INTRO TO GDPR

★ ★ ★ ★ ★ ★ ★ ★

A Plain English Guide to Compliance

PUNIT BHATIA

Intro to GDPR

Punit Bhatia

Intro to GDPR

A Plain English Guide to Compliance

Advisera Expert Solutions Ltd
Zagreb, Croatia

Limit of Liability / Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. This book does not contain all information available on the subject. This book has not been created to be specific to any individual's or organisation's situation or needs. You should consult with a professional where appropriate. The author and publisher shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have been incurred, directly or indirectly, by the information contained in this book.

First published by Advisera Expert Solutions Ltd
Zavizanska 12, 10000 Zagreb
Croatia
European Union
http://advisera.com/

Editor: Dejan Kosutic.

ISBN: 978-953-8155-18-51

First Edition, 2018

ABOUT THE AUTHOR

Punit Bhatia is a senior professional with more than 18 years of experience in executing change and leading transformation initiatives. Across three continents, Punit has led projects and programs of varying complexity in business and technology. Across multiple industries, he has experience on both sides of the table; i.e., he has served as a consultant who worked for IT consulting companies, and as a key influencer and driver who has defined and delivered change for large enterprises. He has proven expertise in the areas of data privacy, sourcing and vendor management, and digital transformation.

In the last three years, Punit has advised and driven multiple initiatives to ensure compliance with the EU General Data Protection Regulation (GDPR). Part of this effort has involved attending multiple events, exchanging implementation approaches and dialogue with many experts. Based on these experiences, he is an active speaker or panellist at many different GDPR and sourcing events. Punit is also the author of another book: “Be Ready for GDPR”, which is available on Amazon in print and e-formats.

An engineer and MBA through qualifications, Punit is a Certified Information Privacy Professional – Europe (CIPP-E), a Certified Information Privacy Manager (CIPM), and a Certified Outsourcing Professional (COP). Punit delivers guest lectures at Solvay Brussels School of Economics and Management on topics of privacy and sourcing.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Thank you to Namita Bhatia (my wife), for being patient with my ideas.

To Yash Bhatia (my son), for bringing new ideas and energy into my life.

And to Dejan Kosutic, for reviewing this book and improving it.

And, special thanks go to all my family, colleagues and friends who stand by me, work with me, and challenge me to learn every day. I also take this opportunity to thank Advisera for publishing this book.

1. INTRODUCTION

The European Union General Data Protection Regulation (GDPR) is a key regulation in the field of privacy. So, in this section, we'll cover the following:

- Which companies need to be compliant with GDPR?
- How is this book structured?
- Who is this book for?

Note: Beyond the above questions, this book elaborates on the key requirements of GDPR and provides a simple introduction to setting and monitoring your GDPR compliance project.

1.1 Which organisations need to be compliant with the GDPR?

The General Data Protection Regulation is a significant piece of legislation, applicable to the processing of personal data of individuals in the European Union. The key to understanding when the EU GDPR is applicable is to understand the meaning of "in the Union". The EU GDPR will only apply to personal data about individuals within the Union, and the nationality or habitual residence of those individuals is irrelevant.

This implies that, for example, in a situation where a U.S. company that processes personal information of EU citizens in the U.S. for a service provided in the U.S., the EU GDPR would not be applicable to that company. However, if the same company processes personal information of EU citizens or any other persons presently in the EU for a service provided in the

EU, the EU GDPR would be applicable to the company. So, irrespective of whether your organisation is based in Asia, Australia, America or any other continent, the GDPR may apply if your company provides services to, and / or processes the personal data of, individuals in the EU.

Some of the most commonly impacted industries and organisations include:

1. Industries that provide services to individual customers: Industries wherein the core business is to provide services to individual customers generally include the processing of personal data on a large scale. These industries would include financial services, insurance, retail, etc. All of these companies would need to take significant steps to comply with the EU GDPR.

2. Industries that provide marketing, business, process and system support services: A significant number of organisations provide business, process or system management services. All of these companies will become processors of personal data on behalf of their controllers (by whom they are contracted). While their controllers need to be GDPR-compliant, the GDPR also demands that processors be compliant, and they have the same liability if they do not fulfil this obligation. These organisations will include cloud-based services, platform-based services, law services, analytics, event management, marketing companies, etc.

3. Automobile industry: Most automobile manufacturers love to collect and process personal data about who buys their products. But, with the GDPR being applicable, these companies would need to be more transparent with regard to what data they have, what they do with it, and why.

4. **Professional organisations:** Most clubs or member organisations like football clubs, fitness clubs, golf clubs, tennis clubs, etc. collect the personal data of their members. At present, these organisations may not be transparent about what they collect and why; but, with GDPR coming into effect, the transparency requirements shall apply to these companies if their members are in the EU.

5. **Non-profit organisations and charities:** Charities and non-profit organisations usually collect personal data. In some cases, they also keep information about the bank details of their members. At present, these organisations may not be obliged to disclose what personal data they collect and why, but with the GDPR coming into effect, the transparency requirements shall also apply to these companies if their members are in the EU.

In short, GDPR shall apply to your organization if your process personal data of individuals in EU - this is irrespective of what industry the company may be operating in. The only thing that shall matter is whether the individuals are in EU or not, and whether the data being collected or handled is personal or not.

1.2 The positive side of the GDPR

While the GDPR applies to most organisations, the benefits a company can achieve by taking steps towards compliance are often misunderstood. Some examples of GDPR requirements and their benefits include:

1. **Make a register of data processing**. That is, list what personal data is being captured, as well as when, for what purpose, and so on. This will bring a lot of insight into the data that exists in your company. Once your

company knows all this, your investments into data analytics will become much more valuable than the typical current approach of taking your CRM systems and starting to analyse them.

2. **Demonstrate transparency**. Specify what data you collect, why you collect it and how you process it. Again, doing so requires a huge effort, but once done correctly, your customers will have a lot of trust in what you do and why. Once they understand this, and feel confident about your approach, they should trust your company more. And, we all know that customer trust is one of the core elements in the growth of any business.

3. **Minimise the data that is collected**. Now, this is easier said than done, but if a company really invests in minimising the data that is being collected, there can be immense benefits: business processes will become efficient, the costs of storing data will be reduced because you reduce the data that is captured, and so on.

4. **Secure the personal data**. Security of data has always been a big topic, but not every company has done enough. Now, the GDPR asks for ensuring the security of personal data, and if this is done well, it should reduce the number of personal data breaches. And, if the number of breaches is reduced, it is certainly very good for business when examined through cost, reputation, and many other perspectives.

The GDPR is not about fines, but about being transparent and accountable while protecting personal data. If you do this well, your company has an opportunity to increase customer trust, generate more business and reduce threats of personal data breaches. So, next time you have a conversation about the GDPR, start with why it will be good for your business. And, being in business yourself, you should be able to think of many more reasons than the ones listed above.

1.3 How is this book structured?

Before we begin, I would like to suggest two points that will greatly increase the value you get from this book. First and foremost, I want to emphasise that this is not a book that you read once and then forget about. To begin, read it completely once; then, refer back as you start your GDPR compliance journey.

Second, I would like to make it explicit that this is not legal advice; rather, this is my personal perspective on the GDPR for anyone willing to learn about the regulation. The content in this book is not my experience with any one organisation for which I work or have worked; it is the sum total of what I have observed and learned throughout my career thus far. Hence, expect this to provide you with general information about the GDPR and ideas on how best to implement GDPR compliance.

To make it easier for you, each chapter ends with a section called "Success factors", which will assist you in implementing the GDPR quickly and more effectively through key actions you may take. Some chapters also include a "Free tool tip", which provides a link to a completely free tool that will help you on your way toward compliance.

And, if you use this book as intended, I am confident that you will gain a better understanding of the GDPR and decide on the best compliance approach for your company.

1.4 Who is this book for?

Company executives are becoming increasingly concerned about the impact of the new General Data Protection Regulation that takes effect on 25 May 2018. Most of them understand that this new law will have a huge impact, but the extent and areas of impact are not always clear. In such situations, you need a simple and easy-to-follow explanation of the core requirements of the GDPR. Ideally, this information should include actionable suggestions. If you find yourself in need of this sort of help, then this book is your solution.

The ideal reader of this book is any person who seeks to understand the General Data Protection Regulation from a perspective of understanding core requirements. The book is particularly suited for persons in companies aspiring to become GDPR-compliant.

1.5 Additional resources

Here are some resources that will help you, together with this book, to learn about the GDPR:

- EU GDPR online courses – free online courses that will teach you GDPR basics.
- EU GDPR free downloads – a collection of white papers, checklists, diagrams, templates, etc.
- EU GDPR tools – a couple of free tools like the EU GDPR Readiness Assessment Tool and the full text of the EU GDPR.
- Conformio – a cloud-based document management system (DMS) and project management tool focused on ISO standards and other frameworks and regulations.
- EU GDPR Documentation Toolkit – a set of templates of all the documentation that is required by EU GDPR, with included expert support for the implementation.

2. ORIGIN OF PRIVACY AND GDPR BASICS

2.1 Introduction

This chapter focuses on the concept and history of privacy while providing insights into some of the basics of the General Data Protection Regulation. At the end of this chapter, you shall understand that privacy is not a new topic, but one that has been in existence for a long time. You will also become familiar with the objectives of the EU GDPR. The GDPR concepts and requirements discussed in this chapter can be found in Article 4 of the EU GDPR 2016/679 text.

2.2 History of privacy

Ever since the origin of mankind, there has been an aspect of human beings wherein we want to be able to keep certain aspects of our lives to ourselves, and share these aspects selectively with those whom we trust. This aspect of being able to keep information, data or facts to oneself and share selectively based on choice is called "privacy". So, privacy is an important aspect of life and is not a new thing; rather, it is a concept that has existed for ages.

Some of the legislation on privacy can be traced back to the Privacy Act of 1974 in the United States, wherein individuals' right to access and correct personal information was formally stated. This was followed by various guidelines and laws on privacy from the Organization for Economic Cooperation and Development countries, which are also known as OECD countries. All the same, the EU Data Protection Directive of 1995, reference 95/46/EC, provides one of the first formal adoptions of privacy principles in Europe. This directive mandates comprehensive protection of personal information and puts clear restrictions around data transfers. It also determined that data could be transferred to a third country, if that country offers an adequate level of protection.

So, data privacy and protection are not entirely new topics.

However, the evolution of technology, internet and social media in the last two decades or so means that individuals and organisations have much more at stake in terms of their privacy. This change has called for privacy rules that are more explicit in definition and scope. Hence, the European Commission decided to come up with this new regulation, which was named the "General Data Protection Regulation". So, the GDPR is the latest, and arguably the most sophisticated law when it comes to privacy.

2.3 What is the GDPR?

The GDPR is a set of rules that define guidelines for processing the personal data of natural persons (which simply means individual human beings, as opposed to a legal "person", like a company). These natural persons could be your customers and / or employees, or the employees of suppliers to your company. These natural persons are consistently referred to as "data subjects".

The GDPR is set to replace the existing EU Directive 95/46/EC on 25 May 2018, and covers:

- guidelines for companies on what is expected from them when they process the personal data of EU citizens

- rights of data subjects
- powers of the supervisory authority

2.4 Objectives of the GDPR

Here is what the GDPR wants to achieve:

- to protect the freedom and rights of EU citizens
- to enable free movement of personal data across EU states while, at the same time, stipulating guidance for movement of personal data outside of the EU

2.5 Who does the GDPR apply to?

The GDPR applies to all companies around the world that process the personal data of persons inside the EU. It is not applicable when:

- processing of personal data is purely a personal or household activity – for example, when personal data is being processed within a family
- processing is for prevention of criminal offences

Free tool tip: This EU GDPR Foundations Course will explain all the basics of the regulation.

2.6 Related frameworks (ISO 27001 and other)

While the GDPR is the European regulation on privacy, one should be aware that the International Organization for Standardization has published standards and guidelines for security of data in the ISO 27000 series. Specifically, ISO 27001 explains how to structure the information security documentation, and requires an organisation to apply only those security controls or safeguards that are necessary to its business. It provides the tools needed to permanently review the entire Information Security Management System (ISMS) and improve it whenever possible, and to make company employees aware of the importance of information security.

In addition, there is the ISO/IEC 29100 privacy framework. It provides privacy terminology, roles and responsibilities, considerations to safeguard privacy and references to privacy principles for IT implementation.

Also, OECD continues to work on its privacy framework and publish guidance for the data-driven economy. This framework provides principles for data flow in cross-border situations and goes deep into the risks associated with data transfers.

There are many more standards and best practices. In short, when implementing the GDPR, one should consider leveraging best practices from one or more of these existing standards, even though they are not mandatory requirements of the GDPR.

2.7 e-Privacy regulation

The e-Privacy regulation is set to become the replacement for the current e-Privacy directive, and its purpose is to align online privacy rules across all EU member states. Online privacy rules cover topics such as cookies, unsolicited marketing and online communications.

It is important to note that this regulation is still in draft form, but it has been vetted extensively by member states and now awaits the approval of the EU parliament. So, for now, the old e-Privacy directive and local privacy laws remain in force, but the e-Privacy regulation is expected to go into effect sometime during 2018.

Though they are two different regulations, there are some similarities between the e-Privacy regulation and the EU GDPR:

- Both are regulations. This means that both shall become de-facto law in all EU member states. Therefore, member states do not need to create local laws.
- Both will impose high fines for non-compliance. If the EU parliament approves the current draft, the maximum fine would be similar to that imposed by the EU GDPR, i.e., 4% of total annual turnover or € 20 million, whichever is higher.
- Both regulations relate to the protection of personal data of data subjects who are in the EU.

Let us now understand the key differences between the two regulations.

- The GDPR was created to provide protection for the personal data of individuals; i.e., a data subject has rights and is informed about what processing is being carried out on his or her personal data. The e-Privacy regulation was created to provide privacy in private and family life; i.e., the data subject is aware of and can make choices in the context of communications that impact him or her. And, in the case of e-Privacy, the user may be either an individual or a legal entity.
- The EU GDPR defines requirements for the handling of personal data, while the e-Privacy regulation will define requirements for online communications.

- The GDPR comes into effect on 25 May 2018, while the e-Privacy regulation is still in the approval stage with the EU parliament.

When the e-Privacy regulation goes into effect, the rules around content and metadata of electronic communications may be specified further. Most likely, these will include:

- electronic communications like text or voice messages, audio, video and images
- interpersonal communications like WhatsApp, Skype, e-mail, etc.
- sending direct marketing communications, etc.

With the EU GDPR already in place, the e-Privacy regulation is aimed at enabling the Digital Single Market Strategy of the EU, as the focus of the Strategy is to create trust and security in digital services. The GDPR and the e-Privacy regulation are complementary, and they both strengthen the privacy and protection requirements to ensure that personal data is protected at all times.

Because the content and metadata of communications use personal data processing that is governed by the GDPR, these regulations will have some overlap. The full extent and impact of this overlap will be determined once the final text of the e-Privacy regulation is approved.

For now, until the e-Privacy regulation is published, it is important that you do your utmost to comply with the EU GDPR.

2.8 Key terms in the GDPR

Before we move into further details, it is important to familiarise ourselves with the definitions of key terms that form the basis of the GDPR, and will be used frequently in subsequent chapters.

Personal data: As per the GDPR, any information that can be used, either directly or indirectly, to identify a natural person, i.e., a data subject, is referred to as "personal data". This means that ID number, IP address, name, email, home address, date of birth, etc. would all be classified as personal data.

Special categories of personal data: Personal data revealing race or ethnic origin, religious beliefs, health, sex, biometric info, political opinions, criminal history, etc. are classified as "special categories" of personal data. Such information is also referred to as "sensitive data" by some experts.

Processing: Processing is any operation that is performed on personal data. This constitutes actions like collection, recording, storage, usage, modification, linking, sending or deleting personal data. So, even the reading of customer data by an external provider would constitute processing of personal data.

Profiling: Profiling is any automated operation that is performed on personal data to analyse or predict certain aspects of a natural person. These aspects may be economic situation, health, behaviour, etc. For example, a website that provides loans to individuals may ask questions and process answers to make judgments on their creditworthiness. This processing of personal data to make judgments would be classified as profiling.

Controller: A natural person or legal entity that processes the personal data of data subjects can be classified as either a controller or a processor. A controller is the natural person or legal entity that determines the purposes and means of the processing of personal data (e.g., when processing employees' personal data, the employer is considered to be the controller). It is possible to have joint data controllers in certain circumstances. For example, when a company operates in multiple countries, but decisions on processing purposes are being made both by central and local entities, the combined entities in this scenario would qualify as a joint controller.

Processor: A natural person or legal entity that processes personal data on behalf of the controller (e.g., call centres acting on behalf of their clients would be considered processors). At times, a processor is also called a "third party".

Recipient: A natural person, legal entity or public body to which personal data is disclosed in accordance with the law.

Data Protection Officer: The Data Protection Officer (DPO) is a leadership role required by the EU GDPR in companies that process the personal data of EU citizens, though the regulation does not require this to be a single, dedicated person. A DPO is responsible for overseeing the data protection approach and strategy, and their implementation. In short, the DPO is responsible for GDPR compliance. It is possible that certain companies can choose not to appoint a DPO, and instead assign the responsibility to an existing person in the organisation (for example, the head of the legal department). Normally, the choice of appointing a DPO, or not, is based on the scale of the personal data that is processed in the company. For example, a small company that offers analytical services on medical records should have a DPO because they process the personal data of patients, while a mid-sized manufacturing company may choose not to have a DPO, as the only personal data they process is that of staff and suppliers.

Supervisory authority: A supervisory authority is a public authority in an EU country (also known as a “member state”) responsible for monitoring compliance with the GDPR. This is typically a privacy commission, a data protection authority, or some equivalent organisation in each member state. It may have a different name in each country; for example, in the UK it is the Information Commissioner’s Office. The GDPR envisages that in the future, there will also be a European Data Protection Board that unites all the presidents of such local data protection authorities.

Lead supervisory authority: A controller or processor that has operations in multiple countries can choose to appoint a single supervisory authority as their lead supervisory authority (LSA). Once appointed, the LSA becomes the primary contact for GDPR compliance matters like registration of a Data Protection Officer, data breach notifications, etc.

When a company chooses an LSA, it is possible that a data subject could lodge a complaint with a supervisory authority other than the one chosen as LSA. In such circumstances, the supervisory authority informs the LSA without delay. And, within three weeks, the LSA decides which supervisory authority will handle this complaint. Either way, both would cooperate in line with the requirements stated in the GDPR; i.e., the draft decision would be shared with both.

Pseudonymisation: Pseudonymisation is a technique of replacing one or more attributes of personal data to make identification of a natural person difficult. This is simple and straightforward, but it is a reversible process in that personal data can be retrieved based on a certain key or handle. Because this personal data can be restored, pseudonymised data is still considered personal data within the scope of the GDPR.

Anonymisation: In contrast, anonymisation is a technique of replacing one or more attributes of personal data to make identification of a natural person impossible. This is generally a complex and irreversible process. As personal data can no longer be identified, the anonymised data is not considered personal data within the scope of the GDPR.

A simplified example of these two terms could be when some customer data attributes, like customer ID, account ID, name, date of birth, etc., are substituted with fictitious values to make identification of the customer more difficult. Now, if the logic for the replacement of data is stored to allow reverse engineering to restore the original data, it is pseudonymisation. However, if the logic is much stronger, random and not stored, it is impossible to restore the data, and the process is anonymisation. The example has been simplified for description, though in reality, the processes can be complex to implement.

2.9 Myths about the GDPR

Being a new topic, there are some myths that surround the GDPR. Let us look at some of these to start understanding what the GDPR is *not*.

The GDPR is only applicable in the EU

This is one of the most common myths – that the GDPR is an EU law, so it only applies to EU companies. The fact is that the GDPR is applicable to all companies that process the personal data of people within the EU. This is true irrespective of where the company is located. So, lots of non-European companies, especially those in the Americas and Asia, will fall within the scope of the GDPR and must comply with it.

Consent is the only way to process personal data

This is also a common myth – that consent is required for all processing of personal data. The fact is that consent is one of six legitimate purposes, not the only option for processing personal data. And, in my view, this should not be the starting point when companies are considering the processing of personal data. I say this because consent can be withdrawn by the data subject at any time; and, if it is withdrawn, the controller and processor must stop processing that personal data. So, the choice to use consent as the sole basis for processing should be evaluated carefully.

The GDPR is about fines

Another common myth is that the GDPR is all about fines. The fact is that the GDPR is about putting the data subject first. Yes, non-compliance with the GDPR can invite hefty fines, but these are likely to be the last resort when the warning(s) of the supervisory authority have been ignored. The objective of the GDPR is to make organisations follow accountability and transparency, rather than the supervisory authority having to ask for reports and documents.

All organisations need a DPO

The final myth we will discuss is that each and every organisation needs to appoint a Data Protection Officer. The fact is, a DPO should be assigned if your organisation is a public authority or engages in large-scale processing of personal or sensitive data. If your organisation does not meet these criteria, then you do not need to assign a DPO. This is a decision to be made by the management of your company while considering the requirements of the GDPR and the need for the DPO role.

Be aware that there are many other myths surrounding the EU GDPR. So, focus on finding facts so that you know what is a myth, and what is a fact. Separating myths from facts will allow you to take an objective and rational view of GDPR requirements based on key GDPR principles. This will allow you to take the right steps in your implementation of the GDPR.

2.10 Business activities that are most impacted by the GDPR

It is likely that the GDPR will have a significant impact on certain parts of your organisation. Departments feeling the biggest impacts may include:

Marketing: Because marketing departments now process personal data to create personalised or targeted campaigns towards customers, it is likely that their analysis process may need to change, because customers can exercise their rights to stop such processing.

IT: Because any action on personal data is processing, and personal data needs to be protected, most IT systems will need to ensure that privacy principles are thought through when systems are being designed. This is likely to create a need for architects who understand the GDPR.

Procurement: Because of the obligations that processors will have when processing data, procurement departments will need to educate procurement officers to ensure that personal data protection is adequately covered in contracts being signed with processors.

Legal: As teams in organisations take time to understand the GDPR and its consequences, it is likely that legal departments will have more queries, and even customer queries. This would result in a need for privacy specialists who are knowledgeable about the GDPR and other laws.

Human resources: Human resources (HR) teams process personal data of employees, and now they need to be aware of GDPR requirements before processing such personal data, and they need to inform employees as well.

Privacy specialists: In addition, in the longer term, large companies will likely set up privacy offices or departments to handle privacy-related matters. The Data Protection Officer is already one such role that is mandatory.

Key timelines

The final text of the GDPR was approved on 25 May 2016, and organisations were provided a two-year period to take compliance actions in relation to data privacy and protection. So, the GDPR comes into effect on 25 May 2018.

2.11 Success factors

Your success will be enhanced significantly if you develop a thorough and deep understanding of the following:

- The concept of privacy has existed for ages, but the advent of internet and social media means that the rules of privacy need to be explicit.
- The EU General Data Protection Regulation is a new privacy law in Europe that empowers individuals with rights, asks organisations to be accountable and transparent about processing of personal data, and provides supervisory authorities with sanction powers.
- Key terms in the context of privacy include "personal data", "processing" and "Data Protection Officer". You should take time to understand these key terms.

.

BIBLIOGRAPHY

'Be Ready for GDPR' by Punit Bhatia

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Articles at https://advisera.com/eugdpracademy/blog/

EU GDPR Guide at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Privacy by design https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

DPIA guidance https://www.cnil.fr/en/guidelines-dpia

Consent guidance https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/23--guide-to-the-gdpr--consent.pdf?la=en

Retention http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

Lead supervisory authority http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

INDEX

Intro to GDPR

A Plain English Guide to Compliance

All the knowledge you need about the EU GDPR privacy regulation is written in plain English and presented in this practical guide.

Introducing the new book by Punit Bhatia: Intro to GDPR. Punit has served as the Privacy and Protection Officer in an EU-based bank and a lecturer at the Solvay Brussels School of Economics and Management. He is a Certified Information Privacy Professional - Europe (CIPP-E), Certified Information Privacy Manager (CIPM), and Certified Outsourcing Professional (COP). The book is filled with all the knowledge you need to fully understand the requirements of the new General Data Protection Regulation. It is written in an easy-to-follow format that even beginners can understand. No matter whether you have previous knowledge of data protection or you are new to the field, this book is a must-read.

- ✓ This plain English handbook explains all GDPR requirements
- ✓ Learn which companies the GDPR applies to
- ✓ Get the knowledge you need to start a compliance project
- ✓ Develop a structured privacy notice and other mandatory documentation
- ✓ Make sure your company is fully compliant with the GDPR

Written in plain English, *Intro to GDPR* is a practical guide for normal people. Whether you're experienced in data protection or new to the field, it's the only book you'll ever need on the subject.