Brought to you by:

GDPR Compliance

for dummies®
A Wiley Brand

Explore ramifications of the GDPR

Rethink how you handle data

Get ahead of the compliance curve

Steve Kaelble

Informatica Special Edition

About Informatica

Informatica is the only Enterprise Cloud Data Management leader that accelerates data-driven digital transformation. Informatica enables companies to unleash the power of data to fuel innovation, become more agile, and realize new growth opportunities, resulting in intelligent market disruptions. With over 7,000 customers worldwide, Informatica is the trusted leader in Enterprise Cloud Data Management. For more information, call +1 650-385-5000 (1-800-653-3871 in the U.S.), or visit www.informatica.com/.

GDPR Compliance

Informatica Special Edition

by Steve Kaelble

for dummies®
A Wiley Brand

GDPR Compliance For Dummies®, Informatica Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-45691-9 (pbk); ISBN 978-1-119-45689-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it.

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

Project Editor: Martin V. Minner

Senior Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Selvakumaran Rajendiran

Table of Contents

Introduction

Hardly anything is more ubiquitous these days than data. Air and water may be more prevalent, maybe, but not much else. That's certainly not a bad thing, because the world has benefited tremendously from the ability to collect, process, analyze, and share data, and use it to provide personalized and powerful services to customers and businesses. But this prevalence of data brings plenty of risks, too, including unwelcome privacy intrusions and nefarious breaches.

Not surprisingly, people are demanding more control over the personal data related to them. That's a big part of what's driving the new General Data Protection Regulation (GDPR), enacted by the European Union with an effective date in May 2018. It's requiring businesses around the world — not only in Europe — to take a fresh look at how they handle data on individuals. It's even forcing new thinking on what constitutes sensitive or personal data.

All businesses everywhere need to explore the ramifications of the GDPR, because it affects many organizations that may not expect it. The price of ignoring this compliance minefield is potentially high. The good news is: Getting ahead of the curve can provide benefits that go well beyond the satisfaction of simply living within the law.

About This Book

GDPR Compliance For Dummies, Informatica Special Edition, offers an introduction to the world of GDPR compliance. It offers background on the regulation, why it was enacted, who it affects, what enforcement looks like, and what it means for the way your organization operates.

And, at the risk of giving away spoilers, this book has a happy ending. Despite its plot filled with uncertainties, threats, twists, and turns, it reveals that there is opportunity. Specifically, there are experts to help you on your path to GDPR compliance. Just as important, technology solutions have been created specifically to tackle what otherwise would be a daunting and potentially impossible compliance task. The happy ending is this: Not only can your organization survive this challenge, but you may be in a better place once it's all said and done.

Foolish Assumptions

Not to go too far out on a limb, but in the preparation of this book I've made some basic assumptions about you, the reader:

- Your work has a lot to do with data, the "D" in GDPR. You're a data steward of some kind, a data analyst, an enterprise architect, a privacy or information security officer, a data governance professional, or maybe even the chief data officer.
- You have a sinking feeling that GDPR affects your organization, and you know you'd better get out in front of this train before it runs you over.
- You're busy, so you'd appreciate some basic information in an easy read, some tips for success, and ideas for making compliance something other than a nightmare.

Icons Used in This Book

They're there, in the margins, screaming for your attention. They're icons — little pictures next to the text. Whatever could they mean?

REMEMBER

If you're breezing quickly through the book, be sure not to pass over the information in the paragraph spotlighted by this icon.

TIP

You wouldn't have picked up this book if you didn't think it would offer helpful advice. The paragraph next to this icon offers some specific suggestions.

TECHNICAL STUFF

Regulations and compliance are certainly never simple. If you're fascinated by the technical details of complex things, the paragraph next to this icon may interest you.

WARNING

This whole book aims to help you with your GDPR compliance efforts. The information next to this icon deals with a potential threat you might need to be aware of.

How This Book Is Organized

This book consists of a half-dozen chapters, each of which focuses on a particular topic related to the GDPR and the approach your organization should consider taking to deal with it. Here's a glimpse:

Chapter 1 — "Getting to Know the GDPR": What is GDPR anyway, who does it affect, and how? What does it require, who's overseeing it, who can help? And, is there perhaps a silver lining?

Chapter 2 — "Understanding What Data is Affected": All kinds of different data types exist out there, some that fall under the watchful eye of the GDPR and some that don't. How can you tell the difference, and what kind of governance will help you deal with the challenge?

Chapter 3 — "Finding the Data": The larger your organization, the more places in-scope data may be stored (or hiding). You need to find all of the in-scope data, assess the risks each data store poses, and figure out how to minimize those risks.

Chapter 4 — "Preventing Unauthorized Access": GDPR governs what you can and cannot do with the data you have gathered. But it also underscores the need to keep prying eyes from gaining access to data they should not see. How can you gain the required control?

Chapter 5 — "Managing Data Subject Information": Because personal data can be found in so many places across your organization, you need the ability to easily access it when an individual makes a request. This chapter explores strategies for taming the data beast.

Chapter 6 — "Ten Key Takeaways About the GDPR": Like all For Dummies books, this one provides a rundown of helpful information and insights.

Chapter 7 — "Ten Helpful GDPR Resources": You're ready to begin your GDPR journey. This chapter offers useful resources to help expand your knowledge.

Where to Go From Here

The answer is: Go wherever you want to go! The way this book has been prepared, you'll run across helpful information wherever you start, whatever you read, and whatever you skip over. If you're a traditionalist and want to begin with Chapter 1, by all means, go for it! If you're a contrarian and want to begin at the end, that's fine, too, because the information you read in Chapter 6 should make sense all on its own. However you proceed, I hope you'll enjoy the book and find the information helpful as you journey toward being compliant with the GDPR!

IN THIS CHAPTER

- Defining the GDPR
- Understanding whom it affects, and how
- Outlining the initial requirements
- Spelling out rights and responsibilities
- Grasping the challenges
- Learning who the regulators are
- Discovering opportunity amid the challenge
- Finding technology to help you comply

Chapter 1
Getting to Know the GDPR

The book you're reading right now isn't particularly massive. It's 48 pages, 12,000 or so words, maybe 70,000 characters. It's a book, but it's also a collection of data. Now consider, how are you reading this collection of data? Is the book on a printed page in your hands? Are the words on your computer screen? Have they been delivered to you on your smartphone?

The point of those last questions is to illustrate that data can really get around these days, from one side of the world to the other in an instant. You can be almost anywhere on the planet as you're perusing this particular collection of data that happens to be on the topic of data.

The first chapter of this book discusses a new way of governing and protecting a particular subset of the multitude of data floating about. It discusses a new data regulation called the GDPR, outlines whom it affects and how, highlights the basic rules, reveals who enforces those rules, and hints at ways that technology can help

businesses live within the rules. It also encourages you to see the regulation as not only a challenge but an opportunity to give your organization a competitive advantage down the road.

What is the GDPR?

REMEMBER

The best place to begin is by establishing just what GDPR stands for. GDPR is short for *General Data Protection Regulation*. It sounds simple enough, and at a broadly conceptual level, it is. It's a regulation put forth by the European Union (EU), with an effective date of May 25, 2018.

Here is the basic, easy-to-grasp concept: The world these days revolves around data. Much of it is pretty general and public, just like the temperature outside, the score of yesterday's football match, and the closing stock price of a particular company.

However, much of the data is highly personal to each and every individual, such as each person's name and address, his or her medical records and bank account information, photos, videos, and passport information. Most people would like to retain some control over their individual, personal data. The GDPR intends to help protect that data and provide enhanced rights around it.

See? That wasn't so complicated, right? As they say, however, the devil is in the details. Consider how data is shared and collected and transmitted — and, unfortunately, how it is sometimes hacked or accidentally released. You can begin to imagine just how complicated it is to govern and protect the data of millions and millions of people who live and work and travel and do business in multiple countries across the EU and all around the world.

Whom it Affects, and How

Here's one place the details of the GDPR start to get interesting. It's an EU regulation, so it follows logically that it affects businesses and organizations that are located within EU member states. It also makes sense that the GDPR would apply to non-European companies that are operating in an EU member state. If you're an American or Canadian who travels to Europe and rents a car, you're expected to follow the local traffic rules as you drive around. On a very basic level, it's kind of like that.

Remember, though, that we're talking about data, and remember how data easily zaps around the world these days in the time it takes you to sneeze. GDPR applies to any organization (anywhere in the world) that processes personal data about EU individuals, even if you never leave the comfort of your Northern California headquarters or your base in Asia, Australia, Zimbabwe, or somewhere else.

To call forth another driving-related metaphor, it would be as though you invited some European visitor into your car for a drive across San Jose — and as a result of who your passenger is, you were instantly required to observe European traffic regulations. The regulation applies to anyone who processes personal data about EU *data subjects*, which is a technical-sounding term that simply means any EU customer, consumer, partner, staff, or other individual. It is focused on the individuals it protects.

REMEMBER

That's the bottom line. You need to pay attention to GDPR requirements if you process the personal data of EU data subjects, offer them goods or services, monitor or track their activities, or otherwise do business with them. It doesn't matter whether you're in the EU or on an island in the South Pacific.

It applies to you in a variety of ways, too. Its requirements have an impact on data storage, processing, access, transfer, and disclosure. It spells out how you interact with data subjects and how you must respond to various requests they might make of you.

WARNING

And it's well worth paying attention to the requirements of the GDPR. That's because the potential penalties for running afoul of the GDPR can be rather large — up to 4 percent of an organization's global revenues, or €20 million, whichever is greater.

Privacy and information risk rise to the top of the agenda with the advent of the GDPR. Under its mandates and principles, privacy requirements apply to just about every kind of relationship:

- **Business to consumer (B2C):** The requirements bring a duty of care for EU personal data.
- **Business to business (B2B):** Your GDPR-related obligations extend into third-party relationships involving processing.
- **Business to employee (B2E):** If an EU data subject is your employee, your data on that person is within the scope of the GDPR.

Suffice it to say that GDPR is a whole lot of different issues, all wrapped up into one regulatory scheme. It's a security issue and it's a compliance issue. It's a matter of risk, and a matter of proper governance and control of data.


REMEMBER

It's also worth noting that GDPR is what's known as a *principles-based regulation*. That means organizations are responsible for considering what obligations they may or may not need to meet, all based on the unique and specific circumstances of their business and their use of data.

Put another way, its principles-based nature means compliance is anything but straightforward. Many organizations will have to create an interpretation of these principles, and that interpretation will help guide and steer their GDPR compliance initiative.

The Initial Requirements

You may already be familiar with the *European Union Data Protection Directive*. It emerged in the mid-1990s, which of course is ancient history in the world of technology. Much has happened in the realm of data collection and processing in the past decade or two, especially online, and the Data Protection Directive doesn't effectively cover some of the things that have developed since it was first established. The GDPR is a reaction to those kinds of concerns about the growing need for data protection.

As an organization, you need to fully understand how you use your information assets to ensure that you are incorporating the various new data privacy requirements. Given how data weaves its way through many different systems and processes, you have to do a thorough evaluation of your current and future data capabilities and be ready to make major adjustments to your information-management practices.


REMEMBER

Like any regulation, the GDPR includes all kinds of specifics to which you must pay attention. There's plenty of time for that later, but for starters, here are some of the most basic requirements:

- The ability to facilitate data subject rights, such as access, correction, objection, erasure, and data portability
- The implementation of design controls relating to the data protection of lawfulness, fairness, and transparency

- Limits on purposes for which you may process and store data
- Data minimization (including pseudonymization, or the replacement of identifying data with pseudonyms)
- Accuracy of data
- Storage limitation integrity and confidentiality
- Accountability


TIP

Under GDPR, it's important that you take a look at data security and data governance across your enterprise. Before making any processing decision that involves personal data, you need to put risk under the microscope and focus on the rights and freedoms of EU data subjects.

Rights and Responsibilities


REMEMBER

With that in mind, it's worth spelling out what those rights and freedoms are that apply to data subjects, because those turn into responsibilities for your organization. If an organization is relying on consent, consent must be specific.

For every organization that does data monitoring on a large scale, a *data protection officer* must be named, according to the GDPR. It also puts forth the idea of *pseudonymization*, whereby identifying data is converted in a way that makes it impossible for unauthorized people to trace it back to an individual. It doesn't necessarily make the data record completely anonymous, but it's more or less like translating the identifying information into secret code.

The GDPR gives data subjects the *right to object* to data processing. That means organizations will be required to show they have a legal and compelling reason to continue processing data on that particular subject. The data subject also has the right to have inaccurate data corrected.


REMEMBER

Here are four other significant rights spelled out by the GDPR:

- **Subject access request:** Individuals have the right to ask for the details of any information you have on them. You need to be able to provide a copy of the data, information about how you use the data, a list of any third parties that might have access to it, and an idea of how long you need to store

the data. If you get this kind of request, your organization must respond in a month or less (unless it's a particularly complex request).

- **Data portability:** Data subjects can ask that you pass along their data to another processor. This kind of right makes it easier for people to move their business to a competitor.
- **Right to be forgotten:** Data subjects can ask that your organization permanently get rid of data on them, particularly when you no longer have a need for it. They can also withdraw a consent that they have previously given you.
- **Notification of breach:** If there's a data breach, your organization must notify regulators within 72 hours, and in typical cases you also must notify those data subjects whose records have been breached. In certain situations, such as with well-encrypted data, you might not have to make a public announcement of the breach.

The Challenges of Compliance

The GDPR poses lots of questions that organizations must consider and raises many distinct data challenges. To begin with, compliance means that your organization must have control and governance of personal data wherever it is across the organization. That is far easier said than done.

Data, as you know, has proliferated throughout every organization and its business ecosystem. Data diversity is a big trend that works against ease of control and governance, and the requirements of data management and security are made all the more difficult by the move toward cloud computing and storage.

REMEMBER

Here are some questions that many organizations struggle to answer with regard to the GDPR:

- Where across this organization and its ecosystem can we find all the relevant and in-scope data to which the GDPR principles apply? Is that data at risk?
- How can our organization keep track of data across the operational ecosystem?

- How can our organization define and manage all of the relevant data assets so we can be certain that we're in compliance with all necessary policies and procedures?
- How can we identify and link all of the in-scope data records to which the GDPR principles apply?
- How can we effectively capture and manage the consents provided by all of the data subjects that we affect? How can we manage changes to each data subject's choice of consent, or manage the definition of consent?
- How in the world can we efficiently and effectively respond to subject access requests, and requests related to portability and the right of erasure, within the required timeframes?
- How do we control access to the relevant data? Do we now remove privacy data when we no longer require it for some relevant function or activity?

Who Enforces the Rules?

REMEMBER

Like the EU Data Protection Directive before it, the GDPR is enforced by the supervisory authority in each member state. The good news is that, unlike the former directive, the GDPR includes mechanisms intended to help harmonize its implementation from one member state to another.

Oh, there will likely be variations from one place to another. GDPR allows for cultural contexts and differences, such as differing age of consent and variations in human resources data. But, on the whole, it is much more homogenous than the Data Protection Directive of yesteryear.

Hassle or Opportunity?

Do you typically see the glass as half-empty or half-full? Do you grumble as you grab an umbrella, or do you sing in the rain? There are, similarly, multiple ways you can view the GDPR.

GDPR requires "data protection by design and by default." Like virtually all regulatory regimes, it is disruptive. Every time your organization is forced to adopt new controls or create and

implement new processes, your productivity can be at least temporarily impaired, and your people can develop bad moods.

On the other hand, though, it offers opportunities, too, that make compliance a worthwhile investment. For one thing, if your GDPR compliance initiative is better planned than your competitor's, that's a plus for you, your employees, and your customers.


TIP

Even more important from a longer-term perspective, effectively complying with the GDPR can help build trust with customers and others whose data you handle. And that, ultimately, is a good thing.

Technology Makes the Difference

You could argue that advances in technology are among the root causes of the many issues that the GDPR addresses. The more dependent we become upon data and the technology used to collect, process, and share that data, the more we need to protect data.


REMEMBER

The good news is that technology provides solutions, too. In fact, with every challenge comes a new opportunity, and the challenge of GDPR can result in opportunities around your organization's use of data.

Technology providers have stepped up to make it easier to address GDPR requirements. Informatica, for example, brings deep expertise in data management and data governance to help organizations on their path to GDPR compliance. Innovative new data management capabilities make it possible for you to wind up in a better spot after GDPR than you were in before. Informatica has developed integrated and intelligent software solutions for governance and compliance that provide an ideal support system for a GDPR initiative.

The foundation for your GDPR journey is your ability to define your policies, processes, and stakeholders for GDPR compliance and then discover the data that you need to protect and manage. Once you've defined and discovered your data, your goals may bring about the need to control access to your data, and it may even be beneficial to centralize your data across your organization. Such approaches are, at the outset, strategies for dealing with the new requirements of GDPR. However, adopting them can leave you in a better place overall in terms of data management.

IN THIS CHAPTER

- Getting a handle on data
- Appreciating the geography
- Understanding data types and technologies
- Taking an enterprise-wide approach
- Uniting IT with business
- Creating a data governance initiative

Chapter 2
Understanding What Data is Affected

Journalists are taught to consider the "five Ws and one H" when reporting and writing a news story. Those Ws are *who, what, where, when, and why,* and the H is for *how.* With respect to GDPR, you'll know all of those things by the time you're done with this book.

This chapter deals primarily with the second W, *what.* Specifically, what data is affected by this regulatory initiative? The chapter spells out data entity types, explores the benefits of tackling the problem across the entire enterprise, discusses how to get IT and business on the same page, and delves into the world of data governance.

Lots of Data . . . Which Falls Under the GDPR?

Every industry is affected by the digital transformation that has upended the way business is done, as well as the growing amount of data that is collected, processed, and shared. Quite a bit

of that data can be attributed to specific individuals, or what the GDPR views as data subjects.

The more data your organization deals with, the more challenging it becomes to figure out ownership, control, and management of any given bit of data. You may know of the risks in some cases, but the fact is that there is a lot of risk in what you *don't* know, too. If your initiative is going to be as successful as possible, you want an enterprise-wide approach to data governance.

REMEMBER

In-scope data can be all sorts of different individually identifying things, some obvious, some maybe less so. Name, date of birth, address, email address, that sort of thing . . . these are pretty standard stuff and not terribly surprising. Criminal records are probably a no-brainer, too — if you have access to those details about an individual, you won't be shocked to learn that the individual would want you to take care with that sensitive information. The same is true with passport information.

However, GDPR covers many other things, too. Photos, for example, which are all over the Internet and may be peppered throughout your data stores; or an individual's location, which many organizations are now gathering information about.

Biometrics and genetic details — if you've watched enough science fiction, you won't have trouble imagining the nefarious things that can happen with that kind of data if it falls into the wrong hands. Religion and religious opinions are considered in-scope data, too, as well as sexual orientation.

The Geographic Scope of GDPR

It can't be overemphasized how geographically wide the impact of GDPR promises to be. It's a regulatory scheme put forth by the European Union (EU), but it will affect virtually any and every organization across the world that does business with people in EU member states.

Put another way, compliance with GDPR has multiple dimensions and is not limited by physical geography. If your organization is in North America, this issue matters to you. If you're in Asia, it does, too — or South America, or Australia, or some remote island in the South Pacific, if your business gets you involved with

European individuals. Even if you don't deal directly with individuals, you could be on the hook. Dedicated data processing companies and their clients — including those that ship EU citizen data across borders for processing — need to pay attention, too, and ensure they can respond in a timely fashion.

Data That Might Be In-Scope

How you respond to the data you hold depends on what type of data it is. There are a couple of distinct ways to think about data types:

- The data entity type
- The technology type that manages the data entity type

REMEMBER

Look at Figure 2-1 to see some of the possibilities spelled out. Most pieces of information that you have on file about virtually any data subject would fit into one of the data entity types shown, and quite possibly more than one. Likewise, most of the data you have on a data subject fits into one or more technology types.

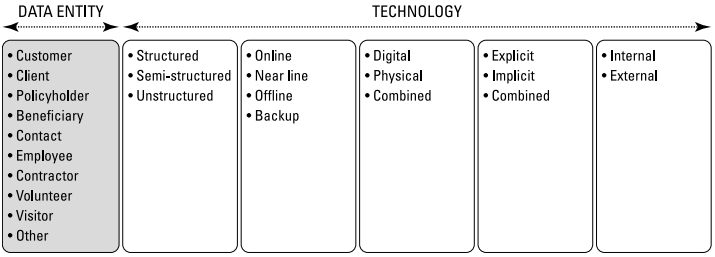

FIGURE 2-1: Data entity types and technology types.

The approaches, methods, and technologies you use to capture and manage in-scope GDPR data assets will vary quite a bit, depending on where within this grid the data types fall.

Taking an Enterprise-Wide Approach

It's a pretty daunting revelation when you realize just how extensive and widespread the in-scope data might be across

your organization. You need an enterprise-wide approach to understand what you're looking for and where to find it.

You have many questions to ponder as you begin this journey. The first series of questions is pretty basic: Do you know what data you hold, what purpose it serves to hold that data, and who has access to it?

If the answer to any of those related questions is "no," then you have a powerful need to figure out what the data you're holding is there for, and who is using it. You'll need this information as you begin to demonstrate how you're aligning with the principles of the GDPR.

A follow-up question to this "no" answer is: How are you going about finding out? Through questionnaires and interviews? Through a lot of manual work? Is your approach accurate? Is it time-consuming? Does it require a lot of resources? Does your approach leave open the possibility that there may be gaps in your knowledge — that you may go through your process and *still* not know where all your in-scope data is? (Can you see where these questions are leading? There must be a better way.)

Where the Technical and Business Environments Meet

REMEMBER

To wrap your arms around the data challenges, you need to get a handle on *policy interpretation*. This means gaining a full understanding of policies, responsibilities, processes, data terms, and logical and physical models. In particular, you need to understand these factors from a business perspective, but also from a technological point of view.

Policy interpretation is, in fact, the place where your understanding of the technical environment is linked to your understanding of the business environment. It's also the one area function for which GDPR requires a specific, named individual to be responsible, the data protection officer. If you can help the data protection officer (DPO) to effectively document policies, roles, processes, data terms, and interpret logical and physical models of systems that support them, then you're on the road toward gaining a holistic view about which data domains are in-scope with regard

to GDPR. This exercise is integral toward determining how best to manage your data assets.

REMEMBER

You could characterize policy response to GDPR as being an enterprise data governance use case. This response is both a top-down and bottom-up view of how your organization manages data, which reveals the links between the business and IT view of the information that the DPO needs to do his or her job. Here are some of the typical requirements that would apply to this use case:

- **Policy definition:** This includes business and IT definitions, plus documentation across all operational levels of the business, and logical and physical data and process models.
- **Responsibilities:** You must determine who owns the data, who uses the data, and what functions within your organization have responsibility for the data's quality and security.
- **Definition of terms and process:** This has to do with business processes, key data entities, attributes, systems, quality and controls, standardization, and how the business captures and acknowledges the consent of data subjects to use their data.
- **Change process:** You need a governed process for definitions, a governed process for change, and overall process governance.
- **Linkage to artifacts:** This refers to logical-to-physical artifact linkage, producing the technical and business data lineage needed to understand the dependencies, and ensure the quality, of in-scope data.

Your Data Governance Initiative

TIP

To succeed in the digital age, your data governance and compliance work needs to emerge from siloes and take a holistic approach. That means business and IT functions are able to work together toward a common goal of *Intelligent Data Governance* — a concept impactful enough that you can imagine what a competitive advantage it will yield.

Your aim should be to make it quick and easy for all subject matter experts to contribute to the data governance initiative. They're the

ones who should define the processes, policies, and data entities that are part of your holistic data governance capability.

An appropriate data governance initiative features wide-ranging capabilities, beginning with business and IT integration. You're looking for collaborative definition of policies, processes, terms, owners, categories, and purpose. It must encompass personal and non-personal data across the entire organization.

Who runs this kind of effort? The answer is lots of key leaders from the various areas affected. Some of the titles to be found in this committee are chief privacy officer, data privacy officer, data protection officer, chief data officer, chief information officer, and chief risk and compliance officer.

REMEMBER

You need the right people, for sure, and also the right technology. Consider the example of Informatica Axon. It's a solution that lets your non-technical business analysts and business line managers efficiently operate data governance programs. It's there to provide definition and direction for your intelligent data governance initiative. It's also specifically designed to unite business and IT views of data, as well as create the link between logical and physical data assets.

TECHNICAL STUFF

The aim is to optimize business outcomes such as regulatory compliance and risk. Axon makes use of a collaborative and automated methodology, letting users define and manage processes, policies, systems, people, and data. When used in conjunction with Informatica Secure@Source — which can automate much of the grunt work of discovering data that's in-scope for GDPR — you have the basic capabilities needed to get your GDPR response off and running.

IN THIS CHAPTER

- Sorting through silos
- Assessing data stores
- Analyzing data risks
- Finding help through technology

Chapter 3
Finding the Data

Your assessment of in-scope data has given you insights into what kind of data you need to be worried about with regard to the GDPR. But that is just the beginning of the quest, because now that you know what you're looking for, you have to find where it's hiding. And it isn't necessarily hiding in plain sight.

This chapter focuses on the search for data and the silos into which it might be divided. It explores how you go about assessing your data stores and analyzing how much risk each one poses so that you can prioritize your work. It outlines some of the technological answers that make this seemingly needle-in-a-haystack task achievable.

Data is All Over the Organization, in Silos

REMEMBER

The prevalence of data across the business world didn't happen overnight, and it didn't necessarily happen in a systematic, well-orchestrated way. Data in most enterprises can be found all over the place, in silos, scattered across many systems, applications, and sources. Data exists in traditional data bases, big data repositories, cloud environments, and document storage servers.

It got that way through the processes of technological evolution, and potentially through the realities of growth by acquisition.

How data became so decentralized and spread across the organization doesn't really matter to the authors of the GDPR. If it's data, and you're the one in charge of that data, and it pertains to data subjects in the EU, then it's likely to be in scope. It really doesn't matter whether it's in one of your core application systems, or a spreadsheet, or a local database, or some big data solution.

REMEMBER

That means one of the first jobs of your data governance initiative is quite simply finding all of the data. It means you need to look not only in the most obvious places where data usually resides, but also in the various other places data might be hiding.

Just as Chapter 2 embarks on its data governance mission with a key, basic question, so does this chapter. Do you know where all your in-scope data is? If the answer is "Yes," congratulations! You already have a handle on what this chapter is talking about. But you're likely in the minority. More importantly, can you produce continuous visualizations of your sensitive and personal data and its risk? If auditors asked for details about a specific data element, would you be able to demonstrate that you know where it is, who has been accessing it, whether it has moved across a border, and whether there is protection applied?

If the answer is "No" to either question, you have plenty of company out there in the business world, and you've come to the right place. The whole point of your GDPR compliance moving forward is to demonstrate that you understand the size and shape of the data risk across domains and data subjects.

As in Chapter 2, the follow-up query is: How are you finding the answer to the question of where your data resides? Does your effort involve interviews and questionnaires? Is it manual? Is it tedious and time-consuming and a drain of your resources? Do you think there might be a better way? (Hint: Yes.)

Assessing Lots of Data Stores

Depending on the size of your organization, in-scope data can be in many, many places — maybe even thousands of data stores, and in many forms (such as a database or a spreadsheet). Assessing it

all will not be easy, not for the average human being or team of human beings.

Indeed, for most organizations, data is usually scattered across many systems, applications, and sources. Typically, the larger the organization, the more spread out the data is. Organizations that have grown by acquisition are especially prone to this situation because each constituent part of the organization was already gathering and storing data before being acquired.

In addition, because an EU data subject might be your customer, a supplier, a partner, or potentially an employee, it isn't at all likely that personal data will be confined to one department or system. It likely won't be only in a big database application either. It might be in something as innocuous-seeming as a spreadsheet on one individual's computer.


TIP

There is, therefore, no time like the present for doing your "what if" planning. The truth is, all of these data stores must be addressed, but you nevertheless need to prioritize your remediation efforts and budget. You need to ensure that the work is done with high levels of accuracy and that the effort is scalable enough to reach all of the data stores that are affected.

Discovering Data, Analyzing Risks


REMEMBER

Sensitive data discovery is pretty much what it sounds like. The aim is to discover sensitive or personal data across a wide range of technology solutions. This is a highly precise and potentially time-consuming process, as you can imagine.

Data discovery is a process that must be done properly for many reasons, and not only because of the risk of missing something important. Going down this path with anything other than best practices can put sensitive or personal data at risk and create even more compliance problems than those you're trying to solve. The good news is: There are tools for this (more on that later).


REMEMBER

Once your effort has discovered the pertinent data, the risk analysis process gets underway. The aim of risk analysis is to create a risk score for data by considering the data itself along with other sources of information, such as the amount of data, who is accessing it, and how the data is moving around. What's the point

of having a risk score? It helps you to understand where you're storing the highest-risk data.

It's all part of the prioritization process. Sensitive or personal data with a high risk score can be elevated to the front of the line for potential remediation or security control requirements.

REMEMBER

What goes into a risk score? Many ingredients determine the level of risk posed by a particular set of data:

- **User access and activity:** How frequent is the user activity involving this data, and how much activity is there?
- **Proliferation:** How much does this data move across geographies, departments, and data stores?
- **Data volume:** How many sensitive or personal data records are there in this set?
- **Liability cost:** How much does the organization stand to lose if this data is lost or breached?
- **Sensitivity level:** Is the data considered confidential? Is it only for internal use?
- **Protection:** What controls are presently in place to secure and protect this data?

However, the work of risk analysis and scoring is more than simply tracking risk and prioritizing work at the beginning of a data compliance project. Just as the score of the big game changes while the match progresses, the risk score will change over time, too.

TIP

Tracking that change helps you determine whether your remediation or control activities have had an impact on the data risk position, or whether new remediation efforts are needed. It also helps you uncover new and emerging risks.

Who gets involved in establishing this element of your GDPR compliance? The answer is some of the same high-level leaders who got the ball rolling with your assessment of in-scope data. Likely participants would include the offices of the chief legal officer, chief information officer, chief information security officer, chief privacy officer, chief data officer, and data privacy officer. Capabilities of this work include in-scope data discovery and classification, proliferation analysis, multi-factor risk scoring, and the ability to receive policy-based alerts when necessary.

Technology that Can Help

It's easy to feel overwhelmed by the challenges you've uncovered. The risk can be substantial, the scale of the issue is broad, it's incredibly complex and volatile, and the clock is ticking. You have plenty of reason to be positive, though.

Technology may have gotten you into this situation, but it can also help lead the way out. Faced with hundreds or thousands of data stores, you can stress out and become overwhelmed at the prospect, or you can turn to technology that will tackle the task meticulously and efficiently.

REMEMBER

You might characterize this as a "detect and protect" technology use case. Your sensitive or personal data discovery and risk analysis put a strong emphasis on the "detect" part of that description. These core capabilities help you know where in-scope sensitive or personal data is as well as where it proliferates to, and it builds valuable analytical insights into data risk. Here are some of the typical capabilities that might be pertinent:

- **Data policy definition:** This capability gets into both business and IT definitions, as well as vague data and policy conflict.
- **Automated data discovery:** This capability is about finding relevant in-scope sensitive or personal data on the first pass, followed by continual monitoring, plus classification of data and integration of supporting systems. Data must be defined in context, with intelligent policies that identify whether a combination of specific data elements (such as name, email, and national ID) can be combined in any data store to identify privacy data of EU subjects.
- **Data proliferation analysis:** Data has a tendency to move around, which is what *proliferation* refers to. It isn't only a matter of finding out where the data is. You need to know where it goes and what new sources of data are emerging.
- **Data risk scoring:** This takes into account the factors listed earlier, including movement of data, proliferation, access, volume, value, and prioritization. This capability should include planning, history, and score monitoring over time. Monitoring would include excess access, anomalous user behavior, and cross-border data transfers.

- **Data protection:** This capability identifies where data access restrictions are needed, spells out what data should be pseudonymized, determines where encryption should be applied, which data can be retired, and governs the viewing of data based on time, location, and role.

As a prime example of a technology solution that delivers on these capabilities, Informatica offers Secure@Source. It was created to help discover the locations of in-scope data, but it doesn't just find it — it helps you figure out how to deal with it.


REMEMBER

The technology offers insights into data location and movement, classifies it, and monitors data proliferation including protection status. It also assigns risk scores, ranking the data stores according to risk in terms of the GDPR scope. That helps you prioritize remediation and monitoring activities and justify their cost. Then it tracks risk over time, so you can see how the changes you make are influencing your compliance efforts, either positively or negatively.

IN THIS CHAPTER

- Understanding the need for and scope of data protection controls
- Building compliant controls
- Employing the latest technology solutions

Chapter 4
Preventing Unauthorized Access

Complying with GDPR may require a lot of process and procedure as you ensure that you can answer data subjects' requests and implement their rights. There's also a fair amount of technology, because all of the data involved must be as secure as it can be.

Security is certainly a technological matter, in terms of building defenses against hacking. But in the end, much of it is a matter of creating controls to ensure that only the right people can access sensitive or personal data. This chapter focuses on the need for properly restricting access to the data you're holding on protected individuals. It describes helpful data protection controls and outlines technology solutions.

Why Data Protection Controls?

Of the requirements of the GDPR, one of the most basic tenets is protecting your data from being accessed by unauthorized users. That calls for some serious data security controls.

To begin with, from an IT perspective, you face various requirements that privacy data be encrypted, access controlled, removed, masked, or pseudonymized. It covers data being used in a wide variety of ways, from internal processes, customer services, and order processing to analytics and reporting. Your concerns about data protection also cover data related to testing and development, activities that bring their own sets of issues and challenges.

In practice, ensuring effective data security means reviewing for compliance purposes all of the applications that contain or access personal data. These applications need tight data access control for personal data at a user level.

The details of the potential scenarios can vary quite a bit. Consider production data. Various people might have access to the data, from administration to product support to app users to partners. Some are authorized, but some are not; and the app infrastructure must remain as is. Because you have unauthorized users in the mix, you would want to mask sensitive or personal data to prevent unauthorized access, through what's known as *dynamic data masking*, illustrated in Figure 4-1.

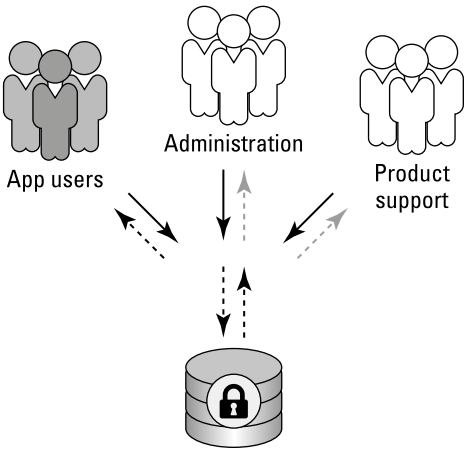

FIGURE 4-1: Dynamic data masking.

Data for analytics, testing, and development data, on the other hand, involves interactions with data analysts, data scientists, and testers and developers, and potentially no one is an authorized user. Your goal is to remove any risk of sensitive or personal data access, so an effective approach is to fictionalize data for

testing or research purposes and permanently change sensitive or personal data. *Persistent data masking* is the name of the game, as illustrated in Figure 4-2 (more on data masking in a minute).

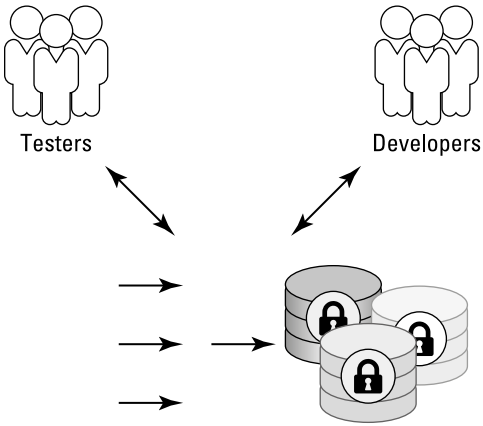

FIGURE 4-2: Persistent data masking.

Controls Must Be In Compliance

So, do you know how you'll protect your organization's data and ensure that you have the appropriate controls? How do you gain the kind of access control you need to protect the in-scope information of data subjects? By enabling strong and sophisticated security controls.

This isn't simple work, by any means. Many individuals across an organization and its ecosystem might have access to information about data subjects. Your data security controls must be able to remove or hide data subject information from people who shouldn't be able to see it while giving those who should have access easy visibility to the same information.

Your chief legal officer, CIO, and chief data officer should be part of the solution to this dilemma. As for the required capabilities, you need enterprise-wide protection and controls over data. These data controls must cover access controls, data deletion and retention, data masking, archiving, and pseudonymization.

Technology to Handle Security


TIP

Once again, there's good news on the technology front. The dawn of the GDPR and other regulations is making data protection solutions more imperative than ever, and also more prevalent.

This is all part of the "detect and protect" use case discussed in Chapter 3. You're in search of core capabilities to protect and secure data access, applying data-centric controls that include masking, encryption, and access controls. In keeping with the time-limited nature of consents, you also must manage the lifecycle of data, including archiving and deletion of data and the application.

Here are some of the typical capabilities that you'll need:

- **Risk analysis input:** You've done the risk scoring; now use it to direct data control methods.
- **Orchestration:** This musical term refers to the ability to schedule and coordinate data protection tasks in accordance with identified risks and ongoing monitoring of unsafe access or conditions.
- **Data security controls:** These include static or dynamic masking, pseudonymization, role-based access controls, encryption, and tokenization.
- **Change/update history:** You're comparing the application against source systems, the record masking or archiving outcomes against a consent record, and generating an audit trail for evidence.
- **Archiving:** This activity takes data out of production systems and archives it, logs the activity to provide evidence, and moves sensitive or personal data offline to prevent accidental usage or access.


TIP

Informatica weighs in with powerful solutions that help with privacy and the security of data assets. You can use Persistent Data Masking and Dynamic Data Masking to help automatically limit the number of people and systems that have unrestricted access to personal data. Informatica's Secure@Source, meanwhile, provides data security remediation by orchestrating updates to

security controls via Ranger, Sentry, and extensible to support other third-party protection systems. Data Archive helps organizations remove data that is no longer needed for business operations but could pose privacy risk if exposed. It also helps support the data minimization principles outlined in the GDPR.

It's tremendously helpful to build this kind of automation into data masking. You reduce the risk of personal data breaches, and make it a whole lot less likely that unprotected personal data finds its way out to an accessible environment.

IN THIS CHAPTER

- Envisioning a single data view
- Matching and merging records
- Creating a data subject repository
- Recognizing benefits beyond GDPR
- Employing the right technology

Chapter 5
Mastering Data Subject Information

Now's the time for dreaming big. Your assessment has found data all over the place. You're preparing to respond when some EU data subject files a request to have a look at the data you are keeping, change a consent, or maybe erase his or her data altogether. You should be dreaming of having a single place where you can look to get the ball rolling on fulfilling that kind of request.

It isn't a crazy dream, in fact. This chapter spells out the possibility of creating a trusted, 360-degree view of all data on each individual with whom your business is connected. It discusses the benefits of centrally managing data on data subjects for a single, consolidated view, discusses the matching and merging that make it possible, and explores technology that's available now.

Gaining a Single View of an Individual's Data

By now it should be evident — a crystal-clear picture of your data situation is hard to come by. You're operating in a world of diverse

data usage across complex IT environments. The idea of creating a single view of all information you hold about individual data subjects . . . are you kidding?

The fact is, different systems use vastly different mechanisms for storing data as well as indexing information so that it's efficient to find. That's why so many systems historically haven't done a very good job of communicating with one another.


TIP

Successful compliance means gaining a complete view of an individual data subject's information, as well as how it is stored, managed, or processed within your organization. It's important to capture the history of it, where it came from, when it changed, and who changed it.

Your system should also support the *privacy-by-design* concept. In a nutshell, this means privacy is a consideration throughout the whole engineering of the system — it's there from the start, a key building block rather than an afterthought.

You'll benefit from an authoritative enterprise-wide view of consents, as well as the ability to associate those consents with personal data attributes. In other words, your efforts involve more than simply tracking consents — it's vital to master them, too. If you can't have a way to master consents, how in the world can you be certain you are taking proper care of any particular data subject's rights? It all seems like a horrifying risk.

So, you might simply take a defensive posture, one intended to help you steer clear of penalties. Certainly many companies with poor existing consent tracking systems may be tempted to do just that. But that approach has its risks, too, including the risk of losing business agility and relinquishing competitive advantage by putting too tight a grip on personal data management.

It's important to realize that yesterday's consent tracking is only a precursor to today's mastering. What was required in the past doesn't rise to the level of what GDPR compliance calls for.


REMEMBER

Tackling this area of data governance begins with another question that seems simple enough but doesn't have a simple answer: How are you going to capture, manage, and distribute consents and manage data rights across channels and business units? Until

you can demonstrate that you have captured the lawfulness of processing across all in-scope data across all of your sources, you can't really say that this question has been fully answered.

The answer begins by determining what, if anything, your organization has in place already and at what level of detail. Perhaps you're planning to extend existing preferences capabilities, or maybe you have another approach. But is your existing approach adequate for GDPR compliance?

Once again, some key people must examine the organization's processes for consent tracking and enacting data rights, and the role that consent mastering can have. The chief legal officer has an interest in this issue, along with the chief risk and compliance officer, chief privacy officer, and data privacy officer.

Matching and Merging Data Subject Records

So, consider how mastering consents and rights might address this challenge. Different systems often take different approaches to storage and indexing. That's only one of the problems, though. Even with systems that play nicely together, it's vital to be able to match every variation of a customer record representing an individual across all systems, and then merge all of this identifiable information and any relevant attributes of the individual to create that trusted, single view of the individual effectively and accurately.

You can't build a complete picture unless you know that a particular John Smith in one system is the very same person as a particular John Smith in another system. Your system must be able to accurately match a John Smith record in one system with a record in another system for the same guy — it's the only way to create the big picture on each and every John Smith, and everyone else. See Figure 5-1 for an illustration of just how challenging this can be.

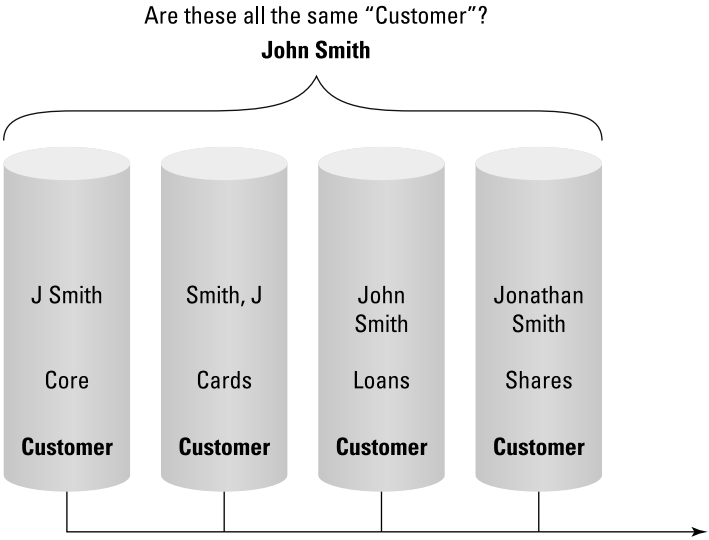

FIGURE 5-1: Matching records from different systems.

REMEMBER

Personal data management is the term for identifying data subject records within all identified sources. The idea is to match and merge records together for each individual data subject and create a single view of information about data subjects. It's essentially a complete picture of all personal data as well as the various consents associated with that data.

The challenge is: How will your organization match and merge in-scope data for each data subject across all relevant data sources? Will you be able to quickly and easily respond to such things as subject access requests, erasure requests, and portability requests?

Manual or siloed processes are not as efficient as what today's technology makes possible. Also, you can potentially reuse existing systems or build your own matching rules, but can you be confident you are matching up with everything you need to find when data is cast about such a wide area?

Such approaches raise plenty of additional questions. Will the system be fast enough, and not prone to generating false positives (the risk of treating two or more distinct customers as a single individual) or false negatives (the risk of not knowing that two or more distinct records represent the same individual)? Will the

records be complete, accurate, and consistent across your systems? Or will they be contradictory, with the data in one source conflicting with the same subject's data elsewhere, creating the need for interpretation?

The Value of the Data Subject Repository

REMEMBER

The *data subject repository* is an excellent rundown of what in-scope data is held across the various sources, its history, as well as how each piece of data can be linked to an individual data subject. It centralizes a 360-degree view of data subjects and becomes the authoritative source of data for times when your organization must respond to such things as subject access, right of erasure, right to be forgotten, or portability requests.

It would be incredibly difficult to fulfill this kind of request if you couldn't quickly identify all of the data you hold about that particular data subject. This view of all such data in your possession, regardless of location or system, would be incredibly valuable.

You will be well-served by an enterprise-wide, single view of each data subject, with automated matching and merging of data subject records. It should work in real time or through batch processing, with an audit and history system that is easy to update. It must also operate across multiple domains, including customers and clients, along with employees and other contacts.

Benefits Beyond GDPR Compliance

This book is, of course, about GDPR compliance, and from that perspective, improving the way you manage and govern subject information and consents will help you enable the rights of data subjects. With accurately mastered and linked data for each individual data subject, you'll be better equipped to deal with the right to understand data usage, the right to be forgotten, and the need to correctly apply consents.

The truth is, however, that your organization will also benefit in many other ways when you employ the kinds of solutions needed to get a handle on GDPR. The benefits are especially apparent when you're talking about the data of customers, who these days

are expecting more tailored personal experiences. To make that happen, you must be confident that you've been granted adequate permission to use personal data creatively.

TIP

Once you can be confident that you are correctly managing consents, data becomes more than simply a risk. You'll be able to see it as the asset it is, helping your organization gain agility and a competitive edge.

Technology that Can Pull it All Together

To effectively manage subject information, the answer is to make strong connections with various systems and create powerful automations. You need a solution that can link to all channels, gather data subject records and consents across all systems, and employ advanced algorithms to match and merge all data from each individual data subject, no matter where it's stored, and then synchronize the data with all required applications.

Think of this as a master data management (MDM) use case. Your solution must be able to identify data subject records across systems and provide a consolidated cross-system view of data by matching and merging like records together and creating relationship linkages to easily view, manage, and share how personal data can be used.

REMEMBER

Here are the typical capabilities that might apply to this need:

- **Access to relevant data:** You need to profile data subject data, extract relevant data from source systems, and apply analytical processes to semi-structured and unstructured content.
- **Data quality processing:** This involves assessing data completeness and validity, applying manual or automatic remediation, ensuring process control for manual remediation, and reporting metrics.
- **Single trusted view of data on data subjects:** This includes consent, how and where it is obtained, and how it is managed and governed, and provides perspective on the uses of the subject data depending on consents.

- **Matching and merging:** Your system must define and apply matching rules based upon business process definitions, match records, merge like records with scoring, and associate consent.
- **Data persistence:** The idea includes persisting merged/unmerged records and analytics.
- **Data governance:** Your legal and data protection officers will appreciate an easy-to-use interface with historical information and details about consent wording and applicable processes.
- **Multidomain capabilities:** This refers to the ability to manage all domains of data subjects, including customers, prospects, employees, and suppliers.

In practice, these capabilities sound exactly like what Informatica has created. Its MDM solution provides the foundation for this kind of single view of data and their relationships. It provides a purpose-based perspective for each data subject required for each process.


TIP

Informatica MDM Multidomain Edition makes use of advanced algorithms to identify data associated with the same data subject from any data source across multiple domains. That includes data on any individual that may take on different roles: customers, prospects, employees, visitors, and anyone else whose information might be on file. Through business process management capabilities, the solution helps organizations establish and govern workflow-based operations, including the right to be forgotten and right of portability.

Consider what a master data management system can pull together into one easily accessed and managed place:

- **Customer relationship management:** Your sales and marketing team may use a system by one or more of these: Salesforce, SAP, Microsoft, or some other vendor. It's packed with data about customers, vendors, and other contacts.
- **Enterprise resource planning:** PeopleSoft, Oracle, Hyperion, SAP, and others make up this segment. You have many choices, all packed with customer information, and all handling important work for your purchasing, operations, and financial management.

- **Human resources:** Your team has all kinds of sensitive or personal data about current, past and prospective employees, external resources, and other providers. In some industries, employees may also be customers.
- **Third-party data:** Your channel management efforts may include customer data and account information through a variety of sources, from Dun & Bradstreet to Bloomberg.

REMEMBER

Imagine all of that in a single view, data and consents, with everything you need to manage, deliver, and view the rights of your data subjects. You have traceability and full access to history, audit, and security.

IN THIS CHAPTER

- Complying or paying up
- Delivering data rights
- Standardizing the rules
- Recognizing the opportunities
- Evaluating the risk
- Finding technology fixes

Chapter 6
Ten Key Takeaways About the GDPR

Here's where I gather ten thoughts that are worthy of your full focus and even extra attention. These key takeaways are far from the only things you need to know about the GDPR, but they're near the top of the list.

Europe Speaks, The World Listens

Some 508 million people make their home in the European Union. That's a major market full of potential customers, and when they want something, smart business people listen. These people want control over their personal data, and they want it protected. That's what the GDPR is all about, and those European individuals have gotten their wish. Wherever you are in the world, if you want to do business with any of these 508 million people, you need to comply with the GDPR.

Ignore the GDPR and It'll Cost You Big Time

That's some nice revenue you've got there. It would be a shame if anything happened to it. But if you do business with European individuals, known in GDPR-speak as *data subjects,* you'd better treat them right or you might lose a good chunk of that change. The GDPR carries with it substantial penalties of up to 4 percent of your organization's global revenues, or €20 million, whichever is greater.

Not Gone, But Forgotten

All kinds of folks want to be remembered. But in today's data-centric world, there are situations in which you'd rather be ignored and relegated to the trash bin of forgotten history. Some have argued that the right to be forgotten is a human right, and the GDPR has enshrined that right by giving individuals the right to demand that their data be deleted when it's no longer needed. Organizations need to be prepared to deliver on that right.

One Set of Rules (More or Less)

Before the GDPR came the EU Data Protection Directive. Its aim was to set forth a variety of safeguards for European citizens, but one of the complaints raised by those whom it protects is the way those protections vary from one place to another. The EU is, after all, a group of sometimes-very-different nations. The GDPR has provisions that "harmonize" its impact from one state to another. That addresses concerns that have been spotlighted in surveys of European citizens, who by and large have been asking for the same level of protection across the continent.

Look on the Bright Side

Yes, complying with the GDPR can cause plenty of sleepless nights, lengthy committee meetings, disruptive process changes, and perhaps some temporarily lost productivity. You can curse

at it, or you can recognize the good that compliance will bring. Obviously, avoiding costly penalties should be reason enough to eagerly comply, but there are more. The biggest reason is that you're giving customers what they want. Surveys show they are concerned about data privacy, misuse of information, and breaches. Solve these issues and you've just earned gold stars for renewed trust. What's more, better data practices can help your business operate more smoothly, and even help deliver more of the personalized and customized experiences that wow customers. So, adjust your perspective — this can be really good for you!

Technology to the Rescue

You didn't *really* think that a major world power would enact a burdensome regulation that affects darn near everyone . . . and no one would step up to help you deal with it. Did you? The challenges of GDPR are real, and so are the technology solutions that can help you not only comply but thrive in the data-centric world of today and tomorrow. Throughout this book are examples of Informatica solutions to GDPR challenges. Just know that you aren't in this alone.

The Changing World of Data

It's quite difficult to keep up with the ways data can be collected and processed. The GDPR updates the directive that came before it by adding more kinds of data that are worthy of protection. The GDPR, for example, introduces definitions of genetic and biometric data — everything from a person's gene sequence to his or her fingerprints and retinal scan and facial recognition. The GDPR considers these to be sensitive or personal data types, which means processing them will require consent.

What Is Considered Risky?

There is some risk inherent in creating just about any data store — risk that something will go wrong with the data or your ability to control it, and the result will cost you in revenues or reputation. The fact is, some data stores are more risky than others, so those

are the ones you need to tackle first and devote the most energy to protecting. A risk score helps you rank the relative riskiness of data stores. It's based on a number of things, including how much activity there is with regard to accessing the data, how big the data store actually is, how much the data moves around from one place to another, where the data store is located, how much the potential loss would be if there were a breach, and how well-protected the data store is already.

Pseudonyms are Personal, Too

The GDPR puts forth the concept of pseudonymization as a means to protect sensitive information. The idea is to take identifying information and transform that data into something that can't be recognized without some sort of key. Make no mistake, pseudonym data is still personal data, and is thus still subject to GDPR protections. But by using pseudonyms, you reduce the chances that people will be exposed in an identifiable way, so your risk is lower.

Mix and Match to Win

You know you have data stored in all kinds of places all over the organization. You also know that because of the GDPR, you can expect to be fielding requests from European data subjects who want to do something involving that data. Your life would be a whole lot easier if you could build just one authoritative source of truth that can access your individual data wherever it is stored — even if an individual has data in a bunch of different systems and locations. That's the Holy Grail of GDPR compliance. All you need is the technology to match and merge records effectively.

IN THIS CHAPTER

- Getting the details
- Counting the costs
- Serving your customers
- Preparing for compliance
- Learning about the solutions

Chapter 7
Ten Helpful GDPR Resources

It's big and complicated, but the good news about the GDPR is that you don't have to face it alone. To begin with, you have this book in your hands. You'll also find plenty of knowledgeable people eager to assist when you check in with the experts at Informatica who brought you this book.

And in addition to all of that, following is a list of ten excellent resources that can help you expand your GDPR knowledge:

- **EUGDPR.org** — Check this online resource for detailed information about the regulation itself, the implementation process, and links to additional informational resources: `www.eugdpr.org`.
- **GDPR: 20 Million Reasons** — Another informational web resource, one that gets its title from the potential cost of non-compliance . . . a fine of €20 million or more: `https://20millionreasons.com`.

- **Informatica News Release** — This announcement provides details of Informatica's solution designed specifically for GDPR compliance: www.informatica.com/about-us/news/news-releases/2017/06/20170620-informatica-delivers-business-outcomes-for-general-data-protection-regulation.html.
- **Financial Services Executive Brief** — An outline of the basic premise of GDPR, with information geared toward financial services institutions: https://now.informatica.com/en_idc-data-governance-customer-centricity-and-the-gdpr_executive-brief_3203.html?asset-id=769e2df18c35f36449db02532f712e7c.
- **Data-Centric Approach to GDPR Compliance** — Informatica offers practical steps for compliance across the enterprise: www.informatica.com/GDPR.
- **Say Goodbye to Big Data's Wild West**—A helpful article from Datanami outlining the impact of the GDPR: www.datanami.com/2017/07/17/gdpr-say-goodbye-big-datas-wild-west.
- **Superior Customer Experience With MDM and Big Data Insights** — A white paper from Informatica on the power of placing customers at the center of your business: www.informatica.com/content/dam/informatica-com/global/amer/us/collateral/white-paper/superior-customer-experience-with-mdm-and-big-data-insights_white-paper_3318en.pdf.
- **Recommendations on How to Tackle the "D" in GDPR** — From Informatica, questions and answers on GDPR compliance: www.informatica.com/content/dam/informatica-com/global/amer/us/collateral/white-paper/gdpr_white-paper_3337en.pdf.
- **Informatica Axon** — Informatica offers details on the industry's first enterprise data governance solution: www.informatica.com/content/dam/informatica-com/global/amer/us/collateral/data-sheet/informatica-axon_data-sheet_3300en.pdf.
- **Informatica Secure@Source** — Your "detect and protect" solution for digital transformation: www.informatica.com/content/dam/informatica-com/global/amer/us/collateral/data-sheet/en_informatica-secure-at-source_data-sheet_2878.pdf.

Govern your data. Secure your data. Trust your data.

Organizations throughout the world are preparing for the General Data Protection Regulation (GDPR). Although GDPR compliance poses challenges, it's an opportunity for you and your organization to take a holistic, intelligent, and automated approach to governance and compliance - to deliver data that is trusted, secured, and governed. This data-centric approach helps you stay competitive and agile as new governance and compliance needs arise, fueling better business outcomes.

Informatica enables companies to unleash the power of data to fuel innovation, become more agile and realize new growth opportunities, resulting in intelligent market disruptions. With over 7,000 customers worldwide, Informatica ensures organizations have trusted, governed data with solutions such as Informatica Axon and Secure@Source to drive their data-driven digital transformation.

For more information on Informatica's Governance and Compliance solutions for GDPR, please visit www.informatica.com/GDPR.

Get ahead of the GDPR compliance curve

The European Union's new General Data Protection Regulation (GDPR) is requiring businesses around the world — not only in Europe — to take a whole new look at how they handle data on individuals. This book offers an introduction to the GDPR compliance. It offers background on the regulation, why it was enacted, who it affects, what enforcement looks like, and what it means for the way your organization operates. GDPR compliance is a challenge, but it's also an opportunity to rethink the way you manage data — and gain a competitive advantage down the road.

Inside...

- Understand what data is affected
- Find your organization's data
- Prevent unauthorized access
- Create a 360-degree view of data subjects
- Find the right technology
- Consult helpful GDPR resources

Steve Kaelble is an author and corporate communications specialist who enjoys bringing complicated subjects to life in easy-to-understand ways.

for dummies®
A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-45691-9
Not for resale

WILEY END USER LICENSE AGREEMENT

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