GDPR Gap Assessment Tools

Evaluating Gaps in GDPR Compliance Better

John Kyriazoglou

bookboon
The eBook company

JOHN KYRIAZOGLOU

GDPR GAP ASSESSMENT TOOLS

EVALUATING GAPS IN GDPR COMPLIANCE BETTER

GDPR Gap Assessment Tools: Evaluating Gaps in GDPR Compliance Better
1st edition

ISBN 978-87-403-3075-5

CONTENTS

1 GDPR GAP TOOL 1: GDPR PERSONAL DATA INVENTORY TEMPLATE

Overview

This template may be used to record the personal data of any enterprise, at the business department or function and process level. It is used for each department or function of the company and for each process within it. It is designed to comply with the specific requirements of the EU GDPR (European Union General Data Protection Regulation), but also be useful for any privacy framework. It contains a blank template and one detail example to help you understand its use in a real corporate environment.

TEMPLATE

Business Department/Function: <name of business function, e.g.: HR, Production, etc.>
Process 1.1: <Name of process, e.g.: Managing HR Personnel files>
Who is responsible: <Tile of manager responsible, e.g.: HR Director>
Data Subject Type: <Type of data subject, e.g.: employee, customer, passenger, etc.>
Type of data: <Detail data per data subject, e.g.: Employee data: name, surname, date of birth, home address, etc. Employment contracts, sick records, disciplinary, medical records, etc.>
Format: <Type of format, e.g.: Electronic or Hardcopy>
Volume: <estimated number of records>
Source: <Who provides the personal data, e.g.: employee, etc.>
Classification: <A classification level according to Classification Policy, e.g.: restricted, public, etc.>
Sensitive data: <Yes or No according to GDPR Article 9 'Processing of special categories of personal data'>
Location: < physical file location or name of computerized system>
Security Measures: <Details of existing security measures, e.g.: Locked and restricted access>
Accessed by: <details of people that can access these data, e.g.: Operations director & first aiders if vital interests threatened>
Categories of recipients: <details of people, functions or systems that receive these personal data, e.g.: National Ministry of employment>
Retention Period: <How long these data are retained, e.g.: as per policy>
Disposal Procedure: < how these data are disposed of, e.g.: Secure shredded>

Third party involvement: <name of third party involved in processing these personal data>
Third party GDPR compliance: <details of implemented measures related to GDPR taken by third party>
Data Transfer Procedure: <details of how and to whom personal data are transferred>
Legal basis to process: <details of legal basis to process these personal data, e.g.: Contract/legitimate interests>
Reference Documentation: <name of form or contract as a proof of the legal basis, e.g.: Contract of employment>
Date of legal basis: <date of effectiveness of legal basis for processing of these personal data, e.g.: Start of employment>
Controller: <name of controller, e.g.: our company>
Processor: <name of processor, e.g.: our company>

EXAMPLE for the example company 'XYZ Corporation'

Business Department/Function: HR Department
Process 1.1: Managing HR Personnel files
Who is responsible: HR Director
Data Subject Type: Employee
Type of data: Employee data: name, surname, date of birth, home address, etc. Employment contracts, sick records, disciplinary, medical records, etc.
Format: Electronic and Hardcopy (manual file)
Volume: 1,000 records.
Source: Employees
Classification: Confidential
Sensitive data: Yes, according to GDPR Article 9 'Processing of special categories of personal data'
Location: Personnel Information System (within the company's data centre)
Security Measures: Passwords for IT System and Locks in office cabinets storing physical records
Accessed by: HR director & first aiders if vital interests threatened
Categories of recipients: National Ministry of employment
Retention Period: As per retention policy
Disposal Procedure: As per disposal policy
Third party involvement: There is no third party involved in processing these personal data
Third party GDPR compliance: Not required
Data Transfer Procedure: Not required
Legal basis to process: Employment Contract, legitimate interests

Reference Documentation: Contract of employment
Date of legal basis: Start of employment
Controller: Assistant General Manager of our Company
Processor: Not required

2 GDPR GAP TOOL 2: TECHNICAL AND ORGANIZATIONAL SECURITY AND DATA PRIVACY MEASURES QUESTIONNAIRE

These questionnaires (see below) relate to assessing the organizational and data privacy measures of the example company ('XYZ Corporation').

Has a security risk and personal data protection analysis been undertaken and have the corresponding measures taken to reduce the respective identified risks?

Answer: Yes: ____ or No: ____

Note the steps you have taken for each area.

Area A: Organizational security and privacy measures

1. Security Responsibilities of the Board of Directors / Senior Management-
   Answer: Yes: ____ or No: ____
2. Organization of IT security (responsible manager, team, process, operation, etc.)-
   Answer: Yes: ____ or No: ____
3. Personnel Management System with security checks for personnel
   Answer: Yes: ____ or No: ____
4. Contracts with security controls for third-party personal data processing companies- Answer: Yes: ____ or No: ____
5. Data protection specifications with third-party data processing companies-
   Answer: Yes: ____ or No: ____
6. Instructions for Security of Confidential Information
   Answer: Yes: ____ or No: ____
7. Information Systems Security Rules- Answer: Yes: ____ or No: ____
8. Obtaining Cyber Security Insurance-Answer: Yes: ____ or No: ____
9. Reporting incidents of privacy violations (data btreaches)
   Answer: Yes: ____ or No: ____
10. Certification (ISO, PCI, SOX, ITIL, etc.)-Answer: Yes: ____ or No: ____
11. Certification of IT in one function (e.g. ISO 27001 for security, etc.)?
    Answer: Yes: ____ or No: ____

Area B: Methodologies

1. Methodology of Integrating Security and Privacy in the Development of Information Systems - Answer: Yes: ____ or No: ____
2. Methodology for the Development of Information Technology Security Strategy - Answer: Yes: ____ or No: ____
3. Methodology for the analysis and management of Information Technology risks - Answer: Yes: ____ or No: ____

Area C: Plans

1. Information security strategy plan-Answer: Yes: ____ or No: ____
2. Business Continuity Critical Functions Plan
   Answer: Yes: ____ or No: ____
3. Civil Treats Plan (Terrorism, Bombs, Natural Disasters, Civil disturbance, etc.)-
   Answer: Yes: ____ or No: ____
4. Corporate Data Protection and IT Security Plan
   Answer: Yes: ____ or No: ____
5. Personal Data Privacy Protection Program
   Answer: Yes: ____ or No: ____
6. Data Protection Awareness, Communication and Education Plan
   Answer: Yes: ____ or No: ____
7. Data Subjects Claims and Complaints Response Plan
   Answer: Yes: ____ or No: ____
8. Third Parties Risk Management Plan-Answer: Yes: ____ or No: ____
9. Corporate Functions Data Protection Integration Plan
   Answer: Yes: ____ or No: ____
10. Data Quality Improvement Plan-Answer: Yes: ____ or No: ____
11. Social Media Governance Plan-Answer: Yes: ____ or No: ____
12. Information Security Management Plan
    Answer: Yes: ____ or No: ____
13. Security Development in IT Systems Plan-
    Answer: Yes: ____ or No: ____
14. Personal Data Breach Response Plan-Answer: Yes: ____ or No: ____

Area D: Data Protection Policies and Procedures

1. Privacy Notice or Data Protection Policy
   Answer: Yes: ____ or No: ____
2. Encryption Policy-Answer: Yes: ____ or No: ____
3. Pseudonymization policy-Answer: Yes: ____ or No: ____
4. Corporate Records Retention and Destruction Policy
   Answer: Yes: ____ or No: ____
5. Data Classification Policy-Answer: Yes: ____ or No: ____
6. Data Quality Policy-Answer: Yes: ____ or No: ____
7. Website Cookie Policy-Answer: Yes: ____ or No: ____
8. Regulatory Compliance Policy-Answer: Yes: ____ or No: ____
9. Network and Internet Management Policy
   Answer: Yes: ____ or No: ____
10. Email Security Management Policy-Answer: Yes: ____ or No: ____
11. Backup and Recovery Policy-Answer: Yes: ____ or No: ____
12. Passwords Management Policy-Answer: Yes: ____ or No: ____
13. Physical Security Policy for Information Technology Systems
    Answer: Yes: ____ or No: ____
14. Security Incident Management Policy-Answer: Yes: ____ or No: ____
15. Third Party Contracts Monitoring Policy
    Answer: Yes: ____ or No: ____
16. End User Application Management Policy-Answer: Yes: __or No: ____
17. IT Assets Withdrawal Policy-Answer: Yes: ____ or No: ____
18. User Logical Access Policy-Answer: Yes: ____ or No: ____
19. Clean Desk and Screen Policy-Answer: Yes: ____ or No: ____
20. Data Breach Management Policy-Answer: Yes: ____ or No: ____

Area E: Software

1. Data loss prevention (DLP) software-Answer: Yes: ____ or No: ____
2. Software tools for aggregation, data masking, pseudonymisation, or anonymization-Answer: Yes: ____ or No: ____
3. Encryption technology-Answer: Yes: ____ or No: ____
4. Intrusion Detection and Prevention System
   Answer: Yes: ____ or No: ____

3 GDPR GAP TOOL 3: OFFICE MANAGEMENT CONTROLS ASSESSMENT

These questionnaires (see below) relate to assessing the Office Management Controls of the example company ('XYZ Corporation').

1. Telephone Call Center

Q1. Personal data? Answer: ...... (YES) ...... (NO)
Q2. Maintenance contract? Answer: ...... (YES) ...... (NO)
Q3. Scramblers, bugging devices monitoring; Answer: ...(YES) ...... (NO)
Q4. Wiring and cabling (routes, ducts, piping, etc.) security?
Answer: ...... (YES) ...... (NO)

2. CCTV

Q1. Personal data? Answer: ...... (YES) ...... (NO)
Q2. Maintenance contract? Answer: ...... (YES) ...... (NO)
Q3. Coverage (within office, outside, etc.)? Answer:... (YES) .... (NO)
Q4. Hours of operation? Answer:...... (YES) ...... (NO)
Q4. Wiring Safety? Answer: ...... (YES) ...... (NO)

3. PCs, Electronic Devices, Other Media

Q1.1. Lap Tops - Personal Data? Answer: ...... (YES) ...... (NO)
Q1.2. Encryption: ...... (YES) ...... (NO)
Q1.3. Maintenance contract? Answer: ...... (YES) ...... (NO)
Q2.1. FAX - Personal data? Answer: ...... (YES) ...... (NO)
Q2.2. Encryption: ...... (YES) ...... (NO)
Q.2.3. Maintenance contract? Answer: ...... (YES) ...... (NO)
Q3.1. Printers - Personal Data? Answer: ...... (YES) ...... (NO)
Q3.2. Maintenance contract? Answer: ...... (YES) ...... (NO)

Q4.1. Smart Phones- Personal Data? Answer: ...... (YES) ...... (NO)
Q4.2. Encryption: ...... (YES) ...... (NO)
Q4.3. Usage Policy? Answer: ...... (YES) ...... (NO)
Q5.1. USBs - Personal data? Answer: ...... (YES) ...... (NO)
Q.5.2. Encryption: ...... (YES) ...... (NO)
Q6. DVDs - Personal data? Answer: ...... (YES) ...... (NO)
Q.7. Portable Storage Devices - Personal Data? Answer: ..(YES) ... (NO)
Q.8. Personal Digital Assistants - Personal Data? Answer: ...(YES) ..(NO)
Q.9. Cloud Storage Devices - Personal Data? Answer: ..(YES) ...(NO)
Q.10. Microfilms / Photographs / Videos / Microfische - Personal data; Answer: ...... (YES) ...... (NO)

4. Alarm System

Q.1. Personal data? Answer: ...... (YES) ...... (NO)
Q.2. Maintenance contract? Answer: ...... (YES) ...... (NO)
Q.3. Coverage (entrance to building, etc.)? Answer:.... (YES) ...... (NO)
Q.4. Hours of operation? Answer:......(YES) ...... (NO)

5. Access Control

Q.1. Personal data? Answer: ...... (YES) ...... (NO)
Q.2. Maintenance contract? Answer: ...... (YES) ...... (NO)
Q.3. Coverage (entrance to office, etc.)? Answer:...(YES) ...... (NO)
Q.4. Hours of operation? Answer:....(YES) ...... (NO)
Q.5. Wiring and cabling (routes, ducts, piping, etc.) security?
Answer: ...... (YES) ...... (NO)

6. Office applications

Q.1. Register; Answer: ...... (YES) ...... (NO)
Q.2. Word Software - Personal data? Answer: ...... (YES) ...... (NO)
Q.3. EXCEL Software - Personal data? Answer: ...... (YES) ...... (NO)
Q.4. PDFs - Personal data? Answer: ...... (YES) ...... (NO)
Q.5. Powerpoint Software - Personal data? Answer: ...... (YES) ...... (NO)
Q.6. Other Software- Personal data? Answer: ...... (YES) ...... (NO)
Q.7. Passwords in documents; Answer: ...... (YES) ...... (NO)
Q.8. Backup of Personal Data? Answer: ...... (YES) ...... (NO)

7. E-Mail

Q.1. Personal data? Answer: ...... (YES) ...... (NO)
Q.2. Encryption: .... (YES) ...... (NO)
Q.3. Maintenance contract? Answer: .... (YES) ...... (NO)
Q.4. Use Hotmail, Gmail, yahoo, etc.? Answer:...(YES) ...... (NO)

8. Evacuation Instructions

Question 1. Posted / Personnel aware; Answer: ...... (YES) ...... (NO)
Question 2. Fire Drills? Answer: ...... (YES) ...... (NO)
Question 3. Earth Quake Drills; Answer:.......................

9. Business Records

Question 1. Filing system; Answer: ...... (YES) ...... (NO)
Question 2. Locking? Answer: ...... (YES) ...... (NO)
Question 3. Archiving (offsite) with security; Answer:......(YES) ...... (NO)

10. Mail Management

Question 1. Incoming? Answer: ...... (YES) ...... (NO)
Question 2. Outgoing? Answer: ...... (YES) ...... (NO)
Question 3. Courier Service; Answer:.............................
Question 4. Checking Suspicious Packages (Bombs, dangerous materials, etc.)? Answer:...... ...... (YES) ...... (NO)

11. Document Management

Question 1. Confidentiality stamping; Answer: ...... (YES) ...... (NO)

12. Safety Vault

Question 1. Onsite? Answer: ...... (YES) ...... (NO)
Question 2. Offsite? Answer: ...... (YES) ...... (NO)
Question 3. Bank deposit box; Answer: .... (YES) ...... (NO)
Question 4. Backup storage register; Answer: .... (YES) ...... (NO) ...

13. Information Disposal

Question 1. Paper shredders; Answer: ...... (YES) ...... (NO)
Question 2. Digital shredders; Answer: ...... (YES) ...... (NO)
Question 3. Paper garbage disposal; Answer: .... (YES) ...... (NO)
Question 4. Backup storage register; Answer: .... (YES) ...... (NO).

14. Cleaning crews

Question 1. Office hours and supervised; Answer: ...... (YES) ...... (NO)
Question 2. Clean desk and screen policy; Answer: ...... (YES) ...... (NO)

15. Dealing with visitors

Question 1. Procedure; Answer: ...... (YES) ...... (NO)

16. HR Records Management

Q.1. Employee performance review procedure; Answer: .. (YES) ...... (NO)
Q.2. Employee records management and security; Answer: ..(YES) ..(NO)
Q.3. Health data / records security; Answer: ......(YES) ...... (NO)
Q.4. Employee attendance records security; Answer: ......(YES) ...... (NO).
Q.5. Employee privacy policy; Answer: ....: ...... (YES) ...... (NO).

4 GDPR GAP TOOL 4: IT PRIVACY ASSESSMENT QUESTIONNAIRE

This questionnaire (see below) relates to assessing the IT Privacy issues of the example company ('XYZ Corporation').

Question 1. Awareness. Have the IT staff been informed of the requirements of the European Union General Data Protection Regulation (GDPR)? Answer: Yes: ____ or No: ____
Question 2. Education. Have the IT staff been trained on data protection issues? Answer: Yes: ____ or No: ____
Question 3. IT Assets Inventory. Have all Systems, Applications, Equipment and Digital Media containing Personal Data recorded in the assets inventory? Answer: Yes: ____ or No: ____
Question 4. Risk Analysis. Have the information security and privacy protection risks been analyzed and have the corresponding measures taken to reduce their respective identified risks? Answer: Yes: ____ or No: ____

Question 5. Consent of Data Subjects. Has a Technical Platform for consent been developed, tested and implemented?
Answer: Yes: _____ or No: _____

Question 6. Rights of Data Subjects. Has a Technical Platform for exercising all rights of data subjects (access, correction, deletion, portability, etc.) been developed, tested and implemented?
Answer: Yes: _____ or No: _____

Question 7. Personal Data Breach. Has a Personal Data Breach process for monitoring, resolving and reporting incidents been developed, tested and implemented? Answer: Yes: _____ or No: _____

Question 8. Data Classification. Has the Data Classification System been developed, tested and implemented? Answer: Yes: _____ or No: _____

Question 9. Upgrading Applications. Have all applications that require privacy indicators or controls on data, files, programs, screens, reports, data bases, etc., been upgraded and changes applied?
Answer: Yes: _____ or No: _____

Question 10. Upgrading Policies and Procedures. Have all IT policies and procedures that require the incorporation of privacy (e.g., DLP, anonymity, masking, developing programs with privacy and security, backup/recovery, logging, network administration, disaster recovery, etc.) been upgraded and changed accordingly?
Answer: Yes: _____ or No: _____

Question 11. Upgrading Application Testing Environment. Has the application testing environment incorporated privacy (e.g., 'dummy' or 'synthetic' data, anonymity, masking, etc.) for the applications requiring privacy for personal data been upgraded and changed accordingly?
Answer: Yes: _____ or No: _____

Question 12. Cloud Service and Solutions

12.1. Are you using the services of a Cloud Services Provider for processing personal data;
Answer: Yes: _____ or No: _____

12.2. Have you conducted a risk assessment before the assignment of the processing of personal data to a selected Cloud Services Provider;
Answer: Yes: _____ or No: _____

12.3. Do you use Cloud Storage Mechanisms such as Dropbox, Onedrive, Google Drive, etc., for personal data?
Answer: Yes: _____ or No: _____

Question 13. E-Mail Service Providers. Are you using Hotmail/Gmail/Yahoo for sending personal data for business purposes?
Answer: Yes: _____ or No: _____

Question 14. Meta data of Digital Documents. Have you developed a policy on clearing metadata on documents containing personal data and organized by software such as Word, Excel, PDF, etc.
Answer: Yes: ____ or No: ____
Question 15. Reviewing Contracts with Third Parties. Have you reviewed contracts with third parties such as software vendors, etc., to ensure that they are upgraded in terms of GDPR?
Question 16. Application/Data Base Logging. Have you implemented a mechanism for recording (Application Log, Data Base Log, Audit Trail, etc.) all changes, updates, accesses, etc., in all applications processing personal data?
Answer: Yes: ____ or No: ____

5 GDPR GAP TOOL 5: FULL GDPR COMPLIANCE DOCUMENTATION LIST

A. Basic GDPR Compliance Documentation

1. Privacy Laws Manual.
2. GDPR Compliance Manager
3. Gap Analysis.
4. GDPR Work Plan
5. GDPR Task Descriptions.
6. Privacy Training Plan
7. Privacy Notice (Website, Employees)
8. Personal Data consent template.
9. Personal Data access template
10. Personal Data erase, correction and portability tools
11. Personal Data Breach Controls (Data Breach Register, Breach Procedure)
12. Encryption Policy.
13. Pseudonymisation Policy.
14. Cookies Policy
15. Upgraded BCP.
16. Upgraded IT Disaster Plan
17. Controller Responsibilities.
18. DPO Responsibilities
19. Updated Processor Contracts.
20. Personal Data Flows Documentation
21. Processing Records Documentation (Personal Data Inventory)
22. Employee Personal Data Management Instructions
23. DPIA Report.
24. Data Protection Measures (review and select according to needs and risks assessment). See next.

B. Additional GDPR Compliance Documentation (Data Protection Measures)

B.1. Strategies

1. Privacy Awareness, Communication and Training Strategy
2. Data Protection Technology Strategy
3. IT Security Strategy

B.2. Plans

1. Privacy Awareness, Communication and Training Plan
2. Requests, Complaints and Rectification Plan
3. Third-Party Risks Management Plan
4. Integration Activities Plan.
5. Data Quality Improvement Plan
6. Data Security Management Plan
7. Social Media Governance Plan.
8. IT Security Management Plan
9. System Development Security Plan
10. Personal Data Breach Incident Response Plan
11. IT Disaster Recovery Plan.
12. Business Continuity Plan

B.3. Policies. A set of policies related to

1. Data Protection,
2. Corporate Records Retention and Destruction,
3. Data Classification,
4. Data Quality,
5. Personal Data Minimization,
6. Encryption,
7. Personal Data Pseudomymisation,
8. IT Governance,
9. IT Security,
10. Password Controls,
11. Security Policy for Personal Computers,
12. Security Policy for Laptops and Smart Devices,
13. Confidentiality,

14. Business Ethics,
15. Clean Desk,
16. Workplace Wellness,
17. Occupational Stress,
18. Health and Safety,
19. Compliance,
20. Data privacy notice,
21. Web site terms/Cookie Consent Policy

B.4. Procedures

1. Personal Data Minimization procedure
2. Encryption procedure
3. Personal Data Pseudomymisation procedure
4. Sensitive data management procedure
5. Automated decision-making handling procedure
6. Data quality improvement procedure
7. Data protection review procedure
8. Personal data collection review procedure
9. Personal data deletion procedure
10. Personal data requests support procedure
11. Personal data rectification procedure
12. Personal data portability support procedure
13. Data Protection Impact Assessment procedure
14. Privacy Reporting Procedure
15. Personal data protection documentation maintenance procedure
16. Personal data breach management procedure
17. Personal data internal audit procedure
18. Personal data external audit procedure
19. Personal data special assessment procedure
20. Data Protection risk resolution procedure
21. Data Protection risk evaluation and reporting procedure
22. Privacy laws monitoring procedure
23. Security risk assessment procedure
24. IT backup/recovery procedure
25. Business Continuity procedure

B.5. Software

1. Software tools for data masking.
2. Online template consent forms.
3. Data protection computerized system
4. Personal Data Minimization software.
5. Encryption software
6. Personal Data Pseudomymisation software
7. Data loss prevention software.
8. Network security software

B.6. Data Protection Responsibilities

1. Board Director for Data Protection Job Description
2. Data Protection Officer Job Description
3. Controller Job Description
4. Personal Data Requests Coordinator Job Description
5. EU Representative Job Description
6. Processor Job Description
7. Information Security Manager Job Description
8. Data Quality Roles and Responsibilities (for Managers; ICT Personnel; Data Quality Officers; Administrative staff; Business Data Librarian; Business Data Steward; and Data Custodian or Data Base Administrator)

B.7. Registers

1. Business Data Elements Register.
2. Data Subjects Register.
3. Personal Data Elements Dictionary
4. Corporate Risks Register

6 GDPR GAP TOOL 6: IT SYSTEMS DEVELOPMENT PRIVACY AND SECURITY PLAN

Phase 1: Preparation Phase

Most business executives and corporate staff assume that web developers have a solid understanding of the most common vulnerabilities that affect web applications. However, this is not the usual case. Most developers around the world who develop web applications have been taught how to make these applications work in practice without knowing how to make these applications safe from attacks.

Developers often have the assumption that all security has to come from the network side (firewalls, SSL, server, etc.). Only a handful of people in each company realize that web application security is within the code of the computer programs. The code contains the vulnerabilities, and is also the only place that corrections can be applied.

On this issue of preparation and for better system security and privacy the following steps will have to be carried out during this phase:

Step 1.1. Training on security and privacy of information systems: Training should be phased in, and strengthened during the year. Start by generalizing security awareness and application data privacy awareness, and then add language classes (HTML, JAVA, C ++, etc.) specifically for developers. Especially for application data privacy, it is advisable to provide training on concepts and principles of privacy. Keep in mind that developers have a lot on their plate, and do not expect them to be data privacy experts. Make the training as specific as possible by linking education to their current projects. Stay away from abstract information that will not be easily absorbed.

Have your developers review the following document: 'An Introduction to Privacy Engineering and Risk Management in Federal Systems' (https://doi.org/10.6028/NIST.IR.8062, January 2017).

Step 1.2. Common security libraries and privacy systems libraries: To write defensive software code, you need to have a set of security and privacy controls in the code of those programs. You want a standard, unified front of security controls to protect your digital assets. It's important to provide developers with guidance on exactly what security and privacy controls you should be using.

For example, when a developer writes SQL Statements into web applications, he must ensure that all user commands for use in the SQL statements are parameterized. Otherwise, this results in an SQL Injection, which may lead to an illegal invasion later.
So do not let the individual developers write code defensively. Even among security professionals, there is often disagreement about security and privacy controls and the best balance between safety, performance and flexibility.
This is why you create a library with examples of security and privacy controls that developers need to use. These controls should be appropriate for your business and vary according to the chosen language and other factors. This is a task that is best left to an internal security team of your company to develop.

Phase 2: Initiation Phase

During this phase, IT system development staff perform a series of actions to collect the needs of the new system and develop the feasibility analysis of the system to decide on further development actions. Regarding the security of the system, the following steps should be considered during this phase:

Step 2.1. Information Systems Risk Management: During the general phase of risk analysis and management, both the IT risks and how to deal with them have been identified. At this point, you need to focus on the risks that are important to the particular information system and how they should be assessed and addressed.

Step 2.2. Sensitivity Analysis: During the feasibility study phase, the need for a system is expressed, the purpose of the system is documented, and any security and privacy needs as well as expectations and specifications are noted. In addition, beyond step 1.1, an assessment should be carried out to examine the sensitivity of the information to be processed by the particular system as well as the system itself**.**

Phase 3: Development Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise manufactured. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle. On the issue of system security and privacy, the following steps should be considered during this phase:

Step 3.1. Defining Security and Privacy Requirements: This step should develop the security and privacy requirements of the system while defining the requirements of system users.

1. These security and privacy requirements may be expressed as technical characteristics (e.g., access controls, encryption of personal data), statements of assurance (e.g., system development audits), or business practices (e.g., awareness and training).
2. Particular attention should also be paid to the security issues of Web and Mobile Applications.
3. **Secure login process**: Use the following procedure to add more security to your online systems.
   - Do not display system IDs until the log-on process has been completed successfully.
   - Display a general notice warning that access to the system is permitted only by authorized users.
   - Do not provide help messages during the log-on process to assist an unauthorized user.
   - Validate log-on process only after all input data has been completed. If errors occur, the system should not report data that is correct or incorrect.
   - Limit the number of unsuccessful login attempts (e.g., three attempts).
   - Record unsuccessful and unsuccessful attempts.
   - Impose a delay before attempting further connection.
   - Send an alarm message when the maximum number of connection attempts has been reached.
   - Display the following information upon successful completion of the connection: Date and time of previous successful login, Details of any unsuccessful connection attempts since the last successful connection, Do not show the entered password or hide the password characters with other symbols, and Do not transmit passwords in plain text over a network (in encrypted format only).

Step 3.2. Integrating Security and Privacy Requirements into Specifications: In this step you will need to integrate the system security and privacy needs identified in the previous step (Step 2.1. Defining Security Requirements) into the specifications, requirements and needs of system users.

Step 3.3. Monitoring System Development: Whether the system is built within the company or purchased ready, you should closely monitor both the system development process itself and the development and integration of system security and privacy features specified in the previous steps.

Step 3.4. Independent Security and Privacy Development Verification: You need to ensure that your developers use security and privacy controls in all cases where required. This is exactly what a code review provides. A second group can look at the code to make sure things are done right.

Step 3.5. Developing Business Practices: In addition to acquiring the system and integrating security and privacy features into it, you must also develop business security practices. These refer to human activities that take place around the development of the system, such as emergency planning, awareness of system users on security, privacy and threats, as well as preparation of documentation, etc.

Phase 4: Implementation Phase

During the application phase, the system has been tested and installed. The following elements should be considered during this phase as regards its security and privacy aspects:

Step 4.1. Enabling Security and Privacy Features: When the system is acquired, this usually comes with the security and privacy features turned off. These should be activated and adjusted according to wht is described in the previous steps. The same is true for a system built within the company.

Step 4.2. Activating the system test plan: Before performing the security and privacy tests discussed in the next step, you must verify that this system has been tested on the basis of a previously prepared test plan. The purpose of this plan is to assure everyone (company management, IT executives, end users, etc.) that this particular IT system will be systematically tested on the basis of a testing methodology and strategy prior to its deployment and launch in production.

Step 4.3. Perform security and privacy tests. Performing system security and privacy tests involves both testing specific parts of the system that have been developed or acquired as well as testing the security and privacy of the entire system.

Phase 5: Operation Phase

During this phase, the system performs its tasks. The system is almost always constantly updated with the addition of hardware and software and many other events and needs. The following elements should be considered during this phase regarding its security and privacy:

Step 5.1. Security and Privacy Management: System operation involves many security and privacy activities, such as: backing up, training courses, managing cryptographic keys, controlling user access privileges, updating security software, etc. Also, security and privacy management examines whether the system is operating in accordance with its current security and privacy requirements. This includes both the actions of the people who operate or use the system and the operation of the system's technical controls.

Step 5.2. Security and Privacy Monitoring: To maintain the operational reliability and security of the system, most organizations and companies use two basic methods: system auditing and monitoring of its activities. The system is checked and its security and privacy evaluated either once or on a periodic basis. Monitoring of system activities and security and privacy incidents refers to an ongoing activity that examines either the system or users or both.

Step 5.3. Production Monitoring: In addition to security and privacy monitoring, it is advisable to monitor, at the senior management level, all systems and applications that are in full production. This will ensure that everything works properly and respond promptly to any problems that occur as quickly as possible.

Phase 6: Archival and Data Removal Phase

This phase of the IT system's lifecycle involves the disposal, archiving and destruction of the information, hardware and software of the specific system. The following elements should be considered during this phase:

Step 6.1. Disposal of information: System information can be moved to another system, archived, discarded, or destroyed. By archiving the information, you should consider the method for retrieving it in the future. While electronic information is generally easier to retrieve and store, the technology used to create the files may not be readily available in the future. You must also take appropriate steps to ensure the secure long-term storage of cryptographic keys for encrypted data. It is equally important to keep in mind all the legal requirements for maintaining files and data when dumping or even destroying the computer systems that have created and maintained them.

Step 6.2. Media Cleanup: Removing (or erasing) information from storage media (such as a hard disk drive, etc.) is called Media Sanitization. Different types of cleansing provide different levels of protection. There are three general methods for cleaning media: overwriting, degaussing (for magnetic media only), and destruction.

Step 6.3. Destruction of printed reports. Bulk printed reports as well as individual pages must be destroyed with special equipment (paper shredders).

Step 6.4. Archival/Destruction Register. You need to record in a register the media and reports that are archived or destroyed. Before destroying anything, you need to make sure of the possible legal implications that often determine how the media and the reports are destroyed, and how long you have to maintain certain data (e.g., payroll, balance sheets, personnel data, etc.). All destructions must also have the signatures of at least 3 approved executives.

Phase 7: Software Privacy Assurance Phase

Ensuring the security and privacy of software is the process of checking that the software is designed to operate at a level of security and privacy that is consistent with the potential harmful consequences that may result from loss, inaccuracy, deterioration, unavailability or misuse. data and resources that it uses, controls, and protects. The following elements should be considered during this phase:

Step 7.1. Software Security and Privacy Assurance Program: You must verify that this program includes at least the following:

1. The security and privacy evaluation has been performed for the software.
2. The security and privacy requirements have been set for the software.
3. Security and privacy requirements have been established for software development and / or operation and maintenance of system processes.
4. Any software review, or audit, shall include an assessment of the security and privacy requirements.
5. The necessary system security and privacy tests have been carried out.
6. The development process is able to provide security for the incorporation of the proposed changes into the system and that these changes do not create unintentional security breaches or vulnerabilities.
7. Physical security for the software is adequate.

Step 7.2. External audit: The security and privacy of the system can also be reviewed by external experts to assure the management of the company or organization that the particular IT system is protected from potential threats, and that certain risks may be accepted as unavoidable. This inspection usually involves examining and evaluating all system security and privacy measures (administrative, operational and technical).

7 GDPR GAP TOOL 7: DATA PROTECTION OFFICER ACTION PLAN

This action plan relates to the DPO actions that may be taken by the example company ('XYZ Corporation').

1. Introduction

The actions of the DPO in accordance with the GDPR (Articles 37, 38 and 39, supporting articles 9, 10, 33, 47 and paragraph 97 of the preamble), experience of similar projects and good governance and corporate governance rules are the following.

2. Actions

Action 1. Assignment of tasks by the Board of Directors

The assignment of duties of the DPO is recorded in the minutes of a meeting of the Board of Directors. or a similar service contract, if assigned to a third party.
The DPO's qualifications include legal expertise and knowledge of data protection practices. The DPO reports to the Board of Directors. and is not a recipient of management orders. The Board of Directors ensures the independence of the DPO, issues guidelines for the use of DPO services, and adjusts the corporate performance review policy for DPO performance issues.
Copies of DPO's qualifications, practices and / or assignment contracts are available in a compliance file for the supervisor data protection authority to review, when required.

Action 2. Ensure DPO independence

The controller or processor, via its board or CEO functions, must ensure the independence of their DPO, by instructing all management staff of the company, to allow him or her to act in a way, such that:

1. The DPO must be able to perform their tasks with sufficient autonomy.
2. The DPO must not be instructed how to deal with a matter, how to investigate a complaint or whether to consult the supervisory authority nor must they be instructed to take a certain view, for example, a particular interpretation of Data Protection legislation.
3. The DPO cannot be dismissed or penalised for performing their tasks.
4. A copy of these DPO independence instructions are included in the compliance file and is available to the Data Protection Authority, as required.

Action 3. Issue DPO Consulting Guidelines

Where appropriate, the controller or processor could develop data protection guidelines that set out when the DPO must be consulted, such that:

1. The DPO is involved from the earliest stage possible in all issues relating to data protection.
2. The controller seeks the advice of the DPO when carrying out DPIAs (data protection impact assessments) and in using aspects of privacy by design in all systems, products, functions and services.
3. The DPO is seen as a discussion partner within the organisation and that he or she is part of the relevant working groups dealing with data processing activities within the organisation.
4. The organisation should ensure, for example, that:
   - 4.1. The DPO is invited to participate regularly in meetings of senior and middle management;
   - 4.2. His or her presence is recommended where decisions with data protection implications are taken.
   - 4.3. All relevant information is passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
   - 4.4. The opinion of the DPO must always be given due weight. In case of disagreement, the controller or processor should document the reasons for not following the DPO's advice.
   - 4.5. The DPO must be promptly consulted once a data breach or another incident has occurred.
5. A copy of these DPO consulting instructions are included in the compliance file and is available to the Data Protection Authority, as required.

Action 4. Issue DPO performance review instructions

1. The controller or processor, via its board or CEO functions, must ensure that DPOs should 'not be dismissed or penalised by the controller or the processor for performing their tasks' (article 38(3)) and update the company performance policy and procedures accordingly.
2. Penalties could be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient if they are intended to penalise the DPO for performing their tasks.
3. **Penalties** are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.
4. As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).
5. Ensure that a copy of company performance review policy and procedures containing these DPO performance review instructions are included in the compliance file and is available to the Data Protection Authority, as required.

Action 5. Statement of confidentiality

1. The Controller or the Processor, through the B o D or his / her managing director, must ensure that the DPO is bound by confidentiality in the performance of his / her duties.
2. This obligation of confidentiality does not prevent the Data Protection Officer (DPO) from contacting and seeking the advice of the Supervisory Authority as provided for in Article 39 (1) (e) that the DPO may consult the Supervisory Authority on any other subject matter, as appropriate.
3. The DPO signs a confidentiality statement as regards the responsibility of confidentiality.
4. This statement is available in a compliance file for the supervisory authority when required.

Action 6. Minutes of meetings of discussions

All data protection issues that are being discussed with everyone (administration, employees, third parties, etc.) are kept in a file.
These are available in a compliance file for the supervisory authority when required.

Action 7. Counseling sessions

For all data protection issues requested and provided by DPO (e.g., DPIA, etc.) to Controller and Processor staff, minutes are kept.
These are available in a compliance file for the supervisory authority when required.

Action 8. Corporate Resources

The company provides the necessary resources (equipment, personnel, time, systems, tools, support, certification, training, access to information, etc.) for all data protection issues requested by the DPO.
Details for all these elements are available in a compliance file for the supervisory authority when required.

Action 9. Train DPO

1. Article 38(2) of the GDPR requires the organisation to support its DPO by 'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'.
2. DPOs should be given the opportunity to stay up to date with regard to developments within data protection.
3. The purpose should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.
4. Training should be provided to the DPO for all data protection issues, such as:
   4.1. Understanding how GDPR impacts all business functions, systems and products
   4.2. Assessing privacy compliance
   4.3. Conducting a privacy breach investigation
   4.4. Responding to access requests
   4.5. Evaluating security and privacy safeguards

4.6. Applying Data Protection Principles
4.7. IT and cyber security issues
4.8. How to effectively set up and monitor privacy compliance using tools such as e.g. privacy impact assessment, data mapping analysis, establishing a effective accountability framework, prepare for a data privacy audit from a data protection authority (DPA) etc.

5. A copy of all documents related to DPO training (plan, budget, seminar descriptions, certificates of attendance, etc.) should be included in the compliance records file and be made available to the supervisory authority when required.

Action 10. Inform staff of DPO's role

1. The controller or processor, via its board or CEO functions, must issue an official communication of the designation of the DPO to all staff (according to article 39, 1b) to ensure that his or her existence and function is known within the organisation.
2. A copy of all documents related to this announcement of the DPO to staff should be included in the compliance records file and be made available to the supervisory authority when required.

Action 11. Educate and train staff

1. The DPO ensures that a Privacy Awareness, Communication and Training Plan is crafted and executed.
2. The objective of this plan should be: to provide ongoing privacy awareness and training to promote compliance with the data privacy practices, policies and procedures.
3. The work tasks of this plan should be:
   3.1. Carry out ongoing data privacy training for the Privacy Office;
   3.2. Execute basic privacy training for staff;
   3.3. Execute additional privacy training for new needs;
   3.4. Include data privacy training into other corporate training;
   3.5. Maintain data privacy awareness;
   3.6. Maintain data privacy professional certification for privacy personnel; and
   3.7. Measure data privacy awareness and training activities.
4. A copy of all documentation related to the above-mentioned tasks of raising staff awareness, implementing training and taking certification on privacy and security, should be included in the compliance records file and be made available to the supervisory authority when required.

Action 12. Oversee the adoption of data protection into the Internal Rules of Operation

1. The DPO oversees the adoption and incorporation of data protection rules into the Internal Rules of Operation and the briefing of all staff.
2. A copy of all documentation related to incorporating data protection into the company's internal rules of operation should be included in the compliance records file and be made available to the supervisory authority when required.

Action 13. Ensure no Conflict of Interests for DPO

1. The controller or processor, via its board or CEO functions, must ensure that the DPO should not hold a position within the organisation that leads him or her to determine the purposes and the means of processing of personal data.
2. Conflicting positions within the organisation may include senior management positions such as:
   2.1. Chief Executive Officer,
   2.2. Chief Operating Officer,
   2.3. Chief Financial Officer,

2.4. Chief Technology Officer,
2.5. Chief Information Officer,
2.5. Chief Medical Officer,
2.6. Head of Marketing Department,
2.7. Head of Human Resources, or
2.8. Any other role that leads to the determination of purposes and means of processing.

3. Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:
   3.1. To identify the positions which would be incompatible with the function of DPO
   3.2. To draw up internal rules to this effect in order to avoid conflicts of interests
   3.3. To include a more general explanation about conflicts of interests
   3.4. To declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
   3.5. To include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests.
   3.6. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.
4. Ensure the DPO signs the Conflict of Interest statement and that a copy of this is filed in the compliance records file for the supervisory authority when required.

Action 14. Establish Contact with Data Protection Authority

Article 37(7) of the GDPR requires the controller or the processor: to publish the contact details of the DPO and to communicate the contact details to the relevant supervisory authorities. The objective of these requirements is to ensure that data subjects (both inside and outside of the organisation) and the supervisory authorities can easily, directly and confidentially contact the DPO without having to contact another part of the organisation.

1. The DPO must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned.
2. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned.

3. To this effect the DPO communicates his or her details and establishes an effective communication mechanism with the local data protection authority.
   3.1. These details include: A name and surname, a postal address, a dedicated telephone number, and/or a dedicated e-mail address.
4. A copy of all documentation related to this communication should be included in the compliance records file and be made available to the supervisory authority when required.

Action 15. DPIA

1. The DPO should design a DPIA methodology for the specific company or become fully aware of the existing methodologies that could be used for carrying out a DPIA.
2. According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller 'shall seek advice' of the DPO when carrying out a DPIA.
3. Article 39(1)(c), in turn, tasks the DPO with the duty to 'provide advice where requested as regards the [DPIA] and monitor its performance'.
4. The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others:
   4.1. whether or not to carry out a DPIA
   4.2. what methodology to follow when carrying out a DPIA
   4.3. whether to carry out the DPIA in-house or whether to outsource it
   4.4. what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
   4.5. whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR
   4.6. If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account36.
5. The DPO assesses the risks for all data processing issues, and maintains the relevant documentation.

Action 16. The DPO's role in data protection impact assessments

1. A copy of all documentation related to the DPIA activities should be included in the compliance records file and be made available to the supervisory authority when required.

Action 17. Informing the public

1. The DPO must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned.
2. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned.
3. All DPO data (name, surname, address, telephone, dedicated e-mail address, etc.) are communicated to the public through the company's privacy policy.
4. A copy of all documentation related to the activitites of the DPO as regards informinh the public (company privacy notice, etc.) should be included in the compliance records file and be made available to the supervisory authority when required.

Action 18. Ensure the execution of data protection audits

1. The DPO ensures that data protection audits are carried out by the appropriate staff and on the basis of a bona fide audit process.
2. The audit process should have the following phases:
   2.1. Plan audit.
   2.2. Prepare audit.
   2.3. Execute GDPR compliance audit.
   2.4. Issue compliance audit report.
   2.5. Perform audit follow-up.
3. A copy of all documentation related to data protection audits should be included in the compliance records file and be made available to the supervisory authority when required.

Action 19. Data Protection Policies

1. Under Article 24(2) a controller must implement proportionate and appropriate data protection policies.
2. Providing advice and monitoring compliance with these policies are tasks of the DPO.
3. The DPO ensures these data protection policies remain appropriate and are up to date.
4. A copy of all documentation related to the activitites of the DPO as regards advising the controller and monitoring compliance of the company's data protection policies should be included in the compliance records file and be made available to the supervisory authority when required.

Action 20. Compliance Monitoring

1. The DPO shall maintain, in writing, and in electronic form, the Record of Processing Activities (Article 30, EU GDPR) and in accordance with the second subparagraph of Article 49 (1) and Article 32 (1).
2. The DPO establishes, organizes and maintains a compliance monitoring system for all aspects of company privacy.

Action 21. Compliance File

All data, correspondence, policies, documentation, etc., mentioned in the previous actions and directly or indirectly related to data protection issues, as well as the documentation of all technical and organizational measures, policies and data protection procedures (e.g., Educational material, GDPR presentation in PowerPoint, Notes, etc., Record of processing activities, Policies of Data Protection, Data Satisfaction Requests and Data Breach Procedures, Compliance Report, etc.) are kept by the company in an electronic and manual file and updated, depending on the changes, etc.
This compliance file is available to the supervisory authority when required.

8 GDPR GAP TOOL 8: GDPR COMPLIANCE ACTION PLAN

This action plan (see below) relates to the compliance actions that may be implemented for the example company ('XYZ Corporation').

PHASE A: PREPARATION (PR)

Step PR1: Review privacy laws and standards relevant to company.
Compliance Action: Establish and maintain Privacy Laws Manual
Responsible: <Name of person responsible to complete this task>
Compliance Evidence (Control): Privacy Laws Manual
Implementation End Date: <DD/MM/YYYY>

Step PR2: Collect and review company policies, procedures, forms and other relevant documentation (company charter, IT inventory, etc.)
Compliance Action: Establish and maintain Company Privacy policies, procedures, forms and registers.
Responsible: <Name of person responsible to complete this task>
Compliance Evidence (Control): Company Privacy policies, procedures, forms and registers
Implementation End Date: <DD/MM/YYYY>

Step PR3: Appoint EU GDPR Compliance manager
Action 1: Select and appoint manager to organize and carry out all activities related to implementing data protection and privacy for your specific company.
Action 2: Allocate the necessary resources (time, people, tools, funds, systems, equipment, etc.) for the implementation of this plan.
Action 3: Carry out a Data Protection and Security readiness exercise.
Action 4: Establish the budget for implementing data protection and privacy.
Compliance Action: Establish and maintain a GDPR Project Plan and Budget.
Responsible: <GDPR Compliance Manager>
Compliance Evidence (Control): GDPR Project Plan and Budget Implementation End Date: <DD/MM/YYYY>

Step PR4: Carry out Gap analysis (management, legal, IT) establishing current level of compliance with the EU GDPR.
Compliance Action: Include the actions noted in the Gap Analysis conducted previously (See chapters 2 to 6 of 'GDPR GAP Analysis' book) into this plan. See also Annex B. Integrated Compliance Actions List.
Responsible: <GDPR Compliance Manager>
Compliance Evidence (Control): GDPR Gap Analysis Report
Implementation End Date: <DD/MM/YYYY>

Step PR5: Define GDPR work plan to meet compliance requirements of EU GDPR
Compliance Action: Ensure GDPR work plan has adequate resources.
Responsible: <GDPR Compliance Manager>
Compliance Evidence (Control): GDPR Project Work Plan
Implementation End Date: <DD/MM/YYYY>

Step PR6: Assign work tasks to company people to implement
Compliance Action: Ensure GDPR work tasks are assigned.
Responsible: <GDPR Compliance Manager> and individual company staff
Compliance Evidence (Control): GDPR Project Work Staff Assignments
Implementation End Date: <DD/MM/YYYY>

PHASE B: ORGANIZATION (OR)

==
Step OR1: Carry out privacy awareness and training activities for all staff
Compliance Action: Ensure execution of GDPR training.
Responsible: <GDPR Compliance Manager>
Compliance Evidence (Control): GDPR Training Plan
Implementation End Date: <DD/MM/YYYY>

Step OR2: Appoint Controller
Compliance Action: Ensure definition of Controller Responsibilities and assignment to a specific person.
Responsible: <GDPR Compliance Manager>
Compliance Evidence (Control): Controller Duties
Implementation End Date: <DD/MM/YYYY>

Step OR3: Appoint Data Protection Officer
Compliance Action: Ensure implementation of DPO Action Plan (see GDPR Gap Tool 7).
Responsible: <DPO Officer>
Compliance Evidence (Control): See outputs of DPO Action Plan
Implementation End Date: <DD/MM/YYYY>

Step OR4: Review Processor needs and make changes to contracts
Compliance Action: Ensure Processor Contracts are upgraded to align with GDPR specifications.
Responsible: <GDPR Compliance Manager>
Compliance Evidence (Control): Updated Processor Contracts
Implementation End Date: <DD/MM/YYYY>

Step OR5: Create plan for implementing additional Privacy management, IT and Legal Controls.
Compliance Action: Ensure creation of additional IT and Legal Controls Plan on the basis of GDPR specifications.
Responsible: <GDPR Compliance Manager>
Compliance Evidence (Control): Additional Privacy management, IT and Legal GDPR Controls
Implementation End Date: <DD/MM/YYYY>

PHASE C: DEVELOPMENT (DV)

Step DV1: Document Personal Data Flows (by company department and process within each department: e.g. HR/Hiring employees, etc.)
Compliance Action: Ensure maintenance of Personal Data Inventory Documentation.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Personal Data Inventory
Implementation End Date: <DD/MM/YYYY>

Step DV2: Create IT Assets Inventory (by company department and process within each department: e.g. HR/Hiring employees, etc.).
Compliance Action: Ensure maintenance of IT Assets Inventory Documentation.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): IT Assets Inventory
Implementation End Date: <DD/MM/YYYY>

Step DV3: Develop a Data Protection Impact Assessment (DPIA) methodology and identify all IT systems, services and products and especially the high-risk operations of processing of personal data that require a DPIA.
Compliance Action: Ensure a DPIA methodology is created and operations are identified for executing a DPIA.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): DPIA Methodology
Implementation End Date: <DD/MM/YYYY>

Step DV4: Create Data Protection Organizational and Technical Measures.
Compliance Action: Ensure a full set of DP Organizational and Technical Measures are developed considering Annex 1, Appendices 1 to 7 of this book and the actions noted in the GAP Analysis executed in Chapters 2 to 6 of 'GDPR GAP Analysis' book.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): DP Organizational and Technical Measures Documentation
Implementation End Date: <DD/MM/YYYY>

PHASE D: IMPLEMENTATION (IM)

Step IM1: Select and implement specific Data Protection Measures (policies and procedures).
Compliance Action: Ensure a selected to the company specifications set of DP Organizational and Technical Measures are implemented considering Annex 1, Appendices 1 to 7 of this book and the actions noted in the GAP Analysis executed in Chapters 2 to 6 of 'GDPR GAP Analysis' book.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Documentation for selected DP Organizational and Technical Measures implemented
Implementation End Date: <DD/MM/YYYY>

Step IM2: Implement data protection measures for Data subjects (consent, access, correct, erase and portability, etc.).
Compliance Action: Ensure a specific to the company's needs, requirements and specifications System to satisfy the Rights of Data Subjects (consent, access functions) is implemented.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Documentation for the implemented System to satisfy the Rights of Data Subjects
Implementation End Date: <DD/MM/YYYY>

Step IM3: Review and update privacy notices to meet GDPR requirements
Compliance Action: Ensure privacy notices are upgraded to GDPR specifications.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Upgraded Privacy Notices Documentation
Implementation End Date: <DD/MM/YYYY>

Step IM4: Ensure all data flows have the correct legal basis
Compliance Action: Ensure the legal basis of all data flows are recorded in PD Inventory.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Upgraded Personal Data Inventory with the legal basis recorded for all processes of personal data
Implementation End Date: <DD/MM/YYYY>

Step IM5: Consider Child Consent and update all consent processes
Compliance Action: Ensure child consent is included in all relevant forms, procedures and business processes.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Upgraded Child Consent Process in all relevant forms, procedures and business processes
Implementation End Date: <DD/MM/YYYY>

Step IM6: Establish and maintain processing records documentation
Compliance Action: Ensure effective maintenance of your company's processing records (article 30).
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Personal Data Inventory (paper and electronic)
Implementation End Date: <DD/MM/YYYY>

Step IM7: Establish and implement personal data breach controls
Compliance Action: Ensure effective implementation of your company's data breach controls.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Personal Data Breach Controls Implementation End Date: <DD/MM/YYYY>

Step IM8: Implement encryption to data at rest and in motion
Compliance Action: Ensure effective implementation of encryption policy to your company's personal data.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Encryption Policy and software
Implementation End Date: <DD/MM/YYYY>

Step IM09: Implement pseudonymisation to personal data of all systems and media
Compliance Action: Ensure effective implementation of pseudonymization to your company's personal data.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): Pseudonymization Policy and software
Implementation End Date: <DD/MM/YYYY>

Step IM10: Include data protection in Business Continuity Plans (BCP)
Compliance Action: Ensure data protection aspects are included in your company's Business Continuity Plans for the processing of critical personal data.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): BCP Plan Documentation
Implementation End Date: <DD/MM/YYYY>

Step IM11: Include data protection in IT Disaster Plan
Compliance Action: Ensure data protection aspects are included in your company's IT Disaster Plans for the processing of critical personal data.
Responsible: <GDPR Compliance Manager or DPO>
Compliance Evidence (Control): IT Disaster Plan Documentation
Implementation End Date: <DD/MM/YYYY>

Step IM12: Upgrade all business functions and incorporate privacy controls (IT, legal and business) into daily operational activities
Compliance Action: Ensure effective implementation of a Protection by Design and by Default Methodology in your company's IT Systems and business functions.
Responsible: <GDPR Compliance Manager or DPO or IT Manager>
Compliance Evidence (Control): Protection by Design and by Default Methodology and Privacy Controls implemented documentation
Implementation End Date: <DD/MM/YYYY>

Step IM13: Carry out a Data Protection Impact Assessment (DPIA) for all IT systems, services and products and especially for high risk operations of processing of personal data
Compliance Action: Ensure effective implementation of a DPIA in your company's IT Systems, services and products.
Responsible: <GDPR Compliance Manager or IT Manager>
Compliance Evidence (Control): DPIA Methodology and DPIA Report
Implementation End Date: <DD/MM/YYYY>

Step IM14: Implement measures for doing personal data processing business with third parties (partners, outsourcing entities, cloud providers, hardware and software vendors, etc.)
Compliance Action: Ensure effective implementation of upgraded to GDPR processor services agreements.
Responsible: <GDPR Compliance Manager or Controller or Procurement Manager >
Compliance Evidence (Controls): Updated processor services agreements
Implementation End Date: <DD/MM/YYYY>

Step IM15: Implement measures for transferring personal data outside the EU
Compliance Action: Ensure effective implementation of measures (Transfer agreements, BCRs, etc.) of transferring personal data outside the EU.
Responsible: <GDPR Compliance Manager or Controller or DPO>
Compliance Evidence (Controls): Documentation for Data Transfer agreements
Implementation End Date: <DD/MM/YYYY>

Step IM16: Ensure all relevant corporate policies (HR, Quality, Marketing, Customer Support, Production, etc.) align to GDPR requirements
Compliance Action: Ensure effective alignment of all corporate policies and procedures with GDPR requirements.
Responsible: <GDPR Compliance Manager or Controller or DPO>
Compliance Evidence (Controls): Documentation for Upgraded Corporate Policies and Procedures
Implementation End Date: <DD/MM/YYYY>

Step IM17: Implement IT and Data Security Controls
Compliance Action: Ensure effective implementation of IT and Data Security Controls in all IT Systems and business functions.
Responsible: <GDPR Compliance Manager or IT Manager>
Compliance Evidence (Controls): Documentation for IT and Data Security Controls implemented
Implementation End Date: <DD/MM/YYYY>

Step IM18: Align information security incident policy and process to GDPR
Compliance Action: Ensure effective integration of your company's security incident policy and procedures to GDPR requirements.
Responsible: <GDPR Compliance Manager or IT Manager>
Compliance Evidence (Controls): Documentation for aligning information security incident policy and process to GDPR
Implementation End Date: <DD/MM/YYYY>

PHASE E: EVALUATION (EV)

Step EV1: Audit and assess data protection and privacy compliance
Compliance Action: Ensure effective Data Protection audits are executed by Internal Audit on an annual basis.
Responsible: <GDPR Compliance Manager or Internal Audit Manager>
Compliance Evidence (Control): Data Protection Audit Report
Implementation End Date: <DD/MM/YYYY>

Step EV2: Improve data protection and privacy organizational and technical measures
Compliance Action: Ensure effective improvement of Data Protection and Privacy Organizational and Technical measures on a periodic basis.
Responsible: <DPO or Internal Audit Manager>
Compliance Evidence (Control): Upgraded Data Protection Measures
Implementation End Date: <DD/MM/YYYY>

Step EV3: Ensure accuracy of all public and internal documentation which references to Data Protection
Compliance Action: Ensure effective execution of data quality improvement procedures for all company personal data on a periodic basis.
Responsible: <Controller or DPO>
Compliance Evidence (Control): Accuracy Assessment Report
Implementation End Date: <DD/MM/YYYY>
Compliance Evidence (Control): Accuracy Assessment Report

Step EV4: Ensure maintenance of GDPR Compliance Records
Compliance Action: Ensure effective maintenance GDPR Compliance records.
Responsible: <Controller or DPO>
Compliance Evidence (Control): GDPR Compliance Records
Compliance Evidence (Control): Accuracy Assessment Report
Implementation End Date: <DD/MM/YYYY>

Annex 1: Data Protection Measures

Set 1: Strategies

1. Privacy Awareness, Communication and Training Strategy
2. Data Protection Technology Strategy
3. IT Security Strategy

Set 2: Plans

1. Privacy Awareness, Communication and Training Plan
2. Requests, Complaints and Rectification Plan
3. Third-Party Risks Management Plan
4. Integration Activities Plan
5. Data Quality Improvement Plan
6. Data Security Management Plan
7. Social Media Governance Plan
8. IT Security Management Plan
9. System Development Security Plan
10. Personal Data Breach Incident Response Plan
11. IT Disaster Recovery Plan
12. Business Continuity Plan

Set 3: Policies

1. Data Protection Policy
2. Corporate Records Retention and Destruction Policy
3. Data Classification Policy
4. Data Quality Policy

5. Personal Data Minimization Policy
6. Encryption Policy
7. Personal Data Pseudomymisation Policy
8. Information Technology (IT) Policy
9. Information Technology (IT) Security Policy
10. Password Controls Policy
11. Security Policy for Personal Computers
12. Security Policy for Laptops and Smart Devices
13. Confidentiality Policy
14. Business Ethics Policy
15. Clean Desk Policy
16. Workplace Wellness Policy
17. Occupational Stress Policy
18. Health and Safety Policy
19. Compliance Policy
20. Data privacy notice policy
21. Web site terms/Cookie Consent Policy

Set 4: Procedures

1. Personal Data Minimization procedure
2. Encryption procedure
3. Personal Data Pseudomymisation procedure
4. Sensitive data management procedure
5. Automated decision-making handling procedure
6. Data quality improvement procedure
7. Data protection review procedure
8. Personal data collection review procedure
9. Personal data deletion procedure
10. Personal data requests support procedure
11. Personal data rectification procedure
12. Personal data portability support procedure
13. Data Protection Impact Assessment procedure
14. Privacy Reporting Procedure
15. Personal data protection documentation maintenance procedure
16. Personal data breach management procedure
17. Personal data internal audit procedure
18. Personal data external audit procedure
19. Personal data special assessment procedure

20. Data Protection risk resolution procedure
21. Data Protection risk evaluation and reporting procedure
22. Privacy laws monitoring procedure
23. Security risk assessment procedure
24. IT backup/recovery procedure
25. Business Continuity procedure

Set 5: Software

1. Software tools for data masking
2. Online consent system, template and forms
3. Data protection computerized system
4. Personal Data Minimization software
5. Encryption software
6. Personal Data Pseudomymisation software
7. Data loss prevention software
8. Network security software

Set 6: Data Protection Responsibilities

1. Board Director for Data Protection Job Description
2. Data Protection Officer Job Description
3. Controller Job Description
4. Personal Data Requests Coordinator Job Description
5. EU Representative Job Description
6. Processor Job Description
7. Information Security Manager Job Description
8. Data Quality Roles and Responsibilities (for Managers; ICT Personnel; Data Quality Officers; Administrative staff; Business Data Librarian; Business Data Steward; and Data Custodian or Data Base Administrator)

Set 7: Data Protection Registers

1. Business Data Elements Register
2. Data Subjects Register
3. Personal Data Elements Dictionary
4. Corporate Risk Register

Annex B. Integrated Compliance Actions List

This actions list is based on the assessment carried out for the example company ('XYZ Corporation'), as per book1 and book 3.

1. PD Processing Management

1.1. PD and IT Inventories

1. 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, etc.).
2. Establish, complete and maintain a PD inventory.
3. Complete and maintain an IT Assets inventory.
4. Assign the responsibility of managing these inventories to two distinct staff: One for the personal data and one for the IT – related assets.

1.2. Awareness and Training

1. Craft and implement training on privacy and security issues to all central office staff (board directors, all level managers and employees)
2. Craft and implement training on privacy and security issues to all crew staff (crew managers, masters, crew office staff, onboard crew members)
3. Train all staff on managing personal data.
4. Ensure all staff are aware about their roles and responsibilities on handling data breaches and protecting personal data.
5. Draft and issue PD Management Guidelines to staff.

1.3. Data Management Policies

1. Review current Data Protection policies, codes of conduct and training to ensure these are consistent with the GDPR principles.
2. Policies for data retention, quality and accuracy must be implemented.
3. Establish Register for Access to Physical Files of Storage of PD in the offices of each business function and assign the responsibility to a manager in each specific function.
4. Craft and implement a Policy and Procedures for managing records and deletion and retention periods for PD for the data subjects of the company (employees, crew members, vendors, customers, etc.)

1.4. Employee Privacy

1. Craft and 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.

2. Data Subjects

2.1. Legal Basis of Processing

1. Ensure the recording of legal basis for all processes of personal data in the company's personal data inventory.
2. Ensure that the 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.

2.2. Consent of Data Subjects

1. Craft and implement a system (forms, policy, procedures, technical platform, etc.) for satisfying Consent of Data Subjects of the company, as required (employees, crew members, vendors, customers, etc.)
2. Ensure consent, as required, is added in all relevant forms and procedures.
3. Ensure all consent details for all processes of personal data are recorded also in the company's personal data inventory.
4. Review methods for collecting consent and ensure there is sufficiently robust audit trails.
5. Review systems to ensure that they can record explicit consent (if relied upon), including parental consent.
6. Review the ability of systems to record withdrawal of consent especially where information is shared between practitioners and other companies.

2.3. Transparency

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.
5. Update the company's web site privacy policy to ensure compliance with GDPR.
6. Update the company's cookies policy to ensure compliance with GDPR.

2.4. Rights of Data Subjects

1. A system (forms, policies, procedures, technical platform, portal, etc.) to satisfy the rights (access, rectification, portability, objection, erasure and restriction of processing) of Data Subjects as required (employees, crew members, vendors, customers, etc.) 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.

3. Governance and Organization

3.1. Controller

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

3.2. Compliance

1. 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.

   For more details, also see '**GDPR Gap Tool 5: Full GDPR Compliance Documentation List**'.
2. The Company must implement a process to carry out internal audits for data protection issues.
3. Examine how to use the ISO 27001 certification for GDPR compliance purposes.

3.3. Data Protection Officer

1. The Company must examine if a DPO is needed and appoint one if the need exists.
2. If a DPO is appointed, 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.

3.4. Processor

1. Implement a GDPR-compliant services contract for processing of PD by the following third parties (companies):
   1.1. 'ABC' External Payroll Services Company.
   1.2. 'AXX' Insurance Services Company.
   1.3. Crew Manning Agencies.
   1.4. Travel Agents.
   1.5. Local Agents.
   1.6. Port Agents.

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

4. Data Security and Privacy

4.1. Risk Assessment and DPIA

1. 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. Design and implement DPIA templates in line with GDPR DPIA.
3. Carry out awareness raising to company staff of the requirement to conduct DPIAs to reflect GDPR requirements.
4. Undertake DPIA on newer systems and determine the risk of older systems.
5. 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'.

4.2. Data Protection by Design and Default

1. Implement the data protection by design and default principles, such as pseudonymization, anonymization, encryption, etc.
2. Implement techniques, such as: EXCLUDE, SELECT, STRIP and DESTROY to minimize the PD collected in information systems.

4.3. Security of Processing

1. Improve the Office Physical Access Controls.
2. Implement technical and organizational Data Protection by Design and Default measures (e.g.: masking, anonymization, pseudonymization, etc.) to ensure that PD are collected only as required for the specific purpose and are deleted when they are not required any more.
3. Implement Data Protection by Design and Default measures in the design and development of the company's computerized systems.
4. Obtain an SSL Certificate for the corporate website.
5. Implement appropriate policies to manage and control the use of all office software packages.
6. Improve the company's required Security and Privacy Controls for Processing of PD on the basis of an ISRA, a PDPRA and a DPIA, such as: Password Policy, Backup Policy, IT Disaster Plan, Examination of using Encryption and Pseudonymization in all Information Systems (PMS, FMS, VMS, CMS, etc., as required),
7. Examine security and privacy controls (encryption, pseudonymization, masking, etc.) 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').
8. Improve IT Security Controls, such as: Encrypting data when transferred via the network, Monitoring policy of network transactions and events, Intrusion Detection/Prevention System, Data Loss Prevention Technology, etc.
9. Install a fail-over server.
10. Enhance IT Security Measures (Clean Desk and Screen Policy, Intrusion Detection / Prevention System, Data Loss Prevention Technology).
11. Audit the accuracy of PD with the support of the external application maintenance company and customers.
12. Correct the data errors with the support of the external application maintenance company.
13. Implement IT Audits to all company computerized applications.
14. Implement IT Application Audit Logs for all company computerized applications.
15. Amend retention policy to ensure that Audit Logs are deleted when they are no longer needed.
16. Implement software tools for data aggregation, data masking, anonymization, pseudonymization, etc.
17. Upgrade the maintenance contracts of the external software services companies to ensure that upgrading of software is included in these contracts.

18. Execute the backup of software and data procedure before any upgrading of the software of the computerized applications of the company.
19. Ensure that a report of all tasks executed by the external software maintenance contractors are issued to the company, right after each and every maintenance carried out by the external authorized parties.

4.4. Breach Management

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.

9 GDPR GAP TOOL 9: PRIVACY RISKS

These risks relate to the example company ('XYZ Corporation').
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 that it is necessary.

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.