports of their data and information as to why their data is being processed.

Importantly, customers can also withdraw consent to the use of their personal data.

Now that you have an idea of what needs to happen, you need to determine how it will happen. How will you handle these requests? How will they be tracked and recorded? What are your departmental and organisational escalation procedures?

Departmentally and organisationally, you'll need processes in place that not only handle these requests but also address the requests within the parameters as defined in the GDPR mandate.

These parameters include response times, the format of the responses, procedures for identification of the Data Subject and the management of unfounded or excessive requests.

Educating your Personal Data Handlers

For the purposes of this book we are defining Personal Data Handlers as anyone within an organisation authorised to handle and process personal data. To educate these people, you need to know who they are. This is determined by analysing your business processes in relation to GDPR-affected datasets.

This process will define who is handling the personal data and how. Once this information is captured, the person responsible (e.g. the designated Data Privacy Champion), needs to explicitly define the processes and procedures that the Data Handlers should use to facilitate compliance.

Controlling personal data transfers

Unless pre-approved in organisation policies, decisions regarding data transfers should involve the DPO, in order to provide guidance and inform those ultimately responsible within your organisation. The DPO will advise you regarding data transfers based on which third country (if any) is involved and what safeguards and controls are in place, and determine whether those safeguards are considered appropriate as per European Commission guidelines. GDPR defines a third country as any country outside the European Economic Area.

Handling privacy-related incidents and breaches

The handling and management of privacy-related breaches will be a team effort within an organisation. Your organisation should have an Incident Response Team – indeed, you may already have one if yours is a large or medium-sized company.

Even if such a team already exists, it will likely need to modify its processes in order to comply with GDPR. In particular, the way in which supporting data is collected and preserved and the manner in which notifications take place will require enhancement to comply with GDPR.

The GDPR states that:

'In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Supervisory Authority.'

'The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach.'

The basis for notification to Data Subjects is not quite so well defined, however. The GDPR describes anything that constitutes a high risk to the rights and freedoms of an individual as a basis for notification. This arguably leaves quite a bit of room for interpretation. There's more on this in Chapter 5.

Instituting a 'Privacy by Design' mindset

Privacy by Design is imposed as a key requirement in the GDPR. As such, it makes sense to start thinking of privacy as a key part of all your new processes, projects and contracts. You should actively ensure that privacy has priority in the initial discussions for these activities. As part of your organisation's PMP, these should serve as guiding principles when planning out the programme and selecting tools.

It is now known that privacy is a key aspect of doing business in the digital world. In the past, privacy was an item that was given scant regard by many organisations. However, a cultural shift in organisational behaviour is required. This involves making Privacy by Design a key step that must be considered as part of the setup of each new policy, business process, project and contract under development. Starting now, mandating a Privacy by Design approach will ensure that new business activities are automatically fit for purpose from a GDPR perspective. This will save significant effort and cost through avoiding the need to retrofit privacy into these activities.

Now, where do you start? As business solutions or capabilities are developed, the datasets that they will interact with should be identified and the business processes should be modelled. When modelling these processes and their interaction with personal data, the requirements of GDPR and privacy best practices should be incorporated at the outset.

Ensuring consent and transparency

Consent is a mechanism of building trust between a user and an organisation. As defined via GDPR, consent is a 'freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Consent is defined as being fairly narrow from a GDPR perspective. For instance, if a user supplies consent for their data to be used for the purpose of cyber-fraud detection and their data is later used for marketing purposes without their knowledge or choice, then that is a violation of the personal privacy of the Data Subject.

Also, consent cannot be embedded in lengthy 'Terms of Service' agreements. To ensure transparency, consent forms must be separate, specific and explicit in nature.

Chapter 4

The Preparation Phase – Establishing Organisational Readiness

In This Chapter

- An overview of the GDPR Preparation phase
- Establishing the organisation's GDPR readiness position
- The role of technology in the Preparation phase

As described in this chapter, preparation for GDPR involves awareness, education, the identification of personally identifiable datasets and the current processing of those datasets.

A comprehensive Personal Data Register should be established to store the processing of the personal data-related datasets. The register becomes your centralised 'single source of truth', detailing the characteristics of the processing for all personal data-related activities for which your organisation is ultimately accountable. The register must be regularly checked and updated to ensure its integrity over time.

It's likely that discovery will take place on an individual business unit basis and roll up into an overall Personal Data Register maintained by your company.

An Overview of the GDPR Preparation Phase

The Preparation phase heavily involves the establishment of awareness and education regarding GDPR concepts, as well as an initial analysis of organisational readiness.

Increasing awareness of and educating staff regarding the GDPR requirements relevant to their role is key to successfully implementing and maintaining GDPR compliance.

Identifying and educating key stakeholders from the outset is crucial. It's important to look broadly across your organisation to ensure that you identify and educate all relevant stakeholder groups. Stakeholders from customer relations, human resources, marketing, procurement, systems development, IT, information security, legal, and risk and compliance are obvious candidates for inclusion. In addition, you should consider other business functions specific to your industry, such as research and development.

While these stakeholders don't need to understand all the fine-grained details, they should at least have an understanding of key concepts such as:

- Consent and transparency
- Data Subjects' rights
- Lawful processing
- Privacy incident handling
- Data transfer procedures

Likewise, those that are on the front lines handling personal data don't necessarily need to understand the entire scope of GDPR. However, as a minimum, these Personal Data Handlers need to understand GDPR as it relates to their specific job function. If a help desk agent, for instance, needs to solicit personal data as part of a password reset procedure, then there should be procedures in place to document and account for this.

Consider leveraging pre-packaged online training or hiring outside training firms to assist your organisation in this regard. Make sure that your legal team or representative is involved in this part of the process from a vetting standpoint.

Establishing the Organisation's GDPR Readiness Position

Here we focus on how you can help your organisation determine, in the most efficient way possible, its current compliance position in relation to the requirements set forth in the GDPR.

Until you know where you currently stand, you can't map out a path to achieving GDPR readiness, either at a business unit level, or ultimately at an organisation level.

Identifying your personal data touch points

GDPR expands the definition of personal data. This can now include online identifiers and even genetic and biometric data such as fingerprints, retina scans, voice recognition and facial recognition. Passwords are also considered to be personal data under GDPR.

During the Preparation phase, your organisation must identify and map out where personally identifiable data is sourced and how it is used. You must also have appropriate consent and a justification as to why the data is being processed.

It's a good idea to consider at this stage not only how you're going to do the initial personal data discovery exercise, but also how you're going to collate this information into a central Personal Data Register to ensure that you are correctly cataloguing your personal data processing activities.

Considering where your third parties fit in

When identifying personal data touch points, it's important to also consider situations that involve third parties who in any way interface with the personal data for which you are responsible. In this context, the third parties are considered Data Processors.

One of the key changes that GDPR brings for all Data Processors is a level of direct accountability and liability that does not apply under the previous EU Data Protection Directive. In addition, the GDPR imposes significant new Data Processor requirements that must be included by Data Controllers in all Data Processor agreements.

The increased level of direct accountability and liability for Data Processors will lead to the negotiation of contracts becoming more complex. Data Processors will likely be more careful about agreement terms. Be careful not to underestimate the time it may take to re-negotiate your Data Processor agreements.

Understanding your current personal data processing activities

Each business unit must assess all their relevant business processes to fully understand the information life cycle (collection, processing, storage and transfer) of the personal data associated with those processes. Procedurally, this will involve mapping data, business processes and data flows within your organisation. This will also involve analysing how the data comes into and goes out of your company. To do this efficiently and effectively, you must consult those people who perform the relevant operational tasks on a day-to-day basis.

The personal data assessments carried out for the relevant business processes will need to establish answers to the following questions:

- What data is being collected?
- Where is the data being sourced?
- Why is the data being collected?
- How is it processed?
- Who has access?
- How long is the data retained?
- Where is the data being transferred to?

Lawful processing of personal data is a key tenet of GDPR. From a consent standpoint, this means that:

- Data processing consent forms require explicit action from the user. For example, a check box must be explicitly checked by the user and not checked by default.
- Before soliciting consent, the affected individual (Data Subject) must be informed of specific rights as defined in GDPR.
- You should have processes in place that allow for users to withdraw consent at any time.
- Your organisation must track consent-related activities such as establishment and withdrawal of consent.
- Parental consent is required if a child is below 16 years of age.

In order to lawfully process personally identifiable information of a Data Subject, there must be a legal basis for doing so:

- The Data Subject must have granted consent.
- Processing is required to protect the interests of the Data Subject or another person where the Data Subject is incapable of providing consent.
- Processing is for specific preventative or occupational medical reasons in order to medically diagnose or provide health treatment or social services.
- Processing of data is within the realm of public interest (specifically public health).

GDPR also introduces the use of pseudonyms. This involves processing data in such a way that the personal data cannot be attributed to a particular user without the use of additional data, such as an encryption key.

Note that using pseudonyms does not preclude the data from being subject to GDPR, nor is it intended to be a sole means of data protection.

It's also important to understand that pseudonymisation is not the same as anonymisation. This is because some level of re-identification is still possible with pseudonymisation. Anonymisation in the strictest sense does not allow for re-identification.

Assessing the risk associated with your personal data processing activities

The GDPR states, 'In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.'

This essentially means that the protection mechanisms for the data should be commensurate with the potential risk. In other words, the GDPR represents a risk-based approach to privacy and data protection.

Let's analyse this a bit further. All items of personally identifiable information as defined in GDPR represent different potential levels of risk. For instance, a national identifier could potentially be used for identity theft. Arguably this is a high level of risk. A first name and last name may not fully represent a unique identifier in and of themselves, and may therefore carry somewhat less of a security risk.

As this data is stitched together into a larger collective which describes a Data Subject, then the data privacy risk increases accordingly.

Only once you have established the privacy risk associated with the personal data processing activities that take place within your business unit, are you able to prioritise those most deserving of your attention.

In practice, if you have a system with first and last name data and another with a national identifier, the privacy impact is lessened. If these data points are combined in a single dataset, the risk is increased.

Additionally, if there is a data point in common that could be used to logically join the records together, then that could represent an elevated privacy risk as well.

Updating your policies and notices

The GDPR states that all organisations must implement appropriate data protection policies outlining the technical and organisational measures needed to ensure that personal data processing is performed in accordance with the regulation. In addition, you must provide privacy notices as a means of being transparent with your customers, ensuring that they know how their information will be used.

It's unlikely that your current policies and notices will be fully GDPR compliant so it's important to factor in time to update and redistribute them to your staff and customers.

Understanding the Role of Technology in the Preparation Phase

Based on what you've read in this chapter, you may have concluded that technology will likely play an important role in compliance – and you're right.

People and processes obviously play a part, but technology can automate and solidify processes to ensure better compliance outcomes.

Additional technology can be used to save time and resources when engaging in compliance activities. If employees have access to an electronic Personal Data Register, for example, then compliance activities will likely be more efficient and effective.

The right technology can also streamline reporting and accountability in relation to GDPR compliance activities.

Privacy management solutions exist that can assist in automating both the discovery and ongoing management activities necessary to ensure ongoing compliance.

Chapter 5

The Operational Phase – Embedding Compliant Operational Behaviours

In This Chapter

- An overview of the GDPR Operational phase
- Living with GDPR within your organisation
- The role of technology in the Operational phase

In the Operational phase, your respective departments and the company at large will be fully engaged in implementing GDPR operationally. This means that there will need to be policies and procedures in place that are clearly defined and deployed at all levels within the company.

An Overview of the GDPR Operational Phase

The Operational phase consists of activities specific to:

- Managing personal data on an ongoing basis
- Understanding consent and transparency obligations
- Handling Data Subject requests
- Identifying and responding to privacy breaches
- Managing personal data transfers
- Operational data handling processes and procedures

Putting in place a register of processing activities

From the Data Controller's perspective, the minimum content of a Personal Data Register should include:

- Name and address of the Controller
- Name of the DPO
- Name of the EU Representative (if the Data Controller is not present in the EU)
- Relevant corporate department (IT, marketing, etc.)
- Details of related IT systems and software
- Name and address of the Joint Controller (another Data Controller who is controlling the same data), if applicable
- Categories of personal data
- Purpose of processing
- Categories of recipients
- Transfers to third countries (i.e. those outside of the EU)
- Documentation of safeguards for third-country transfers
- General description of data protection safety measures

While this information could be captured in a simple spreadsheet, unless you are a very small organisation it's unlikely to adequately serve the desired purpose. Using a third-party application or service is likely to make it easier to track this data and evidence compliance with the GDPR 'records of processing' obligation.

When recording the categories of personal data, the register should include both employee data and customer data.

Examples of employee data could include (but are not limited to) data such as:

- Name
- Job title

- Passport data
- Address

Examples of customer data could include (but are not limited to) data such as:

- Name
- Address
- Telephone number
- Contract details

Ensuring lawful processing

Any data that's processed that falls under GDPR must be processed according to the 'lawful processing' principle. Under GDPR, 'lawful processing' is only possible when:

- There is consent from the Data Subject
- Processing is necessary for the performance of a contract with the Data Subject
- Processing is necessary to comply with a legal obligation
- Processing is necessary to protect the vital interests of a Data Subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller
- Processing is necessary for the purposes of legitimate interests pursued by the Controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject

Some examples of 'lawful processing' in practice include:

- Employee administration
- Employee training and development
- Customer IT support services

Understanding Data Subject consent and transparency obligations

GDPR emphasises explicit consent, meaning active agreement by the user (e.g. checking a box that isn't already checked). The consent must be verifiable in some manner, which means that the consent must be recorded for reporting and auditing purposes.

Where processing is based on a Data Subject's consent, they can withdraw consent at any time. They also have the right to know how long their personal data will be retained for future processing. Parental or parental guardian consent is generally required for those under 16, although the ages required for consent vary by EU participating country. In addition, 'reasonable efforts' should be made to verify the identity of the person providing consent on behalf of the child.

GDPR states that data be handled 'lawfully, fairly and in a transparent manner in relation to a Data Subject'. Transparency is provided by GDPR in the form of various Data Subject rights, which include the right of information access, the right to know the existence of their rights and the right to rectification of inaccurate personal data.

Data Subjects should be provided notifications in a manner that's clear and understandable. Data Subjects also have the right to know what safeguards are in place to protect their personal data and whether any third parties are involved with processing their personal data.

Managing Data Subject requests

The GDPR extends a number of existing individual rights that Data Subjects can exercise against Data Controllers, as well as introducing a number of new rights. Organisations need to consider all aspects of their personal data processing activities in light of the rights afforded to Data Subjects.

Data Subjects must be allowed to exercise their rights free of charge, and the Data Controller receiving the request in connection with an individual right must comply without undue delay, which means within one month, with a maximum two-month extension depending on the complexity and the number of requests.

If a Data Controller is to decline a Data Subject's request, they must inform the Data Subject within one month and explain why they're denying the request.

Responses from Data Controllers must be clear and plain. If directed towards a child, communications with the guardian need to be considered as part of the process. Responses can be in written, oral or electronic form. If a response is provided orally, there should be a record of the communication.

Data Controllers also have the right to request additional identifying information from the Data Subject requestor in order to verify the requestor's identity.

As part of the response, the Data Controller must provide the following information to the Data Subject requestor:

- Lawful purpose of the data being processed
- Category of personal data in question
- The recipients to which the data has been disclosed
- Any third country recipients
- The time frame that their personal data will be retained
- The Data Subject's rights, such as the right to erasure and restriction
- The Data Subject's right to file a grievance with a Supervisory Authority
- Whether or not the user's data is being used for automated decision-making and profiling purposes (many times this is in a marketing context, but not always)
- Substantive information regarding the logic and reasoning behind the processing of the user's data and the intended use of the processed data

Data Controllers are protected from excessive or unfounded consumer requests, which can represent an undue burden. For numerous requests, the Data Controller has the right to charge additional fees or refuse to act upon the request. In order to exercise this right, the Data Controller carries the burden of proving that the requests by the Data Subject have been excessive or unfounded.

Managing privacy incidents and breaches

The GDPR definition of a personal data breach was given in Chapter 2. Essentially, a personal data breach involves the compromise of information to an unauthorised party. In many cases these are cyber breaches: electronic data breaches via hackers, malware, phishing and other devious means. Examples of breaches include breaches of credit card data, personal health records, financial information and many other personal data types.

Sometimes, breaches occur by way of external sources but in many instances these breaches are a result of 'insider threats', that is, personnel such as employees, contractors and business partners that have existing access to a company's data processing environment.

Personal data breaches cost organisations and consumers billions of dollars annually. So, when it comes to managing breaches, it's important to be proactive. Your organisation should use processes and technology where appropriate to mitigate a breach before it happens.

Companies should have an Incident Response Plan in place outlining how incidents will be identified, who will be engaged, how the threat will be contained and eradicated, and how the business will document and report on the breach and to whom. Companies should also have a defined Incident Response Team in place comprising:

- An Executive with decision-making authority
- Departmental team leaders
- Information security and IT personnel

- A Media Relations and Communication Officer
- The Chief Information Security Officer
- Legal, forensic and cyber experts as needed

Once it's known that a privacy breach is in process, the main immediate concern is to contain and stop the breach from continuing.

Executing the Incident Response Plan is likely to be the primary responsibility of the information security team in combination with the IT department. Other business unit stakeholders should work with these teams (or equivalents in your organisation) to manage the breach and then institute procedural enhancements to improve the security of personal data on a preventive basis.

Incidents should never be ignored. If a serious breach occurs, all Data Subjects and relevant authorities must be notified within 72 hours of discovery of the incident. This means that you should have a pre-defined process for notification in place to streamline the communications, such as the one set out in Figure 5-1 below.

The first 24 hours are critical. The longer a breach has taken place without mitigating measures, the greater the risk to the Data Subject in terms of privacy impact.

Best practice dictates that any weaknesses in processing and/or technology controls that led to the breach should be identified and remediated in order to prevent the same type of incident from happening again.

Managing personal data transfers

As the GDPR enables the free transfer of personal data within the EU, the data transfers that we discuss here are specific to the transfer of Data Subjects' personal data records outside of the EU to a third country. Additionally, this includes the onward transfer of data from a third country to another country outside of the EU.

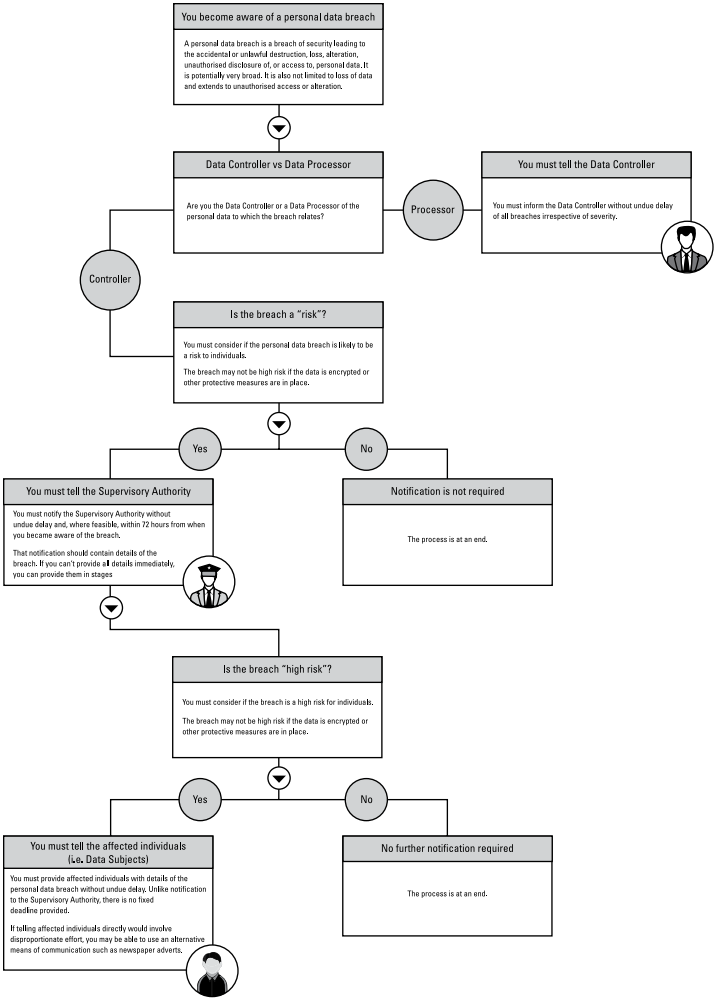

Figure 5-1: GDPR notification requirements in the event of a breach.

Fundamentally, there are three requisite considerations when transferring data outside of EU boundaries: adequacy of data protection, application of appropriate safeguards and the application of any derogations or exceptions.

First, the adequacy of protection must be considered. Decisions specific to adequacy are based upon assessment and analysis of third country laws and enforcement. If a given country has been identified as having laws that meet the

European standard of protection, then by default it will meet the 'adequate protection' standard as defined in the GDPR.

The European Commission is the standards body that makes decisions as to which third countries meet the standards of adequate protection. The European Commission's standards for adequate protections involve but are not limited to:

- The establishment of the rule of law within that country
- Access to justice
- International human rights standards
- General and sectoral laws
- Enforceable rights for individuals
- Effective judicial redress
- Data protection rules and measures

There is a publicly available list of countries that are deemed adequate by the European Commission on their website.

Where you're looking to make a data transfer to a third country not on the European list of adequate countries, you need to look at the deployment, enforcement and auditing of appropriate safeguards to ensure the protection of EU citizen personal data transferred to third countries.

These safeguards are primarily legal constructs. They include:

- Binding corporate rules: These are developed to allow large multinational corporations to adopt a system of policies for handling personal data that bind the company from an accountability standpoint. If a Supervisory Authority signs off on these rules, this helps simplify how multinationals manage and address global compliance issues.
- Standard contractual clauses: Sometimes referred to as model clauses, essentially these are template clauses provided by the European Commission that can be used by Data Controllers and Data Processors. The templates must be used and implemented as-is and are therefore non-negotiable in nature.

- Approved codes of conduct: These codes of conduct must be approved by the Supervisory Authority.
- Ad-hoc contractual clauses: These must also be approved by the Supervisory Authority. The purpose of these clauses is to account for the individual needs and nuances of a given company.
- Reliance on international agreements: This assumes that countries may engage in a distinct agreement that allows for the protection of data. Many times these agreements exist for reasons specific to national security and defence.

Finally, if a third country is not captured in the list of countries that are deemed adequate by the European Commission, and the safeguards listed above are not available to you, the only recourse for legally transferring EU citizen data is by way of derogation or exemption.

Derogations were initially defined in the EU Data Protection Directive, but the constraints are more narrowly defined in the GDPR mandate.

Scenarios outlining operational data handling

Certain lines of business within your organisation will be more impacted by GDPR than others. Let's explore a couple of the potential impacts of GDPR on various lines of business likely to be the most significantly impacted.

Marketing

Marketing departments are perhaps the most impacted line of business when it comes to GDPR.

The current EU Data Protection Directive allows for a soft opt-in approach in relation to Data Subject consent (i.e. assumed consent). However, the GDPR requires explicit opt-in. This means a clear, affirmative action must be taken by the Data Subject. A pre-checked box or inactivity is not adequate. In addition, the GDPR requires that you:

- Clearly indicate that they will be receiving continuous marketing communications from you by opting in
- Give the identity of those who will have access to their personal data (this includes any third parties that will have access) and a way to contact them about their data
- Have an unsubscribe/opt-out message that has no negative connotations attached (i.e. a cost)

It's recommended that marketing departments immediately begin updating their opt-in processes.

Opt-ins must be provable, meaning that there should be adequate tracking of opt-in activities.

Existing customers will also need to provide you with their explicit opt-in for you to be able to continue to send them your electronic marketing communications.

Human resources

HR departments will also be heavily impacted by GDPR. Perhaps the most relevant area to HR is consent. Typically, consent has been assumed on the basis of employment with a company. Now, HR teams will need to create consent forms for employees to sign outlining explicit consent for certain personal data processing activities.

Like customers, employees must be provided with a clear understanding of how their personal data is processed within the company and why.

Employees will also have increased rights under GDPR, including the right to be forgotten. In certain cases, an employer may be required to erase certain employee data when an employee has withdrawn consent for processing.

Employers will need to reconsider the 'lawful purposes' by which employee data is processed. This will likely require review and approval by your legal team.

Understanding the Role of Technology in the Operational Phase

Technology is fundamental to success in the Operational phase. While simple spreadsheets and paper-defined processes might be adequate for smaller business, these solutions will likely not scale-up for medium-sized and large organisations.

Technology offers the value of automation. Key areas which can benefit from automation from a GDPR standpoint include:

- Automation of consent management
- Automation of the Personal Data Register
- Compliance reporting and accountability
- Automation of Data Subject requests
- Automation of breach identification
- Network and data safeguards

Chapter 6

The Maintenance Phase – Demonstrating Accountability through Oversight

In This Chapter

- An overview of the GDPR Maintenance phase
- Oversight and staying GDPR compliant over time
- The role of technology in the Maintenance phase

Reporting and accountability represent the mainstay of activities you'll be engaged in throughout the Maintenance phase. The work isn't over yet!

An Overview of the GDPR Maintenance Phase

The Maintenance phase assumes that both the Preparation and Operations phases have been implemented. In this phase, your organisation will constantly need to review any major changes across your business or customer landscape that may affect ongoing operations and then adjust those operations accordingly.

Oversight and staying GDPR compliant over time

This final phase of the GDPR compliance lifecycle incorporates a series of recurring activities that address the need to evidence accountability with GDPR on an ongoing basis. As mentioned earlier, accountability involves assessing your organisation's implementation of GDPR and demonstrating, to external stakeholders and Supervisory Authorities, the quality of that implementation.

The ability to demonstrate the quality of your GDPR implementation requires forward planning regarding the areas that need to be assessed and the performance metrics that will be used to measure and evidence effectiveness.

Evidencing understanding of data protection policies

Organisationally, you should be able to prove that there is an actual understanding of GDPR-related policies you have put in place – in other words, that the recipients of those policies have both read and understood them.

Being able to provide this evidence puts you in a strong position to show that privacy has become an integral part of your organisation's 'business as usual' model.

Ensuring policy understanding is often best achieved through measurable e-learning programmes. These programmes not only help to conduct knowledge transfer but also measure and audit a learner's comprehension and retention of the policies as they relate to GDPR compliance.

Having these types of programmes in place will not only help ensure effectiveness in terms of the learning experience but also allow you to prove that policies have been properly disseminated throughout the organisation in a meaningful and measurable way.

Assessing your personal data processing practices

Assessing your personal data processing practices is an important factor to consider for demonstrating accountability. Types of operational assessments might include self-assessment at a business unit level, internal audit reviews and third-party audits.

Benchmarking is a best practice when it comes to ongoing accountability. You need to establish a baseline position and then improve your results in comparison to the last audit. If you're making a mistake, it needs to be corrected procedurally, and then be shown at the next audit to have been corrected operationally (i.e. in practice).

Some examples of metrics you might track include:

- Data Subject complaint handling
- Timeliness of Data Subject request handling
- Privacy incident and breach handling

Similar to benchmarking, where such metrics show a need for improvement, the next audit should indicate that the required improvements have been made and the issues corrected.

Ensuring ongoing integrity of your Personal Data Register

As stated in previous chapters, the purpose of the Personal Data Register is to keep track of the personal data that resides across your various business systems, identify how it's processed, when it's processed, by whom and for what purpose.

Naturally, there will be many changes that take place within an organisation. Say, for example, your company moves your marketing activities from an on-site solution to a cloud provider. An event such as this should trigger a Data Privacy Impact Assessment (DPIA) as covered in the next section. Identifying related changes in IT systems is also a critical consideration.

These changes may be at a department level (such as the marketing example above), across the entire organisation (e.g. an acquisition) or even relate to third parties (e.g. change of an IT outsourcing provider). The personal data-related information pertaining to these types of business change events also needs to be kept up to date in the Personal Data Register.

Periodic business system reviews and interviews with front-line staff can help ensure that the information in the Personal Data Register remains current and up to date.

You cannot assume that data that has been captured remains valid or current. It's estimated that data quality typically deteriorates at a rate of 15 per cent or more annually. This can be due to many factors, but particularly changing life circumstances for Data Subjects. People move, people are born and pass away – and all these changes affect the quality and accuracy of your data.

Triggering Data Privacy Impact Assessments for business changes

Businesses do not operate in a vacuum. They're subject to changing market conditions, regulations and global stability. As a result, most businesses will be in an almost constant state of change. As part of the team responsible for GDPR within your company, you need to have mechanisms in place for identifying and dealing with significant business change events that could potentially impact GDPR-related processes.

Examples of such business change events could include:

- Acquisition
- Divestiture
- New product offerings
- Changes in marketing activities
- Entering new market types
- Entering new market geographies
- Changes in providers and suppliers

- Updated procurement activities
- Establishing new business capabilities
- Development of new software
- Deployment of new or updated business systems
- Significant business process changes

Best practice is to have someone from the organisation's GDPR team involved in all personal data-related projects at the Programme Management Office (PMO) level. This ensures that all business changes that are considered significant enough to warrant their own project include representation by someone on the GDPR team, and are reviewed and considered accordingly from a personal data perspective.

If a new or modified personal data processing activity is identified as a result of any of the change triggers identified above, then a discovery process should be initiated in order to identify potential GDPR compliance issues.

These discovery processes might include:

- A systematic review of the personal data processing and its lawful purpose
- Identification of the necessity and proportionality of the personal data processing
- A risk assessment of the personal data processing relative to the rights afforded to the affected Data Subjects
- Measures required to safely address identified risks associated with the new or modified personal data processing

Controlling third-party data processing activities

Your organisation will be required to provide ongoing reporting specific to the compliance of third-party data processing activities.

Your company should have ongoing due diligence and communication procedures in place with third-party suppliers and providers to ensure that they're operationally delivering as outlined in contractual agreements.

These agreements, of course, will need to have clearly defined GDPR-compliant data processing requirements.

Ideally, metrics should be in place that assess third-party risk on a periodic basis and trigger review activities as needed based upon assigned risk ratings.

Some things to look out for when monitoring third-party data processing include:

- Identifying any changes in third-party personal data processing activities
- Collecting evidence indicating that controls adhere to personal data protection requirements operationally
- Identifying any compliance gaps relative to contractual agreements

It's important that contracts with third parties are periodically reviewed and revised to ensure that they remain fit-for-purpose relative to any changes in business requirements or personal data processing activities.

Providing assurance reporting to evidence accountability

As previously stated, accountability involves the ability of an organisation to prove that a proper privacy protection programme has been deployed and is functioning operationally in accordance with the Regulation.

The GDPR mandates that Data Controllers have a personal data protection programme in place. The GDPR specifically states, '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, the Controller shall 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.'

It's important that your business unit and the company as a whole can evaluate and measure the ongoing effectiveness of your personal data processing practices by providing assurance internally to senior management, the board and, in some cases, to external Supervisory Authorities.

If your organisation is acting in a Data Processor capacity, either as a whole or in particular business scenarios, there are also accountability requirements when it comes to record keeping. These include the obligation to maintain records stating the categories of processing activities being performed, information regarding transfers of personal data abroad, and a general description of the technical and organisational security measures applied to the processing activities.

Understanding the Role of Technology in the Maintenance Phase

As discussed in Chapter 3, an effective Privacy Management Programme involves a combination of people, processes and technology to achieve the greatest levels of efficiency and effectiveness.

Paper-based processes should be avoided whenever possible and technology should form a significant part of the solution. That said, all electronic processing should have its own set of safeguards to protect the systems that facilitate GDPR operations and reporting.

These systems should leverage the Privacy by Design principle as set forth in the GDPR (see Chapter 3). This begins when designing any GDPR compliance technology solution.

In relation to Privacy by Design, the GDPR outlines that organisations should build data protection into products throughout their lifecycle and that all necessary safeguards be integrated into those systems. The GDPR also specifically highlights data minimisation and pseudonymisation as privacy-enhancing tools. As such, these should also be

considered when designing any GDPR compliance technology solution and leveraged where feasible and/or necessary to maximise compliance.

When determining the feasibility of implementing a Privacy by Design approach, you should bear in mind:

- The availability of appropriate technology
- The nature of the personal data processing being carried out
- The risks to individuals (and their severity)
- The cost of implementation

Ideally, a GDPR compliance technology solution, whether it's off-the-shelf or custom-developed in-house, should incorporate automation, workflow, audit and reporting capabilities in order to prove accountability relative to GDPR compliance activities.

Chapter 7

Ten Things to do now to Prepare for GDPR

In This Chapter

- Ten things you can be doing now to help you prepare for GDPR

You've learned throughout this book that GDPR incorporates quite a bit of terminology and legalese, as well as processes and procedures. It's easy to get caught up in the details and not know where to start, so here are ten things you should do now to get your GDPR preparation underway.

Increase Awareness of GDPR Within Your Team

Education should start at the top and filter down in order to gain key stakeholder buy-in. Remember that business unit stakeholders don't need to understand all of the subtle nuances of GDPR, but they do need to have a general grasp of the terminology, required controls and desired outcomes.

Appoint Your GDPR Data Privacy Champions

In accordance with GDPR requirements, a Data Protection Officer (DPO) may need to be formally appointed for your organisation. Irrespective of whether or not this is the case, the appointments shouldn't stop there.

Your organisation should have a GDPR Data Privacy Champion within each line of business. The Data Privacy Champion appointed for your department will need to work with the appointed DPO, PMP team members and other key GDPR stakeholders to ensure organisational harmony and cohesiveness in terms of GDPR compliance activities.

Get to Know the Personal Data Elements Under Your Control

Whether you're in marketing, HR, customer services, procurement or one of the many other divisions within your organisation where GDPR will be a focal point, you should immediately start identifying all the personal data relating to EU citizens that is under your control.

Catalogue Your Personal Data Processing Activities

GDPR-compliant personal data processing procedures can be implemented centrally or departmentally. There are no hard and fast rules but you can't create procedures until you understand how you or your department processes the personal data that's under your control. You must also understand the context of that processing as it relates to lawfulness of processing in according with GDPR (see Chapter 5).

Engage Your Legal, Compliance and Information Security Teams

This almost goes without saying. Since GDPR is a regulatory mandate, your legal, compliance and information security teams should be deeply involved from the outset. They should already be working with senior business stakeholders and the DPO to ensure organisational buy-in and be engaged with IT in relation to personal data discovery and safeguards.

It's important that you engage with these teams to ensure that you fully understand what's expected of you from a departmental perspective.

Review Your Consent Requests and Transparency Notifications

Make sure you identify how your part of the business is currently obtaining consent and providing notifications of processing. Review your personal data collection processes and the wording of your existing privacy notices with your legal team.

Identify and Educate Your Personal Data Handlers

Once the senior stakeholder buy-in is in place, you should start engaging and educating those employees within your area of the business that handle or process personal data as part of their everyday responsibilities. Consider e-learning as an efficient and effective means of achieving this.

Plan for Privacy Breach Identification and Response

In order to provide breach notification as per GDPR, you need to actually know that a breach occurred. That sounds straightforward and maybe even common sense, but knowing that a breach has occurred can be challenging.

To help you determine whether you know what's happening with the personal data under your control, here are some questions you and those in your department should be asking:

- How do we know if personal data has been accessed by unauthorised personnel?
- Do we have any personal data stored in the form of unstructured data, such as word documents?

- How are we managing the flow of personal data in and out of our department?
- Are we accounting for the transfer of personal data across email and cloud applications?

Update Your Procedures for Data Subject Request Handling

If your customers and employees (i.e. Data Subjects) are not already asking for the data you store and process about them today, it's very likely they will be once GDPR is fully in effect.

You should have well-defined, consistent processes and procedures for handling requests related to the Data Subject rights covered by GDPR. Ideally, in order to streamline operations and maximise accountability, these processes should be the same across your various lines of business.

Identify and Assess any External Data Processing Activities

Lastly, start documenting any third-party data processing services leveraged by your department. Do you use third parties to consolidate your marketing data and manage mailing lists, for instance? Make sure that you're considering all potential third-party data processing scenarios.

MetaPrivacy

Imagine a cloud solution that automates your GDPR project

MetaPrivacy© is a cloud based privacy lifecycle management system that delivers an automated best practice approach to data privacy compliance.

Getting staff buy-in is critical to the success of any privacy programme and one of the key challenges faced by privacy managers and legal teams. MetaPrivacy© has been designed to increase stakeholder engagement by providing graphically rich, interactive assessments with video instruction, as part of the personal data information gathering phase.

The information obtained as part of the assessment process is used to automatically populate a register of personal data processing activities, which becomes your 'single point of truth' for privacy management.

The software provides an easy to follow workflow to guide specialist stakeholders through the review and approval phases of the lifecycle. Privacy risks and any associated remediation tasks can then be created, assigned and tracked within the system.

In addition, MetaPrivacy© includes role-specific GDPR online learning modules, advanced policy management capabilities, step-by-step guidance for managing privacy incidents and a collection of informative dashboards and reports that allow you to monitor privacy compliance programs and demonstrate accountability as required.

Contact us via **www.metacompliance.com** for more information on our privacy technology and how it could underpin your GDPR project.

The essential GDPR guide for business unit managers

Coming into effect in May 2018, the new General Data Protection Regulation (GDPR) affects all businesses who deal with the personal data of EU citizens. This practical, easy-to-read guide will help you prepare for GDPR, implement compliant operational privacy practices and maintain compliance on an ongoing basis.

- ***Get up to speed* — *understand the basics of GDPR, including what it covers, who is affected and how***
- ***Prepare for GDPR compliance* — *establish organisational readiness by identifying all the personal data you handle, updating your processes, educating your team, and more***
- ***Embed GDPR in your operations* — *get practical advice on how to include GDPR-compliant behaviours into your day-to-day operations***
- ***Maintain GDPR compliance* — *understand the oversight procedures needed to demonstrate compliance and accountability on an ongoing basis***

Open the book and find:

- **How to prepare your team for GDPR compliance**
- **Your GDPR obligations regarding customer and employee data**
- **How to put in place a Privacy Management Programme**
- **The importance of a Privacy by Design mindset**
- **The role of technology in GDPR compliance**
- **Activities you can be doing now to prepare for GDPR**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-41925-9

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.