

# GDPR Gap Analysis by Article

Evaluating Gaps in GDPR Compliance Better

John Kyriazoglou



JOHN KYRIAZOGLU

---

# **GDPR GAP ANALYSIS BY ARTICLE**

**EVALUATING GAPS IN GDPR  
COMPLIANCE BETTER**

GDPR Gap Analysis by Article: Evaluating Gaps in GDPR Compliance Better

1<sup>st</sup> edition

© 2019 John Kyriazoglou & [bookboon.com](http://bookboon.com)

ISBN 978-87-403-3079-3

# CONTENTS

	<b>Preface: Why you need a GDPR GAP Analysis</b>	<b>6</b>
<b>1</b>	<b>Introduction to GDPR GAP Analysis</b>	<b>8</b>
1.1	Introduction to Gap Analysis	8
1.2	Risk Assessment vs. Gap Assessment	9
1.3	GDPR Gap Analysis	9
<b>2</b>	<b>Executing a GDPR GAP Analysis -Part 1</b>	<b>12</b>
2.1	Analyzing Gaps in DP Area 1: Personal Data Management	12
2.2	Gap Analysis for Issues 1 – 7	12
<b>3</b>	<b>Executing a GDPR GAP Analysis-Part 2</b>	<b>27</b>
3.1	Analyzing Gaps in DP Area 2: Organizational and Legal Issues	27
3.2	Gap Analysis for Issues 8 – 13	27
<b>4</b>	<b>Executing a GDPR GAP Analysis-Part 3</b>	<b>39</b>
4.1	Analyzing Gaps in DP Area 3: Technical Issues	39
4.2	Gap Analysis for Issues 14 – 20	39
4.3	Conclusion and next steps	52

www.sylvania.com

**We do not reinvent  
the wheel we reinvent  
light.**

Fascinating lighting offers an infinite spectrum of possibilities: Innovative technologies and new markets provide both opportunities and challenges. An environment in which your expertise is in high demand. Enjoy the supportive working atmosphere within our global group and benefit from international career paths. Implement sustainable ideas in close cooperation with other specialists and contribute to influencing our future. Come and join us in reinventing light every day.

Light is OSRAM

**OSRAM  
SYLVANIA**

<b>Appendix 1. Operating Framework of 'XYZ' Corporation</b>	<b>53</b>
<b>Appendix 2. Privacy Risks</b>	<b>54</b>
<b>End Notes</b>	<b>55</b>
<b>Further Resources</b>	<b>57</b>
<b>Disclaimer</b>	<b>58</b>

# PREFACE: WHY YOU NEED A GDPR GAP ANALYSIS

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for organisations on the collection and processing of personal information of individuals within the European Union (EU).

Businesses and public organizations need to assess their obligations and update their policies, processes and systems to comply with the Regulation. Key requirements of GDPR include transparency, rights of data subjects, consent, and security, etc.

Most, if not all GDPR (General Data Protection Regulation) compliance projects start with a GDPR gap analysis according to consulting practice in a variety of industries and several countries.

If your company is in the early stages preparing for GDPR, a Gap Analysis is a great way to understand how the regulation applies to your organisation and to review the critical, high risk or weak areas of your systems and data processes.

Also, if you want to audit your GDPR Compliance after the implementation of your initial GDPR measures, you may also need to conduct a GDPR Gap Analysis.

In general, a gap analysis is a popular method of assessing compliance against the requirements of the GDPR. It will help you identify the GDPR compliance issues and support you to prioritise the areas that you should effectively address.

A gap analysis is performed by an individual with in-depth expertise of the GDPR's requirements, and a deep understanding of the practical realities of implementing suitable processes, controls and other measures to help the organisation achieve compliance.

A gap analysis will prepare your company better and enable it to take the necessary actions in order to avoid the costly GDPR fines and sanctions by the relevant GDPR Data Protection Authority in your country.

These fines are 2 types:

**Type 1. Administrative fines** are up to €10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, in case of a violation of: obligations of the controller and the processor pursuant to Articles 8, 11, 25 - 39, 42 and 43 and obligations of the monitoring body pursuant to Article 41(4).

**Type 2. Fines of up to €20,000,000 / 4% of turnover where there is a violation of:**

2.1. The basic principles and consent (Articles 5, 6, 7 and 9).

2.2. The data subjects' rights (Articles 12 to 22).

2.3. The transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49.

2.4. Any obligations pursuant to Member State law adopted under Chapter IX (specific processing situations – article 85 - 91).

2.5. Non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority (Article 58).

# 1 INTRODUCTION TO GDPR GAP ANALYSIS

**Overview:** This chapter defines what a GAP Analysis is, the differences between GAP and Risk assessment and the steps required to perform a GDPR GAP Analysis.

## 1.1 INTRODUCTION TO GAP ANALYSIS

Gap analysis is a formal study of what a company or organization is doing currently and where it wants to go in the future.

A gap analysis is an examination of your current performance for the purpose of identifying the differences between your current state of business and where you would like to be.

In management literature, gap analysis involves the comparison of actual performance with potential or desired performance. If an organization does not make the best use of current resources, or forgoes investment in capital, personnel, technology, or other resources, it may produce or perform below an idealized potential.

A gap analysis may also be referred to as a needs analysis, needs assessment or needs-gap analysis.

It can be conducted, in different perspectives, such as:

1. Corporate strategic direction
2. Product or services development
3. Human Resources
4. IT (software development)
5. Compliance (GDPR, ISO 27001, etc.).

In IT (software development), gap analysis tools can document which services and/or functions have been accidentally left out, which have been deliberately eliminated, and which still need to be developed.

In GDPR compliance, a gap analysis can compare what is required by the EU General Data Protection Regulation and each specific article or assessment criterion to what is currently being done to abide by them.



## 1.2 RISK ASSESSMENT VS. GAP ASSESSMENT

**Risk assessments** differ from gap assessments in their essential purposes. According to the ANSI/ASIS/RIMS risk assessment standard (<https://webstore.ansi.org/standards/asis/ansiasisrimsra2015>, <https://www.rims.org/about-us/newsroom/rims-and-asis-international-release-new-risk-assessment-ansi-standard>), risk assessments include the identification, analysis and evaluation of uncertainties to objectives and outcomes of an organization.

Risk assessments provide a comparison between the desired and undesired outcomes and expected rewards and losses of organizational objectives.

Risk assessments analyze whether an uncertainty is within acceptable boundaries and within the organization's capacity to manage risk. The results inform decision-makers of the choices available to manage risk effectively to achieve the organization's objectives, given its priorities.

**Risk assessments** take into account the dynamic nature of the organization's external and internal environments. While considering and possibly evaluating the effectiveness of current controls, risk assessments generally focus on the future, at times using multiple scenarios in light of emerging issues.

**Gap analyses**, on the other hand, are intended to identify differences and considerations between "what is" and "what should be." They tend to represent a point in time, focusing on specific controls or activities as they exist for the single purpose of improving the current environment. Gap analyses generally are not suitable for more complex issues that require a deeper understanding of risk and the use of more sophisticated risk assessment techniques.

If used as a risk assessment, gap analyses may give a false impression that filling gaps will be enough to manage all potential future risk events and trends. Gap analyses may give equal weight to any type of control or activity, without regard to the respective impact that each control or activity may have, or on possible related upstream and downstream interdependencies.

## 1.3 GDPR GAP ANALYSIS

Conducting a GDPR gap analysis can help you improve your business efficiency, your product, your GDPR compliance and your profitability by allowing you to pinpoint "gaps" present in your company operations. Once you complete it, you will be able to better focus your resources and energy on those identified areas in order to improve them.

**This Gap Analysis is part of Step PR4 of ‘GDPR Gap Tool 8: GDPR Compliance Action Plan’.**

A Gap Analysis in GDPR terms usually involves a Compliance Assessment Coding system and a process as defined next.

### 1.3.1 COMPLIANCE ASSESSMENT CODING SYSTEM

The following compliance coding system denotes, at a high level, how to record the Compliance Answers to each compliance question:

- **Compliance Answer: ‘FC’** means Full Compliance for GDPR based on what we know at the time the Gap Analysis was carried out (assessment score=10).
- **Compliance Answer: ‘PC’** means Partial Compliance for GDPR based on what we know at the time the Gap Analysis was carried out (assessment score= 1 to 5).
- **Compliance Answer: ‘NC’** means NC Compliance for GDPR based on what we know at the time the Gap Analysis was carried out (assessment score=1).
- **Compliance Answer: ‘N/A’** means Not Relevant for GDPR based on what we know at the time the Gap Analysis was carried out.

If the compliance answer is ‘FC’ (full compliance) or ‘PC’ (partial compliance) you may want to assess the existing control according to the following rating:

1. **Suitability: Yes or No.** Suitability is the fitness of the specific control for its defined purpose. For example, is the control suitable to direct and control activities of the organization to achieve its quality objectives in the Personal Data Inventory?
2. **Adequacy: Yes or No.** Adequacy is the sufficiency of the specific control to meet requirements. For example, is the Personal Data Inventory adequate to satisfy the applicable GDPR Article 30 regulatory requirements?
3. **Effectiveness: Yes or No.** Effectiveness is the extent to which planned activities are accomplished and the planned results are achieved. For example, to what degree is the Personal Data Inventory representing the actual personal data flows and processing activities of all business functions of the company?  
This rating (**Suitability/ Adequacy/ Effectiveness**) is usually part of a full data protection audit which is outside the scope of this book (GDPR Gap Analysis).

### 1.3.2 GDPR GAP ANALYSIS PROCESS

This process is carried out at 2 levels:

**Level 1 (Vertical Axis):** By GDPR article organized in 3 DP Areas ('Personal Data Management', 'Organizational and Legal Issues', 'Technical Issues'). This entails the assessment of how the company complies with each specific GDPR article's requirements (see Chapters 2 to 4 of this book) on the basis of specific questionnaires and the Compliance Assessment Coding System, defined previously (see paragraph 3.1 above).

**Level 2 (Horizontal Axis):** By Business Function and Process. This includes the navigation across the whole organizational chart and structure of the given company and assessing the compliance of the company's functions and processes that include PD on the basis of 5 criteria ('Principles relating to processing of PD', 'Legal basis of processing of PD', 'Consent of DS', 'Transparency Rights of DS', 'Access and Other Rights of DS') and compliance evidence, as detailed in book 3 'GDPR GAP Assessment by Process'.

The steps of this process at each level are:

**Step 1: Identifying the current state of your compliance.**

**Step 2: Identifying where you want to be as regards the requirements of each article (or criterion) of GDPR.**

**Step 3: Identifying the gaps in each requirement or criterion.**

**Step 4: Designing improvements to close the gaps in each identified article and requirement (or criterion).**

**Step 5: Executing the required actions that close the gaps identified previously.**

These steps are detailed in the next chapters of this book and in the third book of this series of Gap books.

It should also be noted that Book 2 ('Gap Tools') is designed to support and complement and support this book as well as the third book ('Gap Analysis by Process').

*In addition to the examples of improvements noted in the analysis of the requirements of each GDPR article (next chapter), you may use and implement the set good practices included in an integrated data protection system proposed in my books listed in 'Further Resources' at the end of this book.*

## 2 EXECUTING A GDPR GAP ANALYSIS -PART 1

**Overview:** This is the first part, ‘Analyzing Gaps in DP Area 1: Personal Data Management’, of the three-part GDPR GAP Analysis. This chapter assesses the gaps for the first DP Area and for all GDPR relevant articles grouped in 7 Data Protection (DP) issues such as: Personal Data (PD) Processing, Scope of application, Legal Basis of Processing, etc. Chapters 3 and 4 contain the other 2 parts (2 and 3) respectively. This Gap Analysis is based on the operational characteristics of the example company ‘XYZ Corporation’

### 2.1 ANALYZING GAPS IN DP AREA 1: PERSONAL DATA MANAGEMENT

#### Introduction

The GDPR Gap Analysis included in this chapter begins to assess the gaps of the example company (‘XYZ Corporation’) for the first DP Area and the issues contained in it, in full compliance with the relevant GDPR Articles (3, 4 (1, 13, 14, 15), 5-10, 12 – 14, 15 - 22, 24, 26 – 28, 32, 88, 90, etc.) and Recitals (22 – 25, 38, 40 – 56, 58, 59, 63 – 71, 73, 75, 156, etc.), by using the 7 questionnaires (with 51 questions) and other assessment actions described next.

### 2.2 GAP ANALYSIS FOR ISSUES 1 – 7

#### Issue 1: Personal Data (PD) Processing

##### 1.1. Description of GDPR requirements (Issue 1)

The GDPR applies to all personal data that is collected in the EU, regardless of where in the world it is processed. Any database containing personal or sensitive data collected within the EU will be in scope, as will any media containing personal or sensitive data. Any organisation that has such data in its systems, regardless of business size or sector, will have to comply with the GDPR.

Personal data (PD) is anything that can identify a ‘natural person’ (“data subject”); and can include information such as a name, a photo, an email address (including work email address), bank details, posts on social networking websites, medical information or even an IP address, etc. This definition is critical because EU data protection law only applies to personal data. Information that does not fall within the definition of “personal data” is not subject to EU data protection law.

‘Sensitive Personal Data’ are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

For more details, see GDPR articles 4 (1, 13, 14, 15), 5-10, 12.

## 1.2. Current GDPR Compliance Assessment (Issue 1)

*This questionnaire relates to assessing the gaps of the example company (‘XYZ Corporation’).*

Question 1. Do you process PD (GDPR Article 4,1)?

*Answer: ...X...(YES).....(NO)*

Question 2. Do you process sensitive data (GDPR Article 9)?

*Answer: ...X...(YES).....(NO)*

Question 3. Have you conducted a Personal Data Audit?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Does your Personal Data Audit contain:

- What personal data you hold?
- Where it came from?
- Who you share it with?
- Legal basis for processing it?
- What format(s) is it in?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Do you have documented procedures for obtaining, processing and storing personal data?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Is personal data:

- processed lawfully, fairly and in a transparent manner?
- collected for specified, explicit and legitimate purposes only?
- adequate, relevant and limited to what is necessary?

- accurate and, where necessary, kept up to date?
- kept only for as long as is necessary and only for the purpose(s) which it is processed?
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 7. Do you identify and establish the legal basis for all personal data that you process?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 8. Do you have a Records Management and Data Retention Policy?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 9. Have the data subjects given explicit consent to the processing of those sensitive personal data for one or more specified purposes?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 10. As regards sensitive data, is the processing necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law?

*Answer: ...X...(YES).....(NO)*

Question 11. As regards sensitive data, is the processing necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent?

*Answer: ...X...(YES).....(NO)*

Question 12. As regards sensitive data, is the processing necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional?

*Answer: ...X...(YES).....(NO)*

Question 13. As regards sensitive data, is the processing necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices?

*Answer: ...X...(YES).....(NO)*

Question 14. If you process personal data relating to criminal convictions and offences (article 10), have you received consent from the data subject?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 15. Do you collect and process PD of children (under 16 years old – GDPR Article 8 και 12)?

*Answer: ...X...(YES).....(NO)*

Question 16. Do you have a PD Inventory (GDPR Article 30 – see GDPR Gap Tool 1 for more details)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 17. Does your PD Inventory document all PD in IT systems, Call center, Digital devices, Fax, CCTV, etc.?

*Compliance Answer: .....(FC)...X..(PC).....(NC)....(N/A)*

Question 18. Are company staff trained on managing the processing of personal data (see end note 1 for more details)?

*Compliance Answer: .....(FC).....(PC) X..(NC)....(N/A)*

### 1.3. Gaps (Issue 1)

*These gaps relate to the example company ('XYZ Corporation').*

1. An inventory of personal data processed by business functions is not complete.
2. A register (inventory) of IT – related assets (systems, hardware, devices, etc.) that process PD is not complete.
3. Staff are not trained on managing personal data.
4. There are no guidelines issued to staff on managing personal data.
5. A Records Management and Data Retention Policy does not exist.



Discover the truth at [www.deloitte.ca/careers](http://www.deloitte.ca/careers)

**Deloitte.**

© Deloitte & Touche LLP and affiliated entities.

## 1.4. Examples of Actions to remedy the gaps of Issue 1

*These actions relate to the example company ('XYZ Corporation').*

1. Both inventories (PD, IT Assets) need to be completed. You may use 'GDPR Gap Tool 1: GDPR PERSONAL DATA INVENTORY Template' to record the processing of personal data.
2. Company management must assign the responsibility of managing these inventories to two distinct staff: One for the personal data and one for the IT – related assets.
3. Train staff on managing personal data.
4. Draft and issue PD Management Guidelines to staff.
5. Implement a Records Management and Data Retention Policy.

## Issue 2: Scope of Application

### 2.1. Description of GDPR requirements (Issue 2)

This Regulation (GDPR) applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union (EU), regardless of whether the processing takes place in the EU or not.

GDPR also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

the monitoring of their behaviour as far as their behaviour takes place within the Union.

This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

For more details, see GDPR articles 3, 24, 26 – 28 and recitals 22 – 25.

### 2.2. Current GDPR Compliance Status (Issue 2)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Where are your central offices (GDPR Article 3)?

*Answer: <any street 21, any town, Germany>*

Question 2. Are you a controller (GDPR Article 24)?



*Compliance Answer: ...X...(YES).....(NO)*

Question 3. Are there joint controllers (GDPR Article 26)?

*Compliance Answer: .....(FC).....(PC).....(NC).X...(N/A)*

Question 4. Do you have a company outside of EU that monitors the behavior of EU data subjects (GDPR Article 27)?

*Compliance Answer: .....(FC).....(PC).....(NC).X...(N/A)*

Question 5. Have you appointed an EU representative (GDPR Article 27)?

*Compliance Answer: .....(FC).....(PC).....(NC)..X...(N/A)*

Question 6. Are you a processor (GDPR Article 28)?

*Compliance Answer: .....(FC).....(PC).....(NC)..X...(N/A)*

Question 7. Have you added the details of the Controller to the company's privacy notices and announced them to the relevant Data Protection Authorities?

*Compliance Answer: .....(FC).....(PC)...X...(NC)....(N/A)*

### 2.3. Gaps (Issue 2)

*These gaps relate to the example company ('XYZ Corporation').*

1. The details of the Controller do not exist in the company's privacy notice.
2. These details have not been announced to the relevant Data Protection Authority.

### 2.4. Examples of Actions to remedy the gaps of Issue 2

*These actions relate to the example company ('XYZ Corporation').*

1. The details of the Controller must be added to the company's privacy notice.
2. The details of the Controller must be announced to the relevant Data Protection Authorities.
3. The details of the Controller must be communicated to all corporate staff.

## Issue 3: Legal Basis of Processing

### 3.1. Description of GDPR requirements (Issue 3)

GDPR requires (Article 6) that controllers provide the legal grounds on which personal data can be processed, as well as how to determine when further processing is compatible with the original purposes for processing. Such grounds for processing are: with the data

subject's consent; for contract performance; to comply with legal obligations under Union or Member State law; to protect the vital interests of a natural person; to perform a task in the public interest set out by Union or Member State law; or for the purposes of legitimate interests pursued by the data controller or a third party.

For more details, see GDPR article 6 and recitals 40 – 50.

### 3.2. Current GDPR Compliance Status (Issue 3)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Has, each process of PD a legal basis (GDPR Article 6)?

*Compliance Answer: ...X...(FC).....(PC).....(NC)....(N/A)*

Question 2. Is, the legal basis of each process of PD recorded in the PD Inventory?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3. Is, the PD Inventory reviewed and improved on a continuing basis?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Do, sensitive data, have a legal basis of processing?

*Compliance Answer: ...X...(FC).....(PC).....(NC)....(N/A)*

### 3.3. Gaps (Issue 3)

*These gaps relate to the example company ('XYZ Corporation').*

1. The legal basis is not recorded in the personal data inventory.

### 3.4. Examples of Actions to remedy the gaps of Issue 3

*These actions relate to the example company ('XYZ Corporation').*

1. Ensure the recording of legal basis for all processes of personal data in the company's personal data inventory.
2. Ensure your company is clear about the grounds for lawful processing: check these will still be applicable under the GDPR.
3. Review information sharing agreements for any that rely on legitimate interests and amend, to show either proper legislative basis or consent.

## Issue 4: Consent of Data Subjects

### 4.1. Description of GDPR requirements (Issue 4)

GDPR requires (Article 7) controllers to follow the standard for consent when relying on consent as a legal basis for processing personal data (demonstrable consent) and sensitive personal data (explicit consent).

Also GDPR requires (Article 8) controllers to follow the standard that where the legal basis of consent is being relied on in relation to offering information society services to minors under the age of 16 (or to younger children not younger than 13, if the age threshold is lowered by Member State law), consent must be given or authorised by the holder of parental responsibility over the child. The controller must also make reasonable efforts to verify consent, etc.

For more details, see GDPR articles 7, 8 and recitals 38, 51 – 56, 58.

### 4.2. Current GDPR Compliance Status (Issue 4)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Do you request the consent of data subjects?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 2. Do you use consent when there no other lawful basis of processing?

*Compliance Answer: ...X...(FC).....(PC).....(NC)....(N/A)*

Question 3. Do you have evidence for the proof of consent?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Can the data subjects revoke their consent?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Is there a system for consent management?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. If consent was provided in writing, was it presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 7. Prior to consent, do you inform data subjects of their right to withdraw consent?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 8. Do your agreements restrict processing of personal data in accordance with the agreement unless consent is provided?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 9. Do you obtain parental consent or authorization for the processing of personal data of children?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

*Also use the questionnaire contained in end note 2.*

#### **4.3. Gaps (Issue 4)**

*These gaps relate to the example company ('XYZ Corporation').*

1. The consent basis is not recorded in the various forms and procedures as well as the personal data inventory.
2. A consent management system does not exist.

#### **4.4. Examples of Actions to remedy the gaps of Issue 4**

*These actions relate to the example company ('XYZ Corporation').*

1. Ensure consent, as required, is added in all relevant forms and procedures.
2. Ensure all consent details for all processes of personal data are recorded also in the company's personal data inventory (see Issue 1).
3. Review methods for collecting consent and ensure there is sufficiently robust audit trails
4. Review systems to ensure that they can record explicit consent (if relied upon), including parental consent.
5. Review the ability of systems to record withdrawal of consent especially where information is shared between practitioners and other companies.

### **Issue 5: Transparency**

#### **5.1. Description of GDPR requirements (Issue 5)**

GDPR requires (Article 12) that when data controllers are providing information to data subjects, whether through privacy notices, in communications regarding access, rectification, correction and objection rights, or as part of breach notifications, the communication must be in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, etc.

GDPR requires (Article 13) that where personal data relating to data subjects are collected from the data subject, controllers must provide certain minimum information (e.g., details of controller and data protection officer, purpose of processing, data retention time period, access rights and secondary uses of personal data, etc.) to those data subjects through an information notice, etc.

Also in Article 14, controllers are obliged to provide similar privacy notices where data have not been obtained by the controller from the data subject.

For more details, see GDPR articles 12 – 14 and recitals 13, 58, 62, 100.

## 5.2. Current GDPR Compliance Status (Issue 5)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Do you have policies and procedures that address how information should be provided to data subjects (oral, written, electronic, concise, transparent, intelligible and easily accessible form, using clear and plain language)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 2. Do you have a procedure to confirm the identity of a data subject (as the requestor) prior to the fulfilment of an information request?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3. Do you inform data subjects for the data you collect, the purposes of collection, the retention period and their rights?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. When you collect data not directly from data subjects, do you provide them all the needed information?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Do you have a Privacy Notice or Data Protection Policy relevant to GDPR in the web site of the company?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Do you have an Employee Data Privacy Policy?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 7. Do you have a process to review information requests for legitimacy, unfounded or excessive?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### 5.3. Gaps (Issue 5)

*These gaps relate to the example company ('XYZ Corporation').*

1. Data subjects are not informed about their rights.
2. There is no Privacy Notice or Data Protection Policy.
3. There is no Employee Data Privacy Policy.

### 5.4. Examples of Actions to remedy the gaps of Issue 5

*These actions relate to the example company ('XYZ Corporation').*

1. Ensure a Privacy Notice or Data Protection Policy relevant to these requirements is added to the web site of the company.
2. Ensure an Employee Data Privacy Notice is added to the Company Policies and Procedures Manual.
3. Audit existing privacy notices, review and update them.
4. For data which is collected indirectly, ensure that a notice is given at the appropriate time i.e. website, etc.

## Issue 6: Rights of Data Subjects

### 6.1. Description of GDPR requirements (Issue 6)

Individuals (citizens, consumers, customers, users, employees, etc.) referred to as data subjects under GDPR (or individuals), have different rights regarding the processing of their personal data which the company will fully satisfy, unless there are other legal conditions and actions that do not allow this.

These rights are:

1. **The right of access:** the right of individuals to access their personal data (GDPR Article 15).
2. **The right of rectification:** the right of individuals to correct their personal data if these are inaccurate or incomplete (GDPR Article 16).

3. **The right to erasure ('right to be forgotten')**: allowing a person to request the deletion or removal of his or her personal data if there is no good reason to continue processing (GDPR Article 17).
  4. **The right to restrict processing**: when processing is limited, it is allowed to store personal data but not to process it further (GDPR Article 18).
  5. **The right to be informed of the rectification, erasure or limitation**: data controllers must notify any beneficiary whose data is disclosed, of any correction, deletion or limitation of the processing carried out in accordance with Article 16, Article 17 (1) and Article 18, unless this proves impossible or involves a disproportionate effort (GDPR Article 19).
  6. **The right to data portability**: allows individuals to acquire and re-use their personal data for their own purposes in various services (GDPR Article 20).
  7. **The right of objection**: the right of individuals to refuse the use of their data for processing and direct marketing, including profiling (GDPR Article 21).
  8. **Rights related to automated decision-making and profile creation**: individuals have the right not to be subject to a decision when it is based on the automated processing of their data (GDPR Article 22).
- For more details, see GDPR articles 15 – 22, recitals 50, 59, 63 – 71, 73, 75, 156.

## 6.2. Current GDPR Compliance Status (Issue 6)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Have you established a system to satisfy the rights of data subjects?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 2. Is the controller able to satisfy the requests of data subjects within the required time frame?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3. Is there a policy for satisfying requests for access of data subjects to their data (GDPR Article 15)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Is there a policy for satisfying requests for correction by data subjects to their data (GDPR Article 16)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Is there a policy for satisfying requests for deletion by data subjects to their data (GDPR Article 17)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Is there a policy for satisfying requests for objection of processing by data subjects to their data (GDPR Article 18)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 7. Are third parties informed when personal data are deleted or corrected (GDPR Article 19)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 8. Is there a policy for satisfying requests for portability by data subjects to their data (GDPR Article 20)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 9. Are data subjects informed of their right to object to certain types of processing (GDPR Article 21)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 10. Is there a profiling or automated decision-making procedure (GDPR Article 22)?

*Compliance Answer: .....(FC).....(PC).....(NC).X...(N/A)*

### 6.3. Gaps (Issue 6)

*These gaps relate to the example company ('XYZ Corporation').*

1. There is no system, in operation, to satisfy the rights of data subjects.

### 6.4. Examples of Actions to remedy the gaps of Issue 6

*These actions relate to the example company ('XYZ Corporation').*

1. A system (forms, policies, procedures, technical platform, portal, etc.) to satisfy the rights of data subjects (access, rectification, portability, objection, erasure and restriction of processing) must be crafted and implemented.
2. Audit privacy notices and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of 'first communication'.
3. Ensure that members of staff and suppliers who may receive data erasure requests recognize them and know how to deal with them.
4. Determine if systems are able to meet the requirements to mark data as restricted whilst complaints are resolved, or indeed to delete data as required.



## Issue 7: Employee Personal Data Processing

### 7.1. Description of GDPR requirements (Issue 7)

Employers collect a substantial amount of personal information about their employees. Companies need to be aware of their obligations under the profusion of data protection laws and regulations (e.g., GDPR) that govern the collection, use and transfer of personal information.

Companies use the personal data of their employees for a variety of reasons and purposes including evaluating applicants during the hiring process, administering payroll and employee benefit plans, managing separation and other post-employment benefits, etc.

And as more employers adopt enterprise-level information management systems and, in many cases, outsource certain human resources administration functions to third parties, increasing amounts of personal data is being transferred and shared within and between organizations.

**Also**, GDPR (Article 88) states that member states may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, etc.

For more details, see GDPR articles 5, 6 – 9, 12 – 14, 32, 88, 90.

### 7.2. Current GDPR Compliance Status (Issue 7)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1: Have your HR policies and procedures been reviewed (and if applicable, revised) to ensure that employee's individual rights under the GDPR are considered and complied with?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 2: Do you have a Training and Development Policy?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Do employees have training records, files and annual training assessments?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3: Are employees advised of their own rights under the GDPR?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4: Are employees monitored on an ongoing basis for compliance with the data protection laws (i.e. email checks, account audits, monitoring phone calls, etc.)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5: Have you implemented an Employee Privacy Policy?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Is data protection included in the employee agreements?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 7. Have all employees signed a statement of confidentiality especially when they process personal data?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### **7.3. Gaps (Issue 7)**

*These gaps relate to the example company ('XYZ Corporation').*

1. Employee policies and records are not compliant with GDPR.

### **7.4. Examples of Actions to remedy the gaps of Issue 7**

*These actions relate to the example company ('XYZ Corporation').*

1. Implement an Employee Privacy Policy.
2. Ensure data protection is included in all employee agreements.
3. Ensure all employees sign a statement of confidentiality especially when they process personal data.

***The GDPR Gap Analysis continues in Chapter 3, next.***

# 3 EXECUTING A GDPR GAP ANALYSIS-PART 2

**Overview:** This is the second part, ‘Analyzing Gaps in DP Area 2: Organizational and Legal Issues’, of the four-part GDPR GAP Analysis. This chapter assesses the gaps for the second DP Area and for all GDPR relevant articles grouped in 6 Data Protection (DP) issues such as: Data Protection Principles, Controller Obligations, DPO, etc. Chapters 2 and 4 contain the other 2 parts (1 and 3) respectively.

This Gap Analysis is based on the operational characteristics of the example company ‘**XYZ Corporation**’.

## 3.1 ANALYZING GAPS IN DP AREA 2: ORGANIZATIONAL AND LEGAL ISSUES

### Introduction

The GDPR Gap Analysis included in this chapter carries on from the previous chapter and assesses the gaps of the example company ‘**XYZ Corporation**’ for the second DP Area and the issues contained in it, in full compliance with the relevant GDPR Articles (5, 8, 13, 14, 24, 26 -28, 30 - 33, 35 – 39, 4- 50, 58, 83, 84, etc.) and Recitals (2, 13, 19, 28, 39, 49, 75 - 83, 91, 94, 97, 100, 104, 112, 166, etc.), by using the 6 questionnaires (with 48 questions) and other assessment actions described next.

## 3.2 GAP ANALYSIS FOR ISSUES 8 – 13

### Issue 8: Data Protection Principles

#### 8.1. Description of GDPR requirements (Issue 8)

GDPR requires (Article 5) that the general principles that all processing activities of personal data must abide by, include: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage or retention limitation; integrity and confidentiality; and accountability. Also the accountability principle states that data controllers are responsible for and able to demonstrate compliance with the data processing principles.

For more details, see GDPR article 5 and recitals 2, 19, 28, 39, 49, 77, 78, 79, 94.

## 8.2. Current GDPR Compliance Status (Issue 8)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Do you process PD in a legal, fair and transparent way (GDPR Article 5,1 )?

*Compliance Answer: ...X...(FC).....(PC).....(NC)....(N/A)*

Question 2. Do you use PD only for the purposes for which the PD were initially collected (GDPR Article 5,1b)?

*Compliance Answer: ...X...(FC).....(PC).....(NC)....(N/A)*

Question 3. Are PD restricted to the purposes for which they will be processed (GDPR Article 5,1c)?

*Compliance Answer: ...X...(FC).....(PC).....(NC)....(N/A)*

Question 4. Have you established procedures for ensuring the accuracy of PD (GDPR Article 5,1D)?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 5. Have you included data retention in your privacy notice (GDPR Article 5,1e)?

*Compliance Answer: .....(FC).....(PC)...X...(NC)....(N/A)*

Question 6. Have you established the proper integrity and confidentiality measures (GDPR Article 5,1f)?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 7. Can you show evidence for compliance with data protection principles (GDPR Article 5,2)?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

## 8.3. Gaps (Issue 8)

*These gaps relate to the example company ('XYZ Corporation').*

1. Policies for compliance records, data retention and accuracy do not exist.
2. Security procedures need to be improved.

## 8.4. Examples of Actions to remedy the gaps of Issue 8

*These actions relate to the example company ('XYZ Corporation').*

1. Review current Data Protection policies, codes of conduct and training to ensure these are consistent with the GDPR principles.
2. Undertake a personal data audit to understand what data is held, where it is held, in what format it is held, where it is obtained from, basis for holding it (consent/legal basis).

3. Identify means to 'demonstrate compliance', i.e. How you meet GDPR requirements, following codes of conduct as they are issued, maintain paper trails of decisions relating to data processing and, where appropriate, privacy impact assessments, etc. To this purpose a GDPR system to maintain compliance records needs to be established.
4. Policies for data retention, quality and accuracy must be implemented.
5. Additional security measures must be implemented. For more details, see 'Issue 14: Security of processing'.

## Issue 9: Controller Obligations

### 9.1. Description of GDPR requirements (Issue 9)

GDPR (Article 24) requires the data controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. The appropriateness of these measures is based on a risk assessment that takes into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. There is a specific reference that, where proportionate in relation to the processing activities, data protection policies shall be implemented, etc.

For more details, see GDPR articles 24, 26 -28, 30, 31, 58, 83, 84, recitals 75, 76, 83, 97.

### 9.2. Current GDPR Compliance Status (Issue 9)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Is the Company's Top Team (Board, CEO, Senior Managers, etc.) aware and oversee all activities related to GDPR compliance?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 2. Does the Company have clear and documented GDPR compliance policies and procedures?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 3. Does the Company as the controller provide data protection training to all company employees?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Does the Company carry out internal audits for data protection issues?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Does the Company have contracts with its processors that comply with GDPR?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 6. Does the Company maintain proper compliance records and files?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 7. Has the Company announced both the controller and DPO data to the relevant Data Protection Authority?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 8. Has the Company included both the controller and DPO data to the relevant Privacy Notices?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 9. Do you have agreements in place, where personal data is shared between subsidiaries and/or business partners (article 26)?

*Compliance Answer: .....(FC).....(PC)...(NC)...X..(N/A)*

Question 10. Do the agreements reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects?


*Compliance Answer: .....(FC).....(PC)...(NC)...X..(N/A)*

Question 11. Are the joint controllers available to data subjects?


*Compliance Answer: .....(FC).....(PC)...(NC)...X..(N/A)*

SIMPLY CLEVER

ŠKODA



**We will turn your CV into an opportunity of a lifetime**



Do you like cars? Would you like to be a part of a successful brand? We will appreciate and reward both your enthusiasm and talent. Send us your CV. You will be surprised where it can take you.

Send us your CV on  
[www.employerforlife.com](http://www.employerforlife.com)



Question 12. Do the agreements reinforce the ability of data subjects to exercise their rights against each subsidiary or business partner?

Question 13. If required, have you appointed an EU representative (article 27)?

*Compliance Answer: .....(FC).....(PC)...(NC)...X..(N/A)*

Question 14. Have you entered into representative agreement that sets out your EU representative's appointment and obligations?

*Compliance Answer: .....(FC).....(PC)...(NC)...X..(N/A)*

Question 15. Have you provided information about your EU representative to data subjects and the relevant DPA?

*Compliance Answer: .....(FC).....(PC)...(NC)...X..(N/A)*

### 9.3. Gaps (Issue 9)

*These gaps relate to the example company ('XYZ Corporation').*

1. The Company's Top Team (Board, CEO, Senior Managers, etc.) are not fully aware to oversee all activities related to GDPR compliance.
2. The Company does not have clear and documented GDPR compliance policies and procedures.
3. The Company does not provide data protection training to all company employees.
4. The Company does not carry out internal audits for data protection issues.
5. The Company have contracts with its processors but are not fully compliant with GDPR?
6. The Company does not maintain proper compliance records and files.
7. The Company has not announced both the controller and DPO data to the relevant Data Protection Authority.
8. The Company has not included both the controller and DPO data to the relevant Privacy Notices.

### 9.4. Examples of Actions to remedy the gaps of Issue 9

*These actions relate to the example company ('XYZ Corporation').*

1. A GDPR compliance system must be established. For more details, also see '**GDPR Gap Tool 5: Full GDPR Compliance Documentation List**'.
2. Training on GDPR must be given to all staff (board, senior managers, employees, etc.).

3. All processor contracts need to be reviewed to ensure they comply with GDPR.
4. The Company must implement a process to carry out internal audits for data protection issues.
5. The Company must announce the data of the controller and the DPO in the privacy notice as well as the relevant data protection authority.

## Issue 10: Data Protection Officer

### 10.1. Description of GDPR requirements (Issue 10)

GDPR requires (Article 37(1)) the designation of a Data Protection Officer (DPO) in three specific cases:

- a. where the processing is carried out by a public authority or body;
- b. where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
- c. where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

For more details, see GDPR articles 13, 14, 39, 33, 35 – 39, 47, recitals 77, 97.

### 10.2. Current GDPR Compliance Status (Issue 10)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Have you considered appointing a DPO?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 2. Do the DPO's reporting arrangements meet the GDPR requirements (Independence, Direct access to top management, Competence (knowledge of the GDPR), etc.)?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 3. Are roles and duties of DPO defined in job descriptions, hierarchical organizational chart, minutes of meeting, etc.?

*Compliance Answer: .....(FC)...(PC)...X..(NC)....(N/A)*

Question 4. Are compliance activities monitoring and documentation maintenance assigned and well defined?

*Compliance Answer: .....(FC)...(PC)...X..(NC)....(N/A)*



### 10.3. Gaps (Issue 10)

*These gaps relate to the example company ('XYZ Corporation').*

1. The Company has not examined whether a DPO is needed.

### 10.4. Examples of Actions to remedy the gaps of Issue 10

*These actions relate to the example company ('XYZ Corporation').*

1. The Company must examine if a DPO is needed and appoint one if the need exists.
2. Ensure the DPO's team is properly resourced to deliver against the requirements of the GDPR.
3. Put in place a reporting infrastructure that protects the role of the DPO and enables effective reporting through to Board.
4. The DPO will need to ensure that a full compliance program is designed incorporating features such as: Privacy Impact Assessments, regular DP audits, policy reviews and updates, and training and awareness raising programs, etc. See also GDPR Gap Tool 7: DPO Action Plan.

## Issue 11: Processor Obligations

### 11.1. Description of GDPR requirements (Issue 11)

GDPR obliges (Article 28) data controllers to only outsource processing to those entities that have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance and to have a contract or binding act that governs the relationship.

The Article also limits the ability of processors to subcontract without consent of the data controller, and what guarantees need to be in place in this arrangement, etc.

For more details, see GDPR articles 24, 28, recitals 13, 81, 82, 83, 91.

### 11.2. Current GDPR Compliance Status (Issue 11)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Do you have any processors (e.g. accounting services, cloud, marketing, etc.)?

Answer: ...X...(YES).....(NO)

Question 2. Do you carry out due diligence prior to using the processors (risk assessment, financial review, use of sub-processors, assessment of the supplier's security measures, etc.)?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 3. Do you have proper processor contracts, according to GDPR?

Question 4. Does the contract contain terms and conditions (internal controls, security, confidentiality statements of employees, audit and inspection rights, etc.) to ensure compliance with GDPR obligations in processing the personal data of your company?

4.1. Are there are documented instructions?

4.2. Is there evidence of due diligence by the Controller over the suitability of the Processor in respect of the types of personal data being processed?

4.3. Are there are suitable confidentiality clauses in the contract?

4.4. Does the Processor have adequate information security measures in place?

4.5. Does the contract manage the downline use of sub Processors?

4.6. Does the contract put in place measures for the Processor to help the Controller comply with Data Subject Rights?

4.7. Are there mechanisms to assist in cooperation with the Controller and the relevant Data Protection Authorities?

4.8. Are there processes in place to deal with security incidents and data breach notifications?

4.9. Are there are procedures in place to deal with destruction or return of personal data at the end of the contract?

*Compliance Answer .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Do any processors that have access to the company's IT systems comply with GDPR?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Has a company manager been assigned to monitor the good execution of this contract?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 7. Has a representative of a processor not established in the Union been resolved, if there is one?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 8. Has the issue of sub-processor been resolved, if there is one?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 9. Are company staff aware of the duties of the processor in processing the company's personal data?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

### 11.3. Gaps (Issue 11)

*These gaps relate to the example company ('XYZ Corporation').*

1. The Company has several processors that process personal data but their contracts are not GDPR-compliant.

### 11.4. Examples of Actions to remedy the gaps of Issue 11

*These actions relate to the example company ('XYZ Corporation').*

1. Audit existing supplier (processor) arrangements and update the relevant contracts to comply with GDPR.
2. Update the templates and general procurement contracts to reflect the GDPR's data processor obligations.
3. Assign the duty to monitor the processing of PD by third parties to a company manager.

## Issue 12: International Data Transfers

### 12.1. Description of GDPR requirements (Issue 12)

GDPR requires (Chapter V, Articles 44 – 50) that any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined, etc.

For more details, see GDPR articles 44 - 50, recitals 80, 104, 112.

### 12.2. Current GDPR Compliance Status (Issue 12)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Do you transfer PD to your mother company?

*Answer: ... (YES)...X...(NO)*

Question 2. Do you transfer PD outside the EEA?

*Answer: ... (YES)...X...(NO)*

Question 3. Do you transfer PD on the basis of GDPR (Binding Corporate Rules, Other arrangements, etc.)?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

Question 4. Do your policies and procedures, prior to the transfer of data to a third country or international organization, require review by the Commission or reference the published list of approved countries?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

Question 5. Do your policies and procedures, in the absence of a decision, transfer personal data to a third country or an international organisation only if the appropriate safeguards have been provided, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

Question 6. Do your policies and procedures include what safeguards are acceptable if authorised by the supervisory authority in transferring data to third countries?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

Question 7. Are the binding corporate rules legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

Question 8. Do your policies and procedures, in the absence of an adequacy decision or providing sufficient safeguards (including binding corporate rules) provide explicit criteria limiting what kinds of data can be transferred to a third country?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

Question 9. Do your roles and responsibilities require that a DPO monitor member law for limits of specific categories of Personal data to a third country?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

Question 10. Do you record the assessment of personal data and its safeguards?

*Compliance Answer: ..... (FC)..... (PC)..... (NC)..X.. (N/A)*

### 12.3. Gaps (Issue 12)

*These gaps relate to the example company ('XYZ Corporation').*

1. There is no gap as the Company does not transfer any data abroad.

## 12.4. Examples of Actions to remedy the gaps of Issue 12

*These actions relate to the example company ('XYZ Corporation').*

No actions are required as the company makes no transfers of any data. In case this changes in the future, the company must develop BCRs and other Information Sharing Agreements with GDPR safeguards included.

## Issue 13: Codes of Practice and Certifications

### 13.1. Description of GDPR requirements (Issue 13)

Companies and organisations within the same industry, or engaging in similar types of processing, are likely to encounter similar data protection issues. Codes of Conduct and certifications provide such organisations with useful guidance on industry-standard approaches to these issues. Compliance with a Code of Conduct or Certification Scheme (e.g., ISO 27001) may provide evidence of compliance with the GDPR.

GDPR requires (Articles 40 - 43) that the Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors, etc.

For more details, see GDPR articles 24, 25, 8, 32, 40 – 43, recitals 77, 81, 100, 166.

### 13.2. Current GDPR Compliance Status (Issue 13)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Do you have any codes of practice?

*Answer: .....(YES)...X...(NO)*

Question 2. Has the company been certified (e.g., ISO 27001, etc.)?

*Answer: ...X...(YES).....(NO)*

Question 3. Does the company the certification (e.g., ISO 27001, etc.) to ensure GDPR compliance?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### 13.3. Gaps (Issue 13)

*These gaps relate to the example company ('XYZ Corporation').*

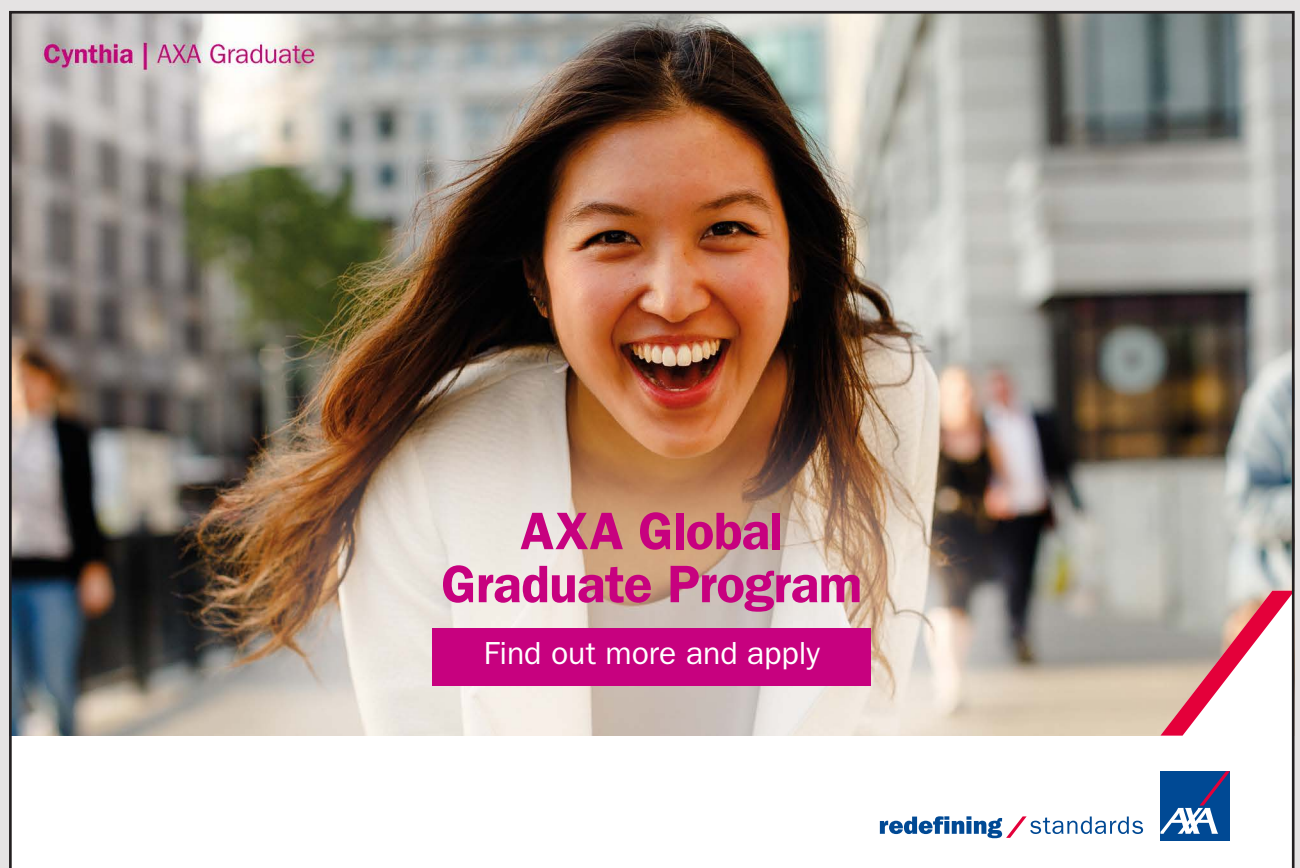
The company does not use the ISO 27001 or other mechanism for certification for GDPR compliance purposes.

### 13.4. Examples of Actions to remedy the gaps of Issue 13

*These actions relate to the example company ('XYZ Corporation').*

1. Examine how to use the ISO 27001 certification for GDPR compliance purposes.


*The GDPR Gap Analysis continues in Chapter 4, next.*



**Cynthia | AXA Graduate**

**AXA Global Graduate Program**

Find out more and apply

redefining / standards 

# 4 EXECUTING A GDPR GAP ANALYSIS-PART 3

**Overview:** This is the fourth part, ‘Analyzing Gaps in DP Area 3: Technical Issues’, of the three-part GDPR GAP Analysis. This chapter assesses the gaps for the third DP Area and for all GDPR relevant articles grouped in 7 Data Protection (DP) issues such as: Security of Processing, Data Breach, Data Protection by Design and by Default etc. Chapters 2 and 3 contain the other 2 parts (1 and 2) respectively.

This Gap Analysis is based on the operational characteristics of the example company ‘**XYZ Corporation**’.

## 4.1 ANALYZING GAPS IN DP AREA 3: TECHNICAL ISSUES

### Introduction

The GDPR Gap Analysis included in this chapter carries on from the previous chapter and assesses the gaps of the example company ‘**XYZ Corporation**’ for the third DP Area and the issues contained in it, in full compliance with the relevant GDPR Articles (4 (1,12), 5, 6 – 9, 12 – 14, 23-25, 27, 30, 32, 33-36, 39, 40, 42, 49, 57, 70, etc.) and Recitals (2, 9, 15, 19, 28, 35, 38, 39, 49, 51, 65, 71, 73-81, 83 - 96, 98, 115, 116, 122, 144,etc.), by using the 7 questionnaires (with 40 questions) and other assessment actions described next.

## 4.2 GAP ANALYSIS FOR ISSUES 14 – 20

### Issue 14: Security of Processing

#### 14.1. Description of GDPR requirements (Issue 14)

Employees must preserve and protect the security, confidentiality and privacy of personal data that are brought to their knowledge:

- a. in the exercise of their duties or
- b. in the event of their (personal data) occurrence and / or
- c. to which personal data they have access and / or



- d. whose personal data they process, throughout their term of office in the company, but also after the termination of such employment for any reason, whatsoever.

GDPR requires (Article 32) that controllers and processors, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- a. the pseudonymisation and encryption of personal data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, etc.

For more details, see GDPR articles 23-25, 27, 30, 32, 33-36, 39, 49, 57, 70, recitals 2, 9, 15, 19, 28, 35, 38, 39, 49, 51, 65, 71, 73-81, 83-86, 89-91, 94, 96, 98, 116, 122, 144.

## 14.2. Current GDPR Compliance Status (Issue 14)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Is there a security program or plan for PD?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 2. Have you used an information risk assessment methodology to assess information risks and design appropriate measures to address the identified security risks?

*Compliance Answer: .....(FC).....(PC)...X.(NC)....(N/A)*

Question 3. Have you used an data privacy and data protection risk assessment methodology to assess privacy risks and design appropriate measures to address the identified privacy risks?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Do you have an encryption policy?

*Compliance Answer: .....(FC)...(PC)...X..(NC)....(N/A)*

Question 5. Do you encrypt your data bases?

*Compliance Answer: .....(FC)...(PC)...X..(NC)....(N/A)*

Question 6. Do you encrypt your emails?

*Compliance Answer: .....(FC)...(PC)...X..(NC)....(N/A)*

Question 7. Do you encrypt your mobile devices?

*Compliance Answer: .....(FC)...(PC)...X..(NC)....(N/A)*



Question 8. Do you carry out a regular network penetration testing?

*Compliance Answer: .....(FC)...(PC)...X..(NC)....(N/A)*

Question 9. Do you destroy PD when they are no longer needed?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 10. Do you use pseudonymization, where possible?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 11. Can you ensure the access and availability of PD, when a physical or technical crisis occurs?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 12. Have you used ‘GDPR Gap Tool 2: Technical and organizational security and data privacy measures questionnaire’, ‘GDPR Gap Tool 3: Office Management Controls Assessment Questionnaire’ and ‘GDPR Gap Tool 4: Information Technology Privacy Assessment Questionnaire’ to determine the gaps in your security and data protection area of your company’s processing of personal data, and identified the needs for more measures?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### 14.3. Gaps (Issue 14)

*These gaps relate to the example company (‘XYZ Corporation’).*

1. The security program for PD is not complete.
2. There is no information risk assessment methodology to assess information risks and design appropriate measures to address the identified security risks.
3. There is no data privacy and data protection risk assessment methodology to assess privacy risks and design appropriate measures to address the identified privacy risks.
4. There is no encryption policy.
5. There is no regular network penetration testing.
6. There is no policy for destroying PD when they are no longer needed.

### 14.4. Examples of Actions to remedy the gaps of Issue 14

*These actions relate to the example company (‘XYZ Corporation’).*

1. The Company must develop and use an information risk assessment methodology to assess information risks and design the appropriate measures to address the identified information security risks.

2. The Company must develop and use a data privacy and data protection risk assessment methodology to assess privacy risks and design appropriate measures to address the identified privacy risks.
3. The final privacy and several security measures that are required to be implemented for the processing of personal data will be the result of using the above 2 methodologies as well as the output of the execution of a full assessment by using:
  - GDPR Gap Tool 2: Technical and organizational security and data privacy measures questionnaire
  - GDPR Gap Tool 3: Office Management Controls Assessment Questionnaire
  - GDPR Gap Tool 4: Information Technology Privacy Assessment Questionnaire.These are contained in book 2 'GDPR GAP Tools'.

## **Issue 15: Data Breach**

### **15.1. Description of GDPR requirements (Issue 15)**

GDPR (Article 33) makes it mandatory to notify supervisory authorities in the event of a data breach that poses a 'risk of harm'. The notification is expected without undue delay and where feasible within 72 hours. As well, detailed content requirements are set out for the notification letter. The circumstances of the data breaches must also be documented. Also, GDPR requires (Article 34) notification to data subjects of breaches that result in a 'high risk' for the rights and freedoms of individuals. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the technical and organisational measures taken by controllers and processors, as required, etc.

For more details, see GDPR articles 4 (1,12), 33, 34, 40, recitals 73, 85 – 88, 115.

### **15.2. Current GDPR Compliance Status (Issue 15)**

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Have all staff (HR, IT, Sales, Procurement, Production, Marketing, etc.) been informed about their roles and responsibilities on protecting personal data (access, use, monitoring, etc.)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 2. Do you have an integrated Data Breach Response Plan?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3. Do you review and test your breach plan regularly?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Do you have a process to inform the data protection authority?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Do you have a process to inform the data subjects?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Do you have a data breach register?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 7. Are all breaches investigated and corrective actions taken, regardless of the size or scope?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 8. Are all staff made aware of the reporting lines for breaches?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 9. Is the breach register reviewed by the DPO monthly to look for patterns or duplicated issues?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 10. Are all breaches investigated and corrective actions taken, regardless of the size or scope?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 11. Do you have a cyber insurance policy?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 12. Where a data breach has been assessed by the DPO and deemed likely to result in a risk to the rights and freedoms, do you report the breach to the Supervisory Authority within 72 hours?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### 15.3. Gaps (Issue 15)

*These gaps relate to the example company ('XYZ Corporation').*

1. The Company has not implemented a data breach monitoring and reporting system.

## 15.4. Examples of Actions to remedy the gaps of Issue 15

*These actions relate to the example company ('XYZ Corporation').*

1. A data breach monitoring and reporting system must be established. This system must include internal breach/incident notification procedures, incident identification processes and incident response plans, etc.
2. Ensure all staff are aware about their roles and responsibilities on protecting personal data.

## Issue 16: Data Protection by Design and by Default

### 16.1. Description of GDPR requirements (Issue 16)

GDPR requires (Article 25) that data controllers must, at the time of determining the means of processing as well as when actually processing personal data, implement appropriate technical and organisational measures to implement the data protection principles set out in Article 5 and integrate necessary safeguards into the processing to meet the GDPR requirements. Data controllers must also implement data protection by default, i.e. implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific purpose are processed, etc.

For more details, see GDPR articles 25, 42, recital 78.

### 16.2. Current GDPR Compliance Status (Issue 16)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. At the time of the determination of the means for processing and at the time of the processing itself do you implement appropriate organisational and technical measures which are designed to implement data protection principles, such as data minimisation, pseudonymization, encryption, etc., in an effective manner and to integrate the necessary safeguards into the processing?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 2. Do you ensure that pseudonyms and their personal identifiers and their secret keys, are always kept separate and secure?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3. Do you ensure that encryption methods and their secret keys, are always kept separate and secure?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Are staff aware of the Privacy by design and by default principles?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Have you implemented Privacy by design and by default in any company systems, products or services?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Do you use data minimisation and only obtaining and processing the minimum information necessary for the purpose specified?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 7. Is data collected by electronic means (i.e. forms, website, surveys, etc.) minimised so only the relevant fields are used according to the processing purpose?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 8. Do you have documented destruction procedures in place for information that is no longer necessary, surplus to requirement or part of an individual's consent withdrawal or right to erasure?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 9. If you must use hard copy data for storing or processing, do you use redaction methods where possible to ensure data minimisation?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 10. Have you implemented Privacy by design and by default in your IT systems?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 11. Have you discussed your requirements regarding the implementation of Privacy by design and by default in your IT systems provided by third parties (as per Gap Tool 6, in book 3)?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### **16.3. Gaps (Issue 16)**

*These gaps relate to the example company ('XYZ Corporation').*

1. There are no Data Protection by design and by default controls implemented in the company's IT Systems.

### **16.4. Examples of Actions to remedy the gaps of Issue 16**

*These actions relate to the example company ('XYZ Corporation').*

1. The Company must implement technical and organisational measures to show that it has considered and integrated data compliance data protection by design and by default measures into their data processing activities. For example, security and privacy controls (encryption, pseudonymization, masking, etc.) must be reviewed and examined to see whether they must be incorporated into the company's IT Application Systems (see 'GDPR Gap Tool 6: IT Systems Development Privacy and Security Plan' in book 2 'GDPR GAP Tools').

## **Issue 17: Data Protection Impact Assessment (DPIA)**

### **17.1. Description of GDPR requirements (Issue 17)**

GDPR requires (Article 35) data controllers of companies and public organizations to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk situation for the rights and freedoms of data subjects. When carrying out the DPIA, the controller must seek the advice of the Data Protection Officer (when a DPO is appointed).

A data protection impact assessment shall in particular be required in the case of:

- a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- b. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- c. a systematic monitoring of a publicly accessible area on a large scale, etc.

For more details, see GDPR articles 35, 36, recitals 84, 89 – 95.

### **17.2. Current GDPR Compliance Status (Issue 17)**

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Have you established a Data Protection Impact Assessment (DPIA) Methodology?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 2. Does the DPIA Methodology include the following steps:

2.1. Identify the need for a DPIA?

- 2.2. Describe the information and data flows?
- 2.3. Identify the data protection, privacy and related risks?
- 2.4. Identify and evaluate the privacy solutions?
- 2.5. Sign off and record the DPIA outcomes?
- 2.6. Integrate the outcomes into the project plan?
- 2.7. Consult with internal and external stakeholders as needed throughout the process?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3. Have you executed DPIAs for the existing systems and services of the company?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Is the DPO consulted on issues related to data protection impact assessments?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Are staff trained on all aspects of executing a DPIA?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 6. Are data subjects and the data protection authority consulted, if required?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### **17.3. Gaps (Issue 17)**

*These gaps relate to the example company ('XYZ Corporation').*

1. The Company has not crafted a DPIA Methodology.
2. The Company has not conducted any DPIAs.

### **17.4. Examples of Actions to remedy the gaps of Issue 17**

*These actions relate to the example company ('XYZ Corporation').*

1. Design and implement DPIA templates in line with GDPR DPIA.
2. Carry out awareness raising of the requirement to conduct DPIAs to reflect GDPR requirements.
3. Undertake DPIA on newer systems and determine the risk of older systems.

## Issue 18: Corporate Web Site

### 18.1. Description of GDPR requirements (Issue 18)

When understanding whether your website is subject to the GDPR, the following items should be considered:

- Are EU citizens a target for your product or service e.g. does your website feature Euro pricing details?
- Does your website collate and store identifying information or online identifiers such as IP addresses via analytics?
- Is there a subscribe function on the website?
- Is there a comment section to the website?
- Do you allow for users to log in with third party applications?

Also, according to GDPR (Article 32 ‘Security of processing’):

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, etc. These measures must also include the company’s website.

For more details, see GDPR articles 5, 6 – 9, 12 – 14, 32.

### 18.2. Current GDPR Compliance Status (Issue 18)

*This questionnaire relates to assessing the gaps of the example company (‘XYZ Corporation’).*

Question 1. Do you have a website?

*Answer: ...X...(YES).....(NO)*

Question 2. Does your website have a Cookies Policy?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 3. Does your website have a Data Protection Policy?

*Compliance Answer: .....(FC)...X...(PC).....(NC)....(N/A)*

Question 4. Does your website have encryption (SSL)?

*Compliance Answer: ... (FC).....(PC)...X..(NC)....(N/A)*



### 18.3. Gaps (Issue 18)

*These gaps relate to the example company ('XYZ Corporation').*

1. The Company's Cookies Policy is not GDPR-compliant.
2. The Company's Website Policy is not GDPR-compliant.

### 18.4. Examples of Actions to remedy the gaps of Issue 18

*These actions relate to the example company ('XYZ Corporation').*

1. Update the company's web site privacy policy to ensure compliance with GDPR.
2. Update the company's cookies policy to ensure compliance with GDPR.
3. Obtain an SSL Certificate for the corporate website.

## Issue 19: CCTV System

### 19.1. Description of GDPR requirements (Issue 19)

Personal data are usually recorded by CCTV systems used by companies and organizations. This Company is also using such as system as indicated below.

The key GDPR issues for CCTV/surveillance equipment operators are:

- the lawful processing ground
- who has access to CCTV data and for what reason.
- how data is kept secure.
- the applicable retention periods.
- how personal data will be extracted and provided to an individual in the event of a subject access request.

GDPR (Article 30) sets out a detailed list of information that must be maintained as records of processing activities carried out by and on behalf of the controller, as well as the requirement to make the records available to data subjects and Supervisory Authorities upon request.

For more details, see GDPR articles 5, 6 – 9, 12 – 14, 30, 32.

### 19.2. Current GDPR Compliance Status (Issue 19)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Do you have a CCTV system in operation?

Answer: X. (YES) ..... (NO)

Notes: There is a system installed in the basement and at the main entrance to the building.

Question 2. Do you inform visitors and employees of the use of the CCTV system?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### 19.3. Gaps (Issue 19)

*These gaps relate to the example company ('XYZ Corporation').*

1. There is no notice of the use of CCTV to visitors and employees.

### 19.4. Examples of Actions to remedy the gaps of Issue 19

*These actions relate to the example company ('XYZ Corporation').*

1. Include a notice of the use of CCTV to visitors at the locations where the cameras are operating.
2. Include a notice to company employees on the use of CCTV and ensure that the recorded data are maintained according to the relevant laws.

## Issue 20: Office Applications

### 20.1. Description of GDPR requirements (Issue 20)

Personal data are usually recorded by office application systems used by companies and organizations. This Company is also using such applications as indicated below. GDPR (Article 30) sets out a detailed list of information that must be maintained as records of processing activities carried out by and on behalf of the controller, as well as the requirement to make the records available to data subjects and Supervisory Authorities upon request.

For more details, see GDPR articles 5, 6 – 9, 12 – 14, 30, 32.

## 20.2. Current GDPR Compliance Status (Issue 20)

*This questionnaire relates to assessing the gaps of the example company ('XYZ Corporation').*

Question 1. Which Office Applications Software, do you have and use?

- Word Software? Answer: ..X.... (YES) ..... (NO)
- EXCEL Software? Answer: ..X.... (YES) ..... (NO)
- PDF Software and documents? Answer: ..X.... (YES) ..... (NO)
- Powerpoint Software? Answer: ...X... (YES) ..... (NO)
- Other Software? Answer: ...X... (YES) ..... (NO)

Question 2. Does this software contain personal data?

- Word Software? Answer: ...X... (YES) ..... (NO)
- EXCEL Software? Answer: ...X... (YES) ..... (NO)
- PDFs? Answer: ...X... (YES) ..... (NO)
- Powerpoint Software: ..X.... (YES) ..... (NO)
- Other Software? Answer: ..X.... (YES) ..... (NO)



**e-learning for kids**

- The number 1 MOOC for Primary Education
- Free Digital Learning for Children 5-12
- 15 Million Children Reached

**About e-Learning for Kids** Established in 2004, e-Learning for Kids is a global nonprofit foundation dedicated to fun and free learning on the Internet for children ages 5 - 12 with courses in math, science, language arts, computers, health and environmental skills. Since 2005, more than 15 million children in over 190 countries have benefitted from eLessons provided by EFKI. An all-volunteer staff consists of education and e-learning experts and business professionals from around the world committed to making difference. eLearning for Kids is actively seeking funding, volunteers, sponsors and courseware developers; get involved! For more information, please visit [www.e-learningforkids.org](http://www.e-learningforkids.org).

Question 3. Have you implemented appropriate policies to manage and control the use of these software packages and how they store and process personal data?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 4. Do you use encrypt e-mails that contain personal data?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

Question 5. Do you use Hotmail, Gmail, yahoo, etc. for sending personal data?

*Compliance Answer: .....(FC).....(PC)...X..(NC)....(N/A)*

### 20.3. Gaps (Issue 20)

*These gaps relate to the example company ('XYZ Corporation').*

1. Policies to manage and control the use of these software packages and the processing of PD are not complete.

### 20.4. Examples of Actions to remedy the gaps of Issue 20

*These actions relate to the example company ('XYZ Corporation').*

1. Implement appropriate policies to manage and control the use of these software packages. See also actions of Issue 14.

## 4.3 CONCLUSION AND NEXT STEPS

The above GDPR gap analysis (Chapters 2, 3 and this chapter) identified your GDPR compliance gaps as regards the specific issues and articles of GDPR and presented examples of required improvement actions to close all identified GDPR gaps in your present company (the example company 'XYZ Corporation') operations as regards the protection of processing of personal data.

Now you have to plan and implement the required improvement actions.

This is done by summarizing the results of *The GDPR Gap Analysis* (contained in Chapters 2 to 4 and this chapter) and by crafting your own GDPR Compliance Action Plan.

*You may also review, customize to your purposes and use the plan included in GDPR Gap Tool 8 ('GDPR Compliance Action Plan').*

# APPENDIX 1. OPERATING FRAMEWORK OF 'XYZ' CORPORATION

**Overview:** This appendix describes the operational characteristics of the example company '**XYZ Corporation**' a fictitious **Ship Management (Maritime) Company** as regards the personal data processed by its functions, processes and information systems.

## **Operating Framework of Personal Data processed by 'XYZ Corporation'**

All departments of the example company (customer support, personnel administration, accounting, maintenance, secretariat, etc.) process personal data of employees, customers, partners, etc.

All these data are either in printed form only or in digital format or in both forms.

Data in printed form are stored in physical (manual) files in the central offices. Data in digital format are collected by, processed and used with the support of (a) information systems and web applications, such as a standardized ERP system for financial accounting, customer support, personnel administration, etc. and (b) the standard application package MS OFFICE to manage office issues (Word, Excel, PowerPoint, etc., of Microsoft).

These digital data are stored in digital files on computer systems, servers and networks in the Company's offices. The full details are contained in the Personal Data and IT Assets Inventories.

Within this operating frame the company has, operates and utilizes information systems, corporate and personal data and communication infrastructures for:

- The smoother and more secure handling and fulfilment of its operational needs and, inter alia,
- The most effective support in achieving the best service and safety of employees, customers, partners and suppliers.

## APPENDIX 2. PRIVACY RISKS

**Overview:** This appendix describes the privacy risks of the example company ‘**XYZ Corporation**’ a fictitious **Ship Management (Maritime) Company** as regards the personal data processed by its functions, processes and information systems.

To achieve the objectives of the protection of personal data and to comply with the provisions of the GDPR the usual risks to be minimized are:

- The sharing and merging of databases can allow businesses to collect a much broader set of personal data than people expect or want.
- Non-effective data protection and disclosure controls by companies increase the likelihood of their sharing of personal data in the wrong way.
- The measures and controls taken against individuals as a result of the collection of personal data for these can be taken as intrusive.
- The context in which personal data are used or disclosed may change over time, leading to the case where the collected personal data are used for different purposes without the knowledge of the data subjects.
- New data collection mechanisms or surveillance methods may be unjustified penetration of privacy of individuals.
- Vulnerable people may be particularly concerned about the risks of identifying or revealing their personal data.
- Personal data that is collected and stored unnecessarily or incorrectly managed, so that duplicate recordings are created, present a much greater security and privacy risk.
- If no data retention period is specified, personal data may be used for larger periods of time than it is necessary.

# END NOTES

## 1. You may also use the following questionnaire:

Q1. Do you educate all employees and management about the GDPR requirements and principles and the possible impact of noncompliance?

Answer: Yes: \_\_\_ or No: \_\_\_

Q2. Do you have an effective data protection training program in place?

Answer: Yes: \_\_\_ or No: \_\_\_

Q3. Does your data protection training program cover:

- GDPR scope and principles?
- Measures and controls for protecting data and minimising risks?
- Data Protection Officer duties?
- Supervisory Authority role and scope?
- Codes of Conduct and/or Certifications?
- Data Protection Impact Assessments (DPIA)?
- Information Audits?
- Processing Activities and Conditions?
- Conditions for Consent and Privacy Notices?
- Data Subject Rights and Subject Access Requests?
- Third Country or International Organisation Transfers
- Reporting Lines & Notifications?
- Data Protection by Design and by Default (i.e. data minimisation, pseudonymisation & encryption)?

Answer: Yes: \_\_\_ or No: \_\_\_

Q4. Are all GDPR and associated data protection procedures audited at least annually for compliance with the Regulations and you own objectives?

Answer: Yes: \_\_\_ or No: \_\_\_

## 2. You may also use the following questionnaire:

Q1. Are you always able to demonstrate that consent has been given?

Answer: Yes: \_\_\_ or No: \_\_\_

Q2. Where processing is based on consent, is the request in a clear and transparent format, using plain language and avoiding any illegible terms or jargon?

Answer: Yes: \_\_\_ or No: \_\_\_

Q3. Is the request in an easily accessible format with the purpose for data processing attached to that consent?

Answer: Yes: \_\_\_ or No: \_\_\_

Q4. Where consent is requested in the context of a written declaration which also concerns other matters, is the request always presented in a manner which is clearly distinguishable from the other matters?

Answer: Yes: \_\_\_ or No: \_\_\_

Q5. Is the data subjects' right to withdraw consent at any time made clear?

Answer: Yes: \_\_\_ or No: \_\_\_

Q6. Is the process for withdrawing consent simple, accessible and quick?

Answer: Yes: \_\_\_ or No: \_\_\_

Q7. Where personal information is obtained and/or processed relating to a child under 16 years (13 years in some countries, e.g. UK), do you ensure that consent is given and documented by the holder of parental responsibility over the child?

Answer: Yes: \_\_\_ or No: \_\_\_

Q8. Where services are provided to children, does your communication information and privacy notice provide clear and plain information that is easy to understand by a child?

Answer: Yes: \_\_\_ or No: \_\_\_

Q9. When physically collecting personal information (i.e. face-to-face, telephone, etc.), are supporting scripts used to remind staff of the conditions for consent and an individual's right to be informed?

Answer: Yes: \_\_\_ or No: \_\_\_

Q10. Do you have clear audit trails to evidence consent and where it came from?

Answer: Yes: \_\_\_ or No: \_\_\_



# FURTHER RESOURCES

For more details on all aspects of GDPR Compliance, see my books listed next:

1. **DATA PROTECTION AND PRIVACY MANAGEMENT SYSTEM DATA PROTECTION AND PRIVACY GUIDE – VOL I**  
<http://bookboon.com/en/data-protection-and-privacy-management-system-ebook>
2. **DP&P STRATEGIES, POLICIES AND PLANS DATA PROTECTION AND PRIVACY GUIDE – VOL II**  
<http://bookboon.com/en/dpp-strategies-policies-and-plans-ebook>
3. **DATA PROTECTION IMPACT ASSESSMENT DATA PROTECTION AND PRIVACY GUIDE – VOL III**  
<http://bookboon.com/en/data-protection-impact-assessment-ebook>
4. **DATA PROTECTION SPECIALIZED CONTROLS DATA PROTECTION AND PRIVACY GUIDE – VOL IV**  
<http://bookboon.com/en/data-protection-specialized-controls-ebook>
5. **SECURITY AND DATA PRIVACY AUDIT QUESTIONNAIRES DATA PROTECTION AND PRIVACY GUIDE – VOL V**  
<http://bookboon.com/en/security-and-data-privacy-audit-questionnaires-ebook>
6. **The CEO's Guide To GDPR Compliance: The guide for C-Suite Members to ensure GDPR compliance, bookboon.com, 2017**  
<https://bookboon.com/en/the-ceos-guide-to-gdpr-compliance-ebook>
7. **GDPR and Travel Industry, bookboon.com, 2018**  
<https://bookboon.com/en/gdpr-and-travel-industry-ebook>
8. **Data Protection (GDPR) Guide, bookboon.com, 2019**  
<https://bookboon.com/en/data-protection-gdpr-guide-ebook>
9. **Data Governance Controls, bookboon.com, 2019**  
<https://bookboon.com/en/data-governance-controls-ebook>

# DISCLAIMER

The material, concepts, ideas, plans, policies, procedures, forms, methods, tools, etc. presented, described and analyzed in all chapters and appendices, are for educational and training purposes only. These may be used only, possibly, as an indicative base set, and should be customized by each organization, after careful and considerable thought as to the needs and requirements of each organization, taking into effect the implications and aspects of the legal, national, religious, philosophical, cultural and social environments, and expectations, within which each organization operates and exists.

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.