GDPR Gap Analysis by Process

Evaluating Gaps in GDPR Compliance Better

John Kyriazoglou

bookboon
The eBook company

JOHN KYRIAZOGLOU

GDPR GAP ANALYSIS BY PROCESS

EVALUATING GAPS IN GDPR COMPLIANCE BETTER

GDPR Gap Analysis by Process: Evaluating Gaps in GDPR Compliance Better
1st edition

ISBN 978-87-403-3078-6

CONTENTS

1 CRITICAL GDPR GAP ANALYSIS CRITERIA

Overview: This chapter contains the Operating Framework of Personal Data processed by the example company ('XYZ Corporation') and a description of the 5 criteria used to assess the Company business functions and processes that contain processing of personal data (PD) of Data Subjects (DS) to detect deviation from GDPR requirements.

1. Operating Framework of Personal Data processed by 'XYZ Corporation'

All departments of the 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.

2. Critical Gap Analysis Criteria

The Critical Gap Analysis Criteria, which are used to assess the Company business functions and processes (example company 'XYZ Corporation') that contain processing of personal data (PD) of Data Subjects (DS) to detect deviation from GDPR requirements, are the following:

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

These are detailed in the next paragraph.

2.1. Criterion 1. Principles relating to processing of PD

According to Article 5 of the GDPR, in order for any processing of personal data (PD) to be lawful, it should be governed by the following principles:

Principle 1 ('lawfulness, fairness and transparency' article 5 (1, a))

PD should be treated legally and fairly and transparently in relation to the data subject. Therefore, the criterion for assessing the legality of any processing is the existence of a legitimate purpose and the transparent information to the data subject regarding the purpose, mode and consequences of processing.

Principle 2 ('purpose limitation' article 5 (1, b))

PD should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

Principle 3 ('data minimisation' article 5 (1, c))

PD should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle 4 ('accuracy' article 5 (1, d))

PD should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Principle 5 ('storage limitation' article 5 (1, e))

PD should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

Principle 6 ('integrity and confidentiality' article 5 (1, f))

PD should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, as specified in several articles (e.g.: Article 25 (Data protection by design and by default), Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority), Article 35 (Data protection impact assessment: DPIA)).

Principle 7 ('accountability' article 5 (2))

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (principles 1 to 6 above).

2.2. Criterion 2. Legal basis of processing

Articles 6, and 9 to 11 of GDPR relate to providing a legal basis of processing of personal data These are detailed in the following paragraphs.

Article 6 (Lawfulness of processing)

According to article 6 paragraph 1 of GDPR, the legal bases of processing are the following: ‘consent’, ‘performance of a contract’, ‘legal obligation’, ‘vital interests of the data subject or of another natural person’, ‘public interest or in the exercise of official authority vested in the controller’, or ‘legitimate interests’, as detailed next:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
   a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   c. processing is necessary for compliance with a legal obligation to which the controller is subject;
   d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 9 (Processing of special categories of personal data)

Article 9 of GDPR provides all the information related to the legal bases of processing of sensitive data. These are summarized in the following paragraphs. The full details are included in the official text of the regulation (GDPR).

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:
   a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, etc.;
   b. processing is 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, etc.;
   c. processing is 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;
   d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association, etc.;
   e. processing relates to personal data which are manifestly made public by the data subject;
   f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
   g. processing is necessary for reasons of substantial public interest, etc,;
   h. processing is necessary for the purposes of preventive or occupational medicine, etc.;
   i. processing is necessary for reasons of public interest in the area of public health, etc.;
   j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, etc.

Article 10 (Processing of personal data relating to criminal convictions and offences)

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11 (Processing which does not require identification)

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation, etc.

2.3. Criterion 3. Consent of DS

Articles 7 and 8 of GDPR provide all the information related to obtaining consent of data subjects and children. These are summarized in the following paragraphs. The full details are included in the official text of the regulation (GDPR).

Article 7 (Conditions for consent)

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding, etc.

Article 8 (Conditions applicable to child's consent in relation to information society services)

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child, etc.

2.4. Criterion 4. Transparency and Information Rights of DS

Articles 12 to 14 and 34 of GDPR provide all the information related to satisfying the transparency and information rights of data subjects. These are summarized in the following paragraphs. The full details are included in the official text of the regulation (GDPR).

Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means, etc.

Article 13 (Information to be provided where personal data are collected from the data subject)

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
   a. the identity and the contact details of the controller and, where applicable, of the controller's representative;
   b. the contact details of the data protection officer, where applicable;
   c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, etc.

Article 14 (Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
   a. the identity and the contact details of the controller and, where applicable, of the controller's representative;
   b. the contact details of the data protection officer, where applicable;
   c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, etc.

Article 34 (Communication of a personal data breach to the data subject)

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3), etc.

2.5. Criterion 5. Access and Other Rights of DS

Articles 15 to 23 of GDPR provide all the information related to satisfying the access and other rights of data subjects. These are summarized in the following paragraphs. The full details are included in the official text of the regulation (GDPR).

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).

9. **Article 23 (Restrictions):** Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms, etc.
   For more details, see GDPR articles 15 – 23, recitals 50, 59, 63 – 71, 73, 75, 156.

3. Minimum GDPR Compliance Evidence (CE)

The minimum compliance evidence (CE) for each criterion are noted next.

3.1. Criterion 1. Principles relating to processing of PD

CE1. Data Protection Policies and Procedures, such as: Information security policy, Data retention policy, Deletion and Retention periods for PD, Training policy, Information Security Risk Assessment (ISRA), PD Privacy Risk Assessment (PDPRA), Data Protection Impact Assessment (DPIA), Security/Privacy Controls for Processing of PD in manual and digital files and the processing of PD carried out by Third Parties, etc. For further details see GDPR articles 5, 25, 32, 33 and 35 and recitals 4, 26, 48, 78, etc.

3.2. Criterion 2. Legal basis of processing of PD

CE2. Documentation of legal basis of processing of PD in PD Inventory and other business forms and documents. For further details see GDPR articles 6 and 9 to 11 and recitals 39, 40, 51, etc.

3.3. Criterion 3. Consent of DS

CE3. Process for obtaining consent of Data Subjects. For further details see GDPR articles 7 and 8 and recitals 42, 43, 50, etc.

3.4. Criterion 4. Transparency Rights of DS

CE4. Website Privacy Notice or Website Data Protection Policy and Cookies Policy, advising DS of breaches, etc. For further details see GDPR articles 12 to 14 and 34 and recitals 13, 39, 60, etc.

3.5. Criterion 5. Access and Other Rights of DS

CE5. Policy/Procedures for satisfying Access and Other Rights of Data Subjects. For further details see GDPR articles 15 to 23 and recitals 50, 72, 73, etc.

2 GDPR GAP ANALYSIS BY BUSINESS FUNCTION AND PROCESS

Overview: This chapter contains the GDPR Gap Analysis by Business Function and Process for the example company **'XYZ Corporation' a fictitious Ship Management (Maritime) Company** on the basis of the compliance criteria of Chapter 1 and a set of Proposed New Compliance Measures to bridge the identified gaps for each business process of the company that processes PD.

1. Company Processes containing Personal Data

According to the company's PD Inventory the following processes contain personal data:

- Business Function 1: Office Personnel Administration
- Business Function 2: Finance/Accounting
- Business Function 4: Marine Operations
- Business Function 5: Technical Department
- Business Function 6: HSQE
- Business Function 7: IT

2. GDPR GAP Analysis by Business Process of PD Processing

This analysis is based on the data recorded in the Personal Data (PD) Inventory of the example company ('XYZ Corporation') which was prepared in compliance with article 30 of GDPR and on the basis of GDPR requirements. It is organized by each business process that processes personal data.

The GDPR Gap Analysis for each business process that processes PD detailed next is based on the 5 Critical GDPR Gap Analysis Criteria (described in Chapter 1) and the minimum GDPR compliance evidence for each of the 5 criteria noted therein.

2.1. Business Function 1: Office Personnel Administration

BP#1.1. Business Process (BP): Collection of Office Applicant C.V.s

Section A: PD Environment

A1. Purpose of Processing: Managing collection of C.V.s of potential employees
A2. Data Subjects: Applicants
A3. Personal Data (PD): See 'Employees' Personal Data' in Appendix 1 (Personal Data Details).
Employees' Personal Data: **A4. Storage of Personal Data**: Personnel Management System (PMS), Storage Cabinets in Personnel Office.
A5. Source of Personal Data: Applicant C.V.s via the website

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Passwords for PMS.
- There is no processing of PD by Third Parties

C2. GDPR Gaps

- There are no measures for satisfying Consent and Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- All staff share the same password. The corporate website has no SSL and the Privacy and Coolies policies are not complying with GDPR. There are no Breach Controls.
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2 and D4.1 in Appendix 2 (GDPR Compliance Measures).

2.2. Business Function 1: Office Personnel Administration

BP#1.2. Business Process (BP): Hiring of Office Employees

Section A: PD Environment

A1. Purpose of Processing: Managing the hiring of office employees
A2. Data Subjects: Employees
A3. Personal Data (PD): See 'Employees' Personal Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Personnel Management System (PMS), Storage Cabinets in Personnel Office.
A5. Source of Personal Data: Employee Agreement and related employment forms, transcripts, etc.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS.
- There is no processing of PD by Third Parties
- All staff share the same password

C2. GDPR Gaps

- There are no measures for satisfying Consent and Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2 and D4.1 in Appendix 2 (GDPR Compliance Measures).

2.3. Business Function 1: Office Personnel Administration

BP#1.3. Business Process (BP): Managing Office Employee Performance

Section A: PD Environment

A1. Purpose of Processing: Reviewing and reporting Office Employees performance
A2. Data Subjects: Employees
A3. Personal Data (PD): See 'Employees' Personal Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Personnel Management System (PMS), Storage Cabinets in Personnel Office.
A5. Source of Personal Data: Employee Performance Review report for each employee.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS.
- There is no processing of PD by Third Parties
- All staff share the same password

C2. GDPR Gaps

- There are no measures for satisfying Consent and Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- HR managers and staff are not trained on privacy issues
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2 and D4.1 in Appendix 2 (GDPR Compliance Measures).

2.4. Business Function 2: Finance/Accounting

BP#2.1. Business Process (BP): Office Employee and Crew Payroll

Section A: PD Environment

A1. Purpose of Processing: Managing the payroll of office employees and crew members
A2. Data Subjects: Employees
A3. Personal Data (PD): See 'Payroll Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Personnel Management System (PMS), Crew Management System (CMS), Financial Management System (FMS), 'ABC' External Payroll Services Company, Storage Cabinets in Personnel, Accounting. Crew and Onboard (masters') Offices.
A5. Source of Personal Data: Employee Data in PMS and CMS Systems.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS and FMS.

C2. GDPR Gaps

- There are no measures for satisfying Consent and Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- Accounting managers and staff are not trained on privacy issues
- All staff share the same password
- There is no GDPR-compliant services contract for processing of PD by External Payroll Services Company
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1, D4.2, and D5 in Appendix 2 (GDPR Compliance Measures).

2.5. Business Function 2: Finance/Accounting

BP#2.2. Business Process (BP): Managing Sickness of Office Employees and Crew members

Section A: PD Environment

A1. Purpose of Processing: Managing health documentation and issues of office employees and crew members
A2. Data Subjects: Employees and Crew members
A3. Personal Data (PD): See ‘Health Data’ in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Personnel Management System (PMS), Crew Management System (CMS), Financial Management System (FMS), ‘ABC’ External Payroll Services Company, ‘AXX’ Insurance Services Company, Storage Cabinets in Personnel and Accounting Offices.
A5. Source of Personal Data: Employee and Crew Health Data and related Medical information.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS and FMS.

C2. GDPR Gaps

- There are no measures for satisfying Consent and Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- All staff share the same password
- There is no GDPR-compliant services contract for processing of PD by 'AXX' Insurance Services Company
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1, D4.2, D5 and D6 in Appendix 2 (GDPR Compliance Measures).

2.6. Business Function 2: Finance/Accounting

BP#2.3. Business Process (BP): Managing Vendor Payments

Section A: PD Environment

A1. Purpose of Processing: Managing payments and related issues of vendors
A2. Data Subjects: Vendors
A3. Personal Data (PD): See 'Vendors' Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Financial Management System (FMS), Storage Cabinets in Accounting Offices.
A5. Source of Personal Data: Vendor Proposals, Purchase Orders and Invoices.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Contractual Obligation' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS and FMS.
- There is no processing of PD by Third Parties

C2. GDPR Gaps

- There are no measures for satisfying Consent and Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD of vendors
- All staff share the same password
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2 and D4.1 in Appendix 2 (GDPR Compliance Measures).

2.7. Business Function 2: Finance/Accounting

BP#2.4. Business Process (BP): Managing Customer Invoicing

Section A: PD Environment

A1. Purpose of Processing: Managing invoicing and related issues of customers
A2. Data Subjects: Customers
A3. Personal Data (PD): See 'Customers' Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Financial Management System (FMS), Storage Cabinets in Accounting Offices.
A5. Source of Personal Data: Customer Data and invoices.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Contractual Obligation' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for FMS.
- There is no processing of PD by Third Parties

C2. GDPR Gaps

- There are no measures for satisfying Consent and Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD of customers
- All staff share the same password
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2 and D4.1 in Appendix 2 (GDPR Compliance Measures).

2.8. Business Function 3: Crew Department

BP#3.1. Business Process (BP): Collection of Crew Applicant C.V.s

Section A: PD Environment

A1. Purpose of Processing: Managing collection of C.V.s of potential crew members
A2. Data Subjects: Crew Applicants
A3. Personal Data (PD): See 'Crew Personal Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Crew Management System (CMS), Storage Cabinets in Crew Management Office and On board vessels (Master's Office).
A5. Source of Personal Data: Crew applicant C.V.s.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Passwords for CMS.
- There is no processing of PD by Third Parties

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- All staff share the same password.
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1 and D4.2 in Appendix 2 (GDPR Compliance Measures).

2.9. Business Function 3: Crew Department

BP#3.2. Business Process (BP): Hiring of Crew

Section A: PD Environment

A1. Purpose of Processing: Managing the hiring of crew members
A2. Data Subjects: Crew members
A3. Personal Data (PD): See 'Crew Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Crew Management System (PMS), Storage Cabinets in Crew Management Office and On board vessels (Master's Office).
A5. Source of Personal Data: Crew detail C.Vs and related hiring forms and records (educational transcripts, health history, etc.).

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for CMS.
- There is no processing of PD by Third Parties
- All staff share the same password

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1 and D4.2 in Appendix 2 (GDPR Compliance Measures).

2.10. Business Function 3: Crew Department

BP#3.3. Business Process (BP): Managing Crew Performance

Section A: PD Environment

A1. Purpose of Processing: Reviewing and reporting Crew
A2. Data Subjects: Crew members
A3. Personal Data (PD): See 'Crew Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Crew Management System (CMS), Storage Cabinets in Personnel Office.
A5. Source of Personal Data: Crew Performance Review Report.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS.
- There is no processing of PD by Third Parties
- All staff share the same password

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- Crew manager, masters and staff are not trained on privacy issues
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1 and D4.2 in Appendix 2 (GDPR Compliance Measures).

2.11. Business Function 3: Crew Department

BP#3.4. Business Process (BP): Communicating with manning agents

Section A: PD Environment

A1. Purpose of Processing: Managing collection of C.V.s of potential crew members via manning agencies
A2. Data Subjects: Crew Applicants, Crew members, Manning Agencies
A3. Personal Data (PD): See 'Crew Data' in Appendix 1 (Personal Data Details). Also details of Manning Agencies (Tile of Company, Name of Contact, Address, Phone, e-mail, etc.)
A5. Source of Personal Data: Crew staffing requirements.
A4. Storage of Personal Data: Crew Management System (CMS), Storage Cabinets in Crew Management Office and In Offices of Manning Agencies.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Passwords for CMS.

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- All staff share the same password.
- There are no GDPR measures for processing of PD by Manning Agencies
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1, D4.2 and D7 in Appendix 2 (GDPR Compliance Measures).

2.12. Business Function 4: Marine Operations

BP#4.1. Business Process (BP): Communicating with Travel Agents

Section A: PD Environment

A1. Purpose of Processing: Managing communication issues with travel agents for office staff and crew members
A2. Data Subjects: Office Staff, Crew Applicants, Crew members, Travel Agents
A3. Personal Data (PD): See 'Employees' Personal Data' and 'Crew Data' in Appendix 1 (Personal Data Details). See also details of Travel Agents (Title of Company, Name of Contact, Address, Phone, e-mail, etc.)
A5. Source of Personal Data: Crew details on travelling documents.
A4. Storage of Personal Data: Storage Cabinets in Personnel Offices, Crew Management Offices, Onboard (masters') Office and in Offices of Travel Agents.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Passwords for CMS.

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- There is no GDPR measures for processing of PD by Travel Agents
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1, D4.2 and D8 in Appendix 2 (GDPR Compliance Measures).

2.13. Business Function 4: Marine Operations

BP#4.2. Business Process (BP): Communicating with Local Agents/Port Agents

Section A: PD Environment

A1. Purpose of Processing: Managing communication issues and related aspects with Local Agents/Port Agents for office staff and crew members
A2. Data Subjects: Office Staff, Crew Applicants, Crew members, Local Agents/Port Agents
A3. Personal Data (PD): See 'Employees' Personal Data' and 'Crew Data' in Appendix 1 (Personal Data Details). See also details of Local Agents/Port Agents (Tile of Company, Name of Contact, Address, Phone, e-mail, etc.)
A4. Storage of Personal Data: Storage Cabinets in Personnel Offices, Crew Management Offices, Onboard (masters') Office and in Offices of Local Agents/Port Agents.
A5. Source of Personal Data: Crew details on travelling documents.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Consent of Data Subject' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets.

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- There is no GDPR measures for processing of PD by Local Agents/Port Agents
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1, D4.2, D9, and D10 in Appendix 2 (GDPR Compliance Measures).

2.14. Business Function 4: Marine Operations

BP#4.3. Business Process (BP): Communicating with Flag Administration

Section A: PD Environment

A1. Purpose of Processing: Informing Flag Authority on Crew health and safety issues
A2. Data Subjects: Crew members
A3. Personal Data (PD): See 'Crew Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Storage Cabinets in Crew Management Offices and Onboard (masters') Office
A5. Source of Personal Data: Crew details on health and safety issues and related documents.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Legal Obligation' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets.

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1 and D4.2 in Appendix 2 (GDPR Compliance Measures).

2.15. Business Function 4: Marine Operations

BP#4.4. Business Process (BP): Communicating with Hotels

Section A: PD Environment

A1. Purpose of Processing: Managing reservation and related issues for employees and crew travelling
A2. Data Subjects: Office Employees and Crew members
A3. Personal Data (PD): See 'Employees' Personal Data' and 'Crew Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Storage Cabinets in Personnel Office, Crew Management Offices and Onboard (masters') Office
A5. Source of Personal Data: Crew and Employee details on travelling documents.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'legitimate interests of Controller' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets.

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1 and D4.2 in Appendix 2 (GDPR Compliance Measures).

2.16. Business Function 5: Technical Department

BP#5.1. Business Process (BP): Managing Vendors

Section A: PD Environment

A1. Purpose of Processing: Managing vendor data, proposals, services rendered and related issues
A2. Data Subjects: Vendors
A3. Personal Data (PD): See 'Vendors' Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Financial Management System (FMS), Vendor Management System (VMS), Storage Cabinets in Accounting and Technical Department Offices.
A5. Source of Personal Data: Vendor Proposals, Purchase Order Requirements.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Contractual Obligation' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS and FMS.
- There is no processing of PD by Third Parties

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD of vendors
- All staff share the same password
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1 and D4.2 in Appendix 2 (GDPR Compliance Measures).

2.17. Business Function 5: Technical Department

BP#5.2. Business Process (BP): Managing Vessel Inspections

Section A: PD Environment

A1. Purpose of Processing: Managing vessel inspections and related issues
A2. Data Subjects: Auditors, Inspectors, Crew Masters and members
A3. Personal Data (PD): See 'Auditors' Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Fleet and Vessels Management System (FVMS), and Storage Cabinets in Technical Department Offices and onboard (masters') office.
A5. Source of Personal Data: Inspection and Audit Reports and related documents.

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Contractual Obligation' and 'Legitimate Interests' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for FVMS.

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD of vendors
- All staff share the same password
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1 and D4.2 in Appendix 2 (GDPR Compliance Measures).

2.18. Business Function 6: HSQE

BP#6.1. Business Process (BP): Managing Health Insurance Plan

Section A: PD Environment

A1. Purpose of Processing: Managing all aspects of the provision of the Corporate Health and Medical Coverage Insurance Plan for all employees and crew members
A2. Data Subjects: All staff (employees and crew members)
A3. Personal Data (PD): See 'Employees' Personal Data' and 'Crew Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Personnel Management System (PMS), Crew Management System (PMS), 'AXX' Insurance Services Company, Storage Cabinets in HSQE, Personnel, Crew Management Offices and On board vessels (Master's Office).
A5. Source of Personal Data: Office employees and Crew detail C.Vs and related hiring forms and records (educational transcripts, health history, etc.).

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Contractual Obligation' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS and CMS.
- There processing of PD by Third Parties ('AXX' Insurance Services Company)
- All staff share the same password

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1, D4.2 and D6 in Appendix 2 (GDPR Compliance Measures).

2.19. Business Function 6: HSQE

BP#6.1. Business Process (BP): Managing Medical Incident Records

Section A: PD Environment

A1. Purpose of Processing: Managing all aspects of receiving, storing and communicating the Medical Incident Records of employees and crew members to all interested parties
A2. Data Subjects: All staff (employees and crew members)
A3. Personal Data (PD): See 'Employees' Personal Data', 'Crew Data' and 'Health Data' in Appendix 1 (Personal Data Details).
A4. Storage of Personal Data: Personnel Management System (PMS), Crew Management System (PMS), 'AXX' Insurance Services Company, Storage Cabinets in HSQE, Personnel, Crew Management Offices and On board vessels (Master's Office).
A5. Source of Personal Data: Office employees and Crew detail C.Vs and related hiring forms and records (educational transcripts, health history, etc.).

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing 'Legitimate Interests' and 'Processing necessary for legal claims' is recorded
- Some Security Controls for Processing of PD exist: Locking of Storage Cabinets and Backups and Passwords for PMS and CMS.
- There processing of PD by Third Parties ('AXX' Insurance Services Company)
- All staff share the same password

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2, D4.1, D4.2 and D6 in Appendix 2 (GDPR Compliance Measures).

2.20. Business Function 7: IT

BP#7.1. Business Process (BP): Managing ICT Systems and Infrastructure

Section A: PD Environment

A1. Purpose of Processing: Managing all aspects of receiving, processing, storing and communicating the corporate data (personal, commercial, customer, financial, etc.)
A2. Data Subjects: Employees, crew members, customers, vendors
A3. Personal Data (PD): Personal Data for Office employees and Crew members (as detailed in previous paragraphs). Personal and other data for customers and vendors (as detailed in previous paragraphs).
A4. Storage of Personal Data: Personnel Management System (PMS), Crew Management System (PMS), Vendor Management System (VMS), Customer Management System (CMS), Financial Management System (FMS). Backup media.
A5. Source of Personal Data: Office employees, Crew detail C.V.s, and related hiring forms and records (educational transcripts, health history, etc.) as well as the data collected by the information systems (PMS, FMS, CMS, VMS).

Section B: Critical GDPR Gap Analysis Criteria

Criterion 1. Principles relating to processing of PD
Criterion 2. Legal basis of processing of PD
Criterion 3. Consent of DS
Criterion 4. Transparency Rights of DS
Criterion 5. Access and Other Rights of DS

Section C: GDPR Gap Analysis

C1. Current Measures

- The Legal Basis of Processing ‘Legitimate Interests’ is recorded
- Some Security Controls for Processing of PD exist: Backups and Passwords for all systems.
- All staff share the same password

C2. GDPR Gaps

- There are no measures for satisfying Rights of Data Subjects
- There are no measures (Policy/Procedures) for Deletion and Retention Periods for PD
- An ISRA, a PDPRA and a DPIA have not been executed

Section D: Proposed New Compliance Measures

See measures D1, D2, D3.1, D3.2 and D4.1 in Appendix 2 (GDPR Compliance Measures). For Privacy Risk Analysis for the IT Applications, see Appendix 3 of this book and GDPR Tool 6 in book 2 ('GDPR Gap Tools').

APPENDIX 1: PERSONAL DATA DETAILS

These details relate to example company ('XYZ Corporation').

Employees' Personal Data: Data for applicants and employees, such as: C.V., Name, Surname, Birthdate, Home Address, Phone Numbers, E-Mail, Tax Identification Number, Bank Account Details, Job Title, Performance Data, Training Records, Educational Transcripts, Health Data, Family Details, Children, Wife, etc.

Payroll Data: Data for employees and Crew members, such as: Name, Surname, Birthdate, Home Address, Tax Identification Number, Bank Account Details, Paid Amount, Tax Levied, Pension and Social Security Deductions, etc.

Health Data: Data for employees and Crew members, such as: Name, Surname, Birthdate, Home Address, Tax Identification Number, Health and Sickness Details, Bank Account Details, Paid Amount, etc.

Crew Data: Personal details for Crew applicant and members, such as: C.V., Name, Surname, Birthdate, Home Address, Phone Numbers, E-Mail, Tax Identification Number, Seaman Documentation (Country of Birth, Travel Document, Nationality, Citizenship, Position on Board, Competency Certificate or License, Educational Transcripts, Discharge book, , Health information, etc.), Bank Account Details, Family Details, Children, Wife, etc.

Vendors' Data: Title of Company, Name and Surname of Individual, Address, Tax Identification Number, Details of Goods or Services obtained, Bank Account Details, Paid Amount, etc.

Customers' Data: Title of Company, Name and Surname of Individual, Address, Tax Identification Number, Details of Goods or Services provided, Bank Account Details, Invoiced Amount, Tax Deducted, etc.

Auditors' Data: Personal data of auditors and inspectors (Title of Company, Name and Surname of Individual, Address, Tax Identification Number, Phone number, e-mail, etc.), Results and reports of vessel audits and inspections (seafarers' employment conditions, safety and health issues, training and instruction, accident report and protective equipment, safety training for personnel, etc.)

APPENDIX 2: GDPR COMPLIANCE MEASURES

These compliance measures relate to the example company ('XYZ Corporation').

D1. Crafting and implementing a system (forms, policy, procedures, technical platform, etc.) for satisfying Consent and Rights of Data Subjects as required (employees, crew members, vendors, customers, etc.)

D2. Crafting and implementing measures (Policy/Procedures) for managing records and deletion and retention periods for PD for the data subjects, as required (employees, crew members, vendors, customers, etc.)

D3.1 Improvements required on Security/Privacy Controls for Processing of PD on the basis of an ISRA, a PDPRA and a DPIA, such as: Data Breach Controls, Password Policy, Backup Policy, IT Disaster Plan, Examination of using Encryption and Pseudonymization in all Information Systems (PMS, FMS, VMS, CMS, etc., as required), upgrading the corporate website with SSL and improving the Privacy and Cookies policies to comply with GDPR, etc.

D3.2. Register for Access to Physical Files of Storage of PD in the offices of each business function and assigning the responsibility to a manager in the specific function

D4.1 Crafting and implementing training on privacy and security issues to all central office staff (board directors, all level managers and employees)

D4.2 Crafting and implementing training on privacy and security issues to all crew staff (crew managers, masters, crew office staff, onboard crew members)

D5. Implementing a GDPR-compliant services contract for processing of PD by 'ABC' External Payroll Services Company

D6. Implementing a GDPR-compliant services contract for processing of PD by 'AXX' Insurance Services Company

D7. Crafting and implementing processor agreements with GDPR measures for processing of PD by Manning Agencies

D8. Crafting and implementing processor agreements with GDPR measures for processing of PD by Travel Agents

D9. Crafting and implementing processor agreements with GDPR measures for processing of PD by Local Agents

D10. Crafting and implementing processor agreements with GDPR measures for processing of PD by Port Agents

APPENDIX 3: IT APPLICATIONS PRIVACY ASSESSMENT

Overview

This appendix contains a summary description of the environment or personal data processing and an assessment of the privacy risks of the IT Applications of the example company **'XYZ Corporation' a fictitious Ship Management (Maritime) Company** including the current measures as well as the proposed new measures that must be undertaken to minimize the identified risks.

1. Operating Framework of Personal Data processed by 'XYZ Corporation'

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

2. IT Application Privacy Issues Assessment

2.1. Privacy Issue #01: Access to Computerized PD

1. Risk Description: Unauthorized access to personal data. Theft of Personal Data.
2. Risk Probability: Possible
3. Risk Impact Assessment: Serious
4. Risk Size: HIGH
5. **Current Compliance Measures**
   5.1. Physical Office Security Measures.
   5.2. Computer Security Measures (Password Policy).
6. **New Proposed Compliance Measures**
   6.1. Encryption.
   6.2. Pseudonymization.
   6.3. Strengthening Office Physical Security Measures.
   6.4. Enhancement of IT Security Measures (Clean Desk and Screen Policy, Intrusion Detection / Prevention System, Data Loss Prevention Technology).

2.2. Privacy Issue #02: Accuracy of Computerized PD

1. Risk Description: Multiple errors in stored computerized PD.
2. Risk Probability: Possible
3. Risk Impact Assessment: Serious
4. Risk Size: HIGH
5. **Current Compliance Measures**
   5.1. No accuracy controls during the input process.
6. **New Proposed Compliance Measures**
   6.1. Auditing the accuracy of PD with the support of the external application maintenance company and customers.
   6.2. Correcting the data errors with the support of the external application maintenance company.
   6.3. Implementing IT Application Audit Logs for all company computerized applications.
   6.4. Amend retention policy to ensure that Audit Logs are deleted when they are no longer needed.

2.3. Privacy Issue #03: Minimization of collection and use of Computerized PD

1. Risk Description: Collection and use of computerized PD that are not required.
2. Risk Probability: Possible
3. Risk Impact Assessment: Moderate
4. Risk Size: LOW
5. **Current Compliance Measures**
   5.1. No controls exist.
6. **New Proposed Compliance Measures**
   6.1. Implement controls to ensure that only the required PD are collected for the purpose initially stated by the company.
   6.2. Implement the data protection by design and default principles, such as pseudonymization, anonymization, encryption, etc.
   6.3. Implement techniques, such as: EXCLUDE, SELECT, STRIP and DESTROY to minimize the PD collected.

2.4. Privacy Issue #04: IT Application Audit

1. Risk Description: Inexistent IT Application Audit procedures.
2. Risk Probability: Possible
3. Risk Impact Assessment: Serious
4. Risk Size: HIGH
5. **Current Compliance Measures**
   5.1. No controls exist.
6. **New Proposed Compliance Measures**
   6.1. Implement IT Audits to all company computerized applications.
   6.2. Implementing IT Application Audit Logs for all company computerized applications.
   6.3. Amend retention policy to ensure that Audit Logs are deleted when they are no longer needed.

2.5. Privacy Issue #05: Network Integrity

1. Risk Description: Inexistent Network protection and integrity procedures.
2. Risk Probability: Possible
3. Risk Impact Assessment: Serious
4. Risk Size: HIGH

5. **Current Compliance Measures**
   - 5.1. No controls exist.
6. **New Proposed Compliance Measures**
   - 6.1. 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.

2.6. Privacy Issue #06: Server Storage Units Integrity

1. Risk Description: Inexistent Server Storage Units protection and integrity procedures.
2. Risk Probability: Possible
3. Risk Impact Assessment: Serious
4. Risk Size: HIGH
5. **Current Compliance Measures**
   - 5.1. No controls exist.
6. **New Proposed Compliance Measures**
   - 6.1. Improve IT Security Controls, such as: Encrypting data in storage units, etc.
   - 6.2. Install a fail-over server.
   - 6.3. Improve the Office Physical Access Controls.

2.7. Privacy Issue #07: Issues related to Data Protection by Design and Default

1. Risk Description: Inexistent Data Protection by Design and Default procedures.
2. Risk Probability: Possible
3. Risk Impact Assessment: Serious
4. Risk Size: HIGH
5. **Current Compliance Measures**
   - 5.1. No controls exist.
6. **New Proposed Compliance Measures**
   - 6.1. 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.
   - 6.2. Implement Data Protection by Design and Default measures in the design and development of the company's computerized systems.
   - 6.3. Implement software tools for data aggregation, data masking, anonymization, pseudonymization, etc.

2.8. Privacy Issue #08: Upgrading Computerized Applications Software

1. Risk Description: Inexistent effective software upgrading process for the computerized applications of the company.
2. Risk Probability: Possible
3. Risk Impact Assessment: Serious
4. Risk Size: HIGH
5. **Current Compliance Measures**
   5.1. No controls exist.
6. **New Proposed Compliance Measures**
   6.1. Upgrade the maintenance contracts of the external software services companies to ensure that upgrading of software is included in these contracts.
   6.2. Execute the backup of software and data procedure before any upgrading of the software of the computerized applications of the company.
   6.2. 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.

APPENDIX 4: MINIMUM GDPR COMPLIANCE CONTROLS

1. Information Security Policy
2. Cookies Policy
3. Web site Privacy Policy
4. Employees Privacy Policy
5. Data Retention/Removal Policy
6. Data Quality Policy
7. Backup/Recovery Policy
8. Malware Protection Policy
9. Encryption Policy
10. Pseudonymization/Anonymization/Data Agregation Policy
11. Consent Management System
12. Subject Rights Satisfaction System
13. Security Incident Management System
14. Data Breach Management System
15. Privacy Education and Training Policy
16. DPIA Methodology
17. Data Protection Audit Methodology
18. Security and Privacy Controls in Information Systems Plan
19. PD Inventory
20. IT Assets Inventory

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. **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.