Personal Data Protection Policy

Falck Group

Table of Contents

1 Purpose and Scope

1.1 Purpose

Falck depends on data and information in order to perform its business, including to collect and use certain types of Personal Data relating to Data Subjects, in order to carry out its business and provide its services. Such Data Subjects include customers, patients, delegates, employees (present, past and prospective), suppliers, associations and other business contacts.

The Personal Data gathered must be handled appropriately in accordance with all applicable laws and regulations. This policy (referred to as the "Policy" or "Personal Data Protection Policy"), together with supporting procedures, templates, standards, guidelines and checklists, aim to ensure compliance with applicable laws and regulations.

The purpose of the Personal Data Protection Policy is to protect Personal Data of customers and employees and other Data Subjects by embedding Personal Data Protection into the core of Falck's activities and by ensuring regulatory compliance with the management of all Personal Data.

1.2 Scope

This Policy applies to all affiliates of the Falck Group (hereafter referred to as "Entity/Entities") and to all practices surrounding Personal Data within the Falck Group, ranging from strategies and business processes to manual Processing as well as all information technology, such as IT systems, IT infrastructure and IT organisations (collectively referred to as "IT Services"). For the avoidance of doubt all requirements in this Policy also apply to IT Services that are hosted/housed in third-party environments.

The Policy applies to all Personal Data regardless of form, including physical archives and manual Processing of Personal Data.

The Personal Data Protection Policy is sanctioned by Falck Executive Management.

1.3 Overview

This Policy covers the following:

A. Principles and Requirements (section 3)
    - Processing Principles
    - Rights of the Data Subject
    - Documentation and Records of Processing Activities
    - Disclosure and Transfer to Third Parties
    - Data Processing Agreement
B. Data Protection Breach Notification (section 4)
C. Data Protection by Design and by Default (section 5)

D. Data Protection Risk Assessment (section 6)
E. Data Protection Impact Assessment (section 7)
F. Data Protection Audit of Data Processors (section 8)
G. Information Management (section 9)

A number of underlying procedures, standard templates and checklists have been prepared to supplement this Policy and to ensure adequate implementation across Falck.

2 Definitions

For purposes of this Policy and the supporting procedures, the terms stated below shall have the meaning set forth therein.

2.1 "Breach"

Breach means the unauthorized destruction, acquisition, access, use, loss, alteration or disclosure of all categories of Personal Data, including protected health information under the United States Health Insurance Portability and Accountability Act of 1996 (hereafter "HIPAA") and the United States Health Information Technology for Economic and Clinical Health Act (hereafter "HITECH") and business critical data covered by breach notification requirements, which compromises the security or privacy of the information.

2.2 "Breach Notification"

Breach Notification means notification to supervisory authorities, Data Controllers or Third Parties as referred to in GDPR Articles 33 and 34 and below section 4.

2.3 "Data Controller"

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, including decisions regarding the purposes for which Personal Data is processed and the way in which it is processed.

2.4 "Data Processing Agreement"

A Data Processing Agreement is a mandatory agreement required when Personal Data is processed by a Data Processor on behalf of a Data Controller and referred to in below section 3.2.5 and in the GDPR Articles 28 and 29.

2.5 "Data Processor"

A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

2.6 "Data Protection"

Data Protection encompasses the rights and obligations of individuals and organisations with respect to the collection, use, retention, disclosure, and disposal of personal information.

2.7 "Data Protection Audit" or "Audit"

As defined in GDPR Articles 28 and 32 and below section 8.

2.8 "Data Protection by Default and by Design"

As defined in the GDPR Article 25 and below section 5.

2.9 "Data Protection Impact Assessment" or "DPIA"

As defined below in section 7 in the GDPR Article 35.

2.10 "Data Protection Officer" or "DPO"

As defined in the GDPR and reference in Article 37, 38 and 39 and below section 4.

2.11 "Data Protection Risk Assessment" or "Risk Assessment"

As defined below in section 6 in the GDPR Articles 24 and 35.

2.12 "Data Subject"

Any individual/natural person who is the subject of Personal Data held and processed by Falck.

2.13 "Documentation"

As defined in section 3.2.3.

2.14 "Entity" or "Entities"

As defined in section 1.2.

2.15 "Falck" or "Falck Group"

Falck A/S and all subsidiaries and/or affiliates directly or indirectly controlled by Falck A/S.

2.16 "Falck Global Compliance Management System" or "GEMS"

The Falck Global Compliance Management System or GEMS is the IT tool where all relevant GDPR documentation is required to be stored and documented, unless otherwise agreed with the DPO.

2.17 "Falck Information Security Policy"

The Falck Corporate Information Security Policy, as amended from time to time.

2.18 "General Data Protection Regulation" or "GDPR"

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data which entered into force on 24 May 2016 and is applicable as of 25 May 2018, as amended from time to time.

2.19 "HIPAA"

As defined in section 2.1.

2.20 "HITECH"

As defined in section 2.11.2.

2.21 "IT Services"

As defined in section 1.2.

2.22 "Personal Data"

Personal Data is information relating to an individual (Data Subject) who can be identified from such information. This data includes, but are not limited to, name, date of birth, contact details (address, email address, and telephone numbers) and indirect information, such as IP address, laptop name, expressions of opinion about the individual, information concerning salary etc.

2.23 "Processing"

Any operation or set of operations which are performed upon Personal Data, whether or not by automatic means or not and relating to the collection, recording, alignment, storage and disclosure of this data.

2.24 "Sensitive Personal Data"

Sensitive Personal Data is a specific category of Personal Data and covers Personal Data of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health information, sexual preference and offences and criminal convictions. In certain countries also social security number, depending on national legislation.

2.25 "Third Country"

A Third Country is a country that is not a member of the European Union and that has not entered into an agreement with the European Union which contains rules corresponding to Directive 95/46/EEC of 24 October 1995 on the protection of physical persons in connection with the processing of personal data and on the free exchange of such data – i.e. the European Economic Area (EEA) countries.

2.26 "Third Party"

Any individual/organisation other than the Data Subject, the Data Controller (Falck) or its Data Processors.

3 Principles and Requirements

3.1 Objective and Scope

The GDPR stipulates the main responsibilities with respect to Personal Data Protection, including the principles for Processing. These principles, duties and responsibilities that Falck needs to comply with are outlined further below.

The principles for Processing are referenced throughout the GDPR primarily in Chapters I, II, III and V.

3.2 Policy

The purpose of this section is to establish how these principles for Processing and associated duties and responsibilities must be implemented across the Entities.

The Entities must be able to document compliance with the requirements by storing applicable documentation in GEMS.

3.2.1 Processing Principles

Falck fully supports and complies with the basic principles of the GDPR which are summarised below:

- Personal data shall be processed and **lawfully**, **fairly** and **transparently**
- Personal data shall only be obtained/processed for specific lawful **purposes** (purpose limitation)
- Personal data held must be **adequate**, relevant and not excessive (data minimisation)
- Personal data must be **accurate** and kept up to date
- Personal data shall not be kept for longer than necessary (storage limitation)
- Personal data shall be processed in accordance with **rights** of Data Subjects.
- Personal data must be kept secure
- Personal Data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection and e.g based on EU Model Contract Clauses

The processing principles are described in a number of articles throughout the GPDR, primarily in Articles 5, 6 and 9.

Supporting procedures, templates and guidelines will describe in further detail, how the above principles are adequately and efficiently implemented throughout the Entities. The supporting procedures, templates and guidelines is listed in Appendix A.

3.2.2 Rights of the Data Subject

Personal data is processed by Falck in accordance with the rights of Data Subjects under the GDPR and applicable legislation. Data Subjects have under the GDPR the following rights:

- Right to receive information whether any Personal Data is being processed and certain additional information in this respect (also referred to as privacy notice);

- Right of access to a copy of the information comprised in their Personal Data. A Data Subject who makes a written request is entitled to be:
    - Told whether any Personal Data is being processed;
    - Given a description of the Personal Data, the reasons it is being processed and whether it will be given to any other organisations or people;
    - Given a copy of the information comprising the data; and given details of the sources of data (where this is available).

- A right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right to have inaccurate Personal Data rectified, and under certain circumstances blocked, erased or destroyed;
- A right to claim compensation for damages caused by a breach of the Act.

Rights of the Data Subject are referenced throughout the GDPR, primarily in Articles 12-22.

3.2.3 Documentation and Records of Processing Activities

The GDPR stipulates a requirement to maintain records of the Processing activities, covering areas such as Processing purposes, data sharing and retention. The records of Processing activities and supplementing documentation is jointly referred to as the Documentation. This Documentation will support good data governance and ensure that each Entity can demonstrate compliance with all aspects of the GDPR. Such Documentation must be stored in GEMS.

The Documentation requirements are referenced throughout the GDPR, and in particular in Article 30.

3.2.4 Disclosure and Transfer to Third Countries

Falck will not disclose Personal Data to unauthorised Third Parties, this means that Falck will not disclose Personal Data to Third Parties except to relevant statutory bodies as per mandatory law and regulation or based on another legal basis, e.g. consent. All employees are asked to exercise caution when requested to disclose Personal Data to a Third Party.

Falck will only transfer data to third countries as per the requirements of the GDPR including with adequate contractual commitment and with sufficient security measures.

Disclosure to Third Parties and transfer to third countries are referenced throughout the GDPR, primarily in Chapter V.

3.2.5 Data Processing Agreements

When Personal Data is processed by a Data Processor on behalf of a Data Controller, Data Processing Agreement is required, and Data Processing Agreements must be entered into for all Processings where Falck is acting as Data Processor or has engaged a Data Processor to process Personal Data on Falck's behalf.

Supporting standard templates, listed in Appendix A, have been prepared and such templates should be used when possible and as described in the guidance.

Data Processing Agreement is referenced throughout the GPDR, the main provisions are Articles 28 and 29.

4 Data Protection Breach Notification

4.1 Objective and Scope

The purpose of this section is to establish the requirements for Breach Notification by Falck to parties outside the Falck Group in order to enable the Entities to comply with applicable law.

Breach Notification is referenced throughout the GPDR, the main provisions are Articles 33 and 34.

4.2 Policy

Following the discovery of a potential Breach, the affected Entity must begin an investigation.

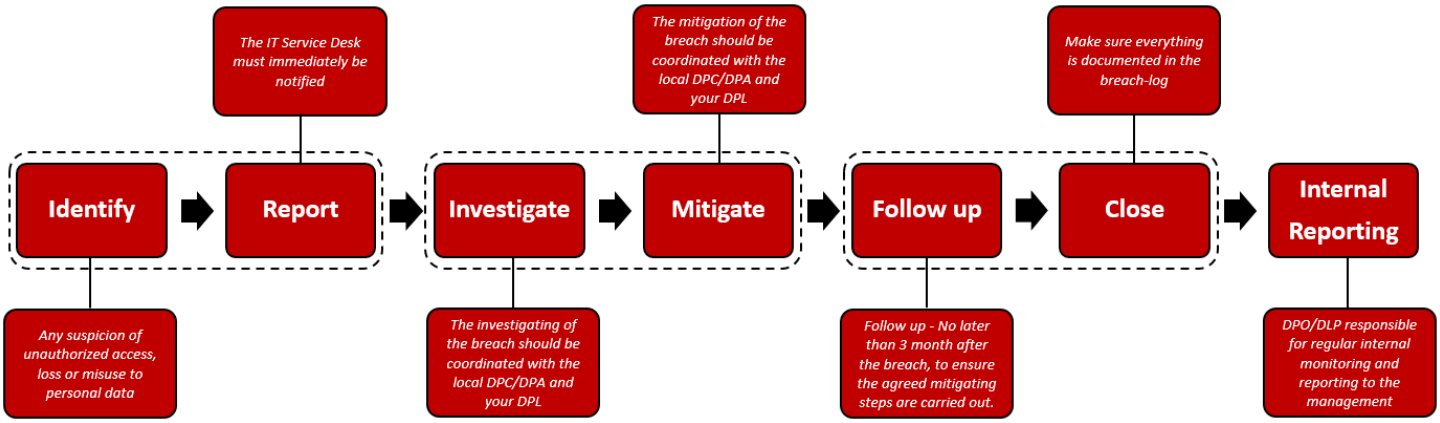
If the investigation determines that Personal Data has been accessed, acquired, used, altered or disclosed as a result of the Breach the Entity must immediately notify the IT Service Desk and the relevant Data Protection Lead in order to determine the specific notification requirements which are further described in related procedure(s). Such procedures are listed in Appendix A.

As per the requirements of the GDPR, a Breach Notification to the supervisory Data Protection authorities must be able to take place by the Data Controller without undue delay and where feasible, no later than 72 hours after becoming aware of the breach, as directed by the DPO. If the deadline is exceeded, the notification must include the reasons for the delay. Breach Notification can be provided by the DPO in phases if necessary. A notification to the affected individuals may also be required.

If the Entity is acting as Data Processor, the Data Controller must be notified without undue delay, as directed by the DPO.

Breach Notification may also be a requirement under other applicable legislation.

Please see overview of Breach Notification process below:



5 Data Protection by Design and by Default

5.1 Objective and Scope

Data Protection by Design and by Default is the GDPR requirements for implementing appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed in alignment with GDPR through, eg. active data minimisation, pseudonymisation and other controls to improve security and Data Protection, as also described in the Falck Information Security Policy.

5.2 Policy

The purpose of this section regarding Data Protection by Design and by Default is to establish how is must be implemented in Falck. Use of the Data Protection by Design and by Default principles is mandatory for all Entities, but actual measures must be based on a Data Protection Risk Assessment.

The Entities must be able to demonstrate and document compliance with this Policy and the related procedures listed in Appendix A as well as applicable legal requirements. Such documentation must be stored in GEMS.

6 Data Protection Risk Assessment

6.1 Objective and Scope

The purpose of this section is to establish the requirements for GDPR Data Protection Risk Assessments in the Entities covered by the GDPR during the Data Protection lifecycle.

Risk Assessment is referenced throughout the GPDR, the main sections outlining the requirements are Articles 24 and 32.

6.2 Policy

Falck products, services and applications that are processing Personal Data must be protected by appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are in fact processed. In order to ensure the appropriate level of technical and organisational measures, a Data Protection Risk Assessment needs to be prepared. To complete a Data Protection Risk Assessment the likelihood and the severity of a negative impact associated with the Processing should initially be evaluated. Thereafter, the nature, scope, context and purpose of the Processing needs to be analysed to assess the vulnerabilities of the IT Systems and operations as well as the nature of the threats.

The supporting and underlying Data Protection Risk Assessment procedure must be used to identify and assess the potential risks in new processes, new solutions, new providers, partners, customers, etc. and must be used in case of high risk Processings before selecting new suppliers and Data Processors, as part of Data Protection Impact Assessments, cf. section 7, and as part of the Data Protection lifecycle.

7 Data Protection Impact Assessment

7.1 Objective and Scope

The purpose of this section is to establish the requirements for GDPR Data Protection Impact Assessment in the Entities as required by the GDPR.

Data Protection Impact Assessment is referenced throughout the GPDR, the main articles are Articles 35 and 36**.**

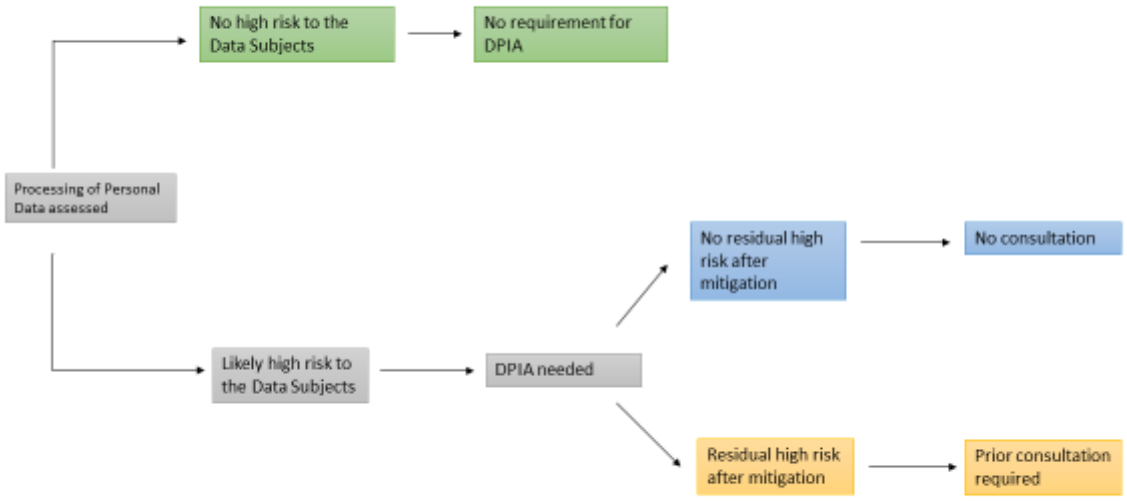
7.2 Policy

DPIA is the GDPR requirements for a process designed to describe the Processing, assess the necessity and proportionality of a Processing and to enable managing the risks to the rights and freedoms of the Data Subjects. A DPIA must be carried out in the Entities when the Processing is likely to result in a high risk to the rights and freedoms of individuals.

The DPIA will identify the most effective way to comply with the Data Protection obligations and ensure that the appropriate level of Data Protection for the Data Subjects' is implemented.

The supporting and underlying DPIA procedure must be used to identify and assess the high-risk Processing.

Please see overview of DPIA process below:



8 Data Protection Audit of Data Processors

8.1 Objective and Scope

The purpose of this section is to establish the requirements for Data Protection Audit of Data Processors in the Entities covered by the GDPR.

Audit is referenced throughout the GPDR, the main sections outlining the requirements are Articles 28 and 32**.**

8.2 Policy

A Data Protection Audit focuses on verifying the Data Processors compliance with the GDPR requirements and the requirements in the Data Processing Agreement. The Audit must take place within a defined scope and in a systematic and documented method, as described in the supporting procedure cf. Appendix A, to obtain and maintain relevant Audit documentation and to evaluate and assess to which extent the Audit criteria are fulfilled.
If it is disclosed, e.g. through an Audit, that a Data Processor is non-compliant with the Data Protection obligations, necessary and appropriate actions must be initiated to ensure compliance.

Relevant Audit documentation must be stored in GEMS.

9 Information Management

9.1 Objective and Scope

The purpose of this section is to establish the requirements for information management in order to enable the Entities to comply with applicable law.

Provisions regarding requirements for information management is referenced throughout the GPDR, primarily in Article 5.

9.2 Policy

It is a requirement of the GDPR that Personal Data shall only be retained for as long as there is a purpose and appropriate technical measures in place. In order to achieve and maintain compliance with the GDPR, an underlying information management procedure has been prepared and implemented across Falck. This procedure outlines the main rules for storage, retention and deletion of e-mails and documents which contain Personal Data.

10 Enforcement

An employee found to have violated this Policy may be subject to disciplinary action, including but not limited to termination of employment.

A violation of this Policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the Falck Group and/or other legal measures.

Revision History

Ver.	Date	Author	Comments	Status
1.0	30.01.2018	Birgitte Poulsen	New Policy	Approved by THI
1.1	10.10.2018	Christian Texel Svendsen	Update of Appendix A	Approved by BIPO
1.2	09.05.2018	Christian Texel Svendsen	Updated after Revi-IT audit	Approved by CW

Personal Data Protection Policy – Appendix A

Supporting Procedures, Templates, Checklists, Guidelines etc.

1 Procedures

The following procedures have been prepared supporting and implementing the Personal Data Protection Policy:

1.1 Data Protection Breach Notification procedure (referred to as “Data Protection Breach Notification Procedure”)

1.2 Data Protection Risk Assessment procedure (referred to as “Data Protection Risk Assessment Procedure”)

1.3 Data Protection Impact Assessment procedure (referred to as “Data Protection Impact Assessment Procedure” or “DPIA Procedure”)

1.4 Data Protection Audit of Data Processors procedure (referred to as “Data Protection Audit of Data Processors Procedure”)

1.5 Data Subject Rights Procedure (referred to as “Data Subject Rights Procedure)

1.6 Information Management Procedure for Personal Data Protection (referred to as ”Information Management Procedure for Personal Data Protection”)

2 Templates

The following templates have been prepared supporting and implementing the Personal Data Protection Policy:

2.1 Template Data Processing Agreement – Falck as Data Processor

2.2 Template Data Processing Agreement – Falck as Data Controller

2.3 Template Data Processing Agreement – short version

2.4 Checklist and template - Consent

2.5 Template – Confidentiality Agreement

2.6 Template and checklist – Privacy Information Notice

3 Checklists, guidelines, forms etc.

The following checklists and guidelines have been prepared supporting and implementing the Personal Data Protection Policy:

3.1 Checklist – Collection, use and disclosure

3.2 Checklist – Data Processor Agreement

3.3 Checklist – Individual rights

3.4 Deletion/retention guideline