Danish Crown

Group Data Protection Compliance Policy

September 2024 – Version 2.0

Document Control

Governance	
Version	2.0
Issuer	Lise Lotte Langston (LILOL)
Approver	Thomas Ahle (TAH)
Issuing date	26-09-2024
Application date	26-09-2024
Scope	Danish Crown Group
Review frequency	Every 2 years

Version history			
Vs.	Date	Modified by	Summary of changes and updates
1.0	01.01.2018	Rasmus Schjoldager	Implementation of policy
1.1	01-01-2021	Jesper Green Schou (JEGSC)	Update for improved communication.
1.2	01-02-2022	Jonas Hvid (JONHV)	Updated In connection with the implementation of standards and other guidelines / SOPs
1.3	02-05-2023	Jonas Hvid (JONHV)	Update of issuer and approver
2.0	26-09-2024	Jonas Hvid (JONHV)	General update of policy

Link to related group documents	
Document file name	Document content
GDPR Guideline	GDPR Guideline for all employees
GDPR Guideline HR	GDPR Guideline for HR employees
GDPR Guideline managers	GDPR Guideline for managers
SOP Conclusion of DPA	Procedure for entering into agreements with data processors.
GDPR Guideline use of photos and statements	Guideline for marketing and HR personnel who uses pictures internally and online
SOP How to exercise data subject rights	Procedure to exercise data subject rights
SOP Audit data processors	Procedure to ensure audit on data processors
SOP Transfer of personal data to countries outside EU/EEA	Procedure for entering into agreements with data processors outside EU/EEA
SOP Yearly GDPR documentation review	Procedure to ensure an annual update of GDPR documentation
Information Security Policy	Policy for all employees outlining requirements for the protection of information
IT Security Guideline	Guideline for all employees outlining requirements for working with IT equipment

Content

1. Our policy

1.1 Our commitment

The management of Danish Crown is strongly committed to ensure the Group's compliance with the data protection legislation in force. This commitment is part of our general commitment as a responsible Group to act with integrity and to satisfy the requirements of the laws in force in the countries in which we operate.

Our commitment to protect personal data is a shared responsibility and each of us is required to understand our joint responsibility to conduct our business in a way that is consistent with our values and in accordance with this policy.

1.2 Our culture

In Danish Crown, we support a compliance culture and provide the necessary guidance and mandatory training to all relevant employees. In this way, we ensure that all relevant employees have a strong awareness of the rules and ability to comply with the guidance provided.

We actively promote a culture where "playing by the rules is business as usual" and we urge employees to raise potential compliance issues openly.

1.3 Our duties to promote compliance

An infringement of national and/or EU General Data Protection Regulation could have serious consequences for Danish Crown and the individual who suffers from a data breach or wrongful processing of his/her personal data. Accordingly, each employee must be aware of the following obligations:

A) All employees are expected to contribute actively to complying with the data protection legislation rules in force;

B) No employee should assume that Danish Crown's interests ever require anything other than compliance with the rules;

C) No-one has authority to give orders or directions that would result in a violation of the rules;

D) Each employee is obliged to seek advice and guidance from his/her immediate manager and/ or the Group General Counsel if in doubt; and.

E) Any violation or suspected violation must be reported to the Group General Counsel. It is also possible to report a concern in the Danish Crown Whistleblower Scheme.

1.4 Globally consistent high standards

This policy is applicable in all jurisdictions in which we operate. Our policy reflects the need for globally consistent and high standards to demonstrate our commitment to conduct our business in a way that is consistent with our values, regardless of the jurisdiction. We acknowledge that there may be potential differences in local legislation, affecting our local operations, and the Group General Counsel will provide further advice and instructions as required.

2. Protection of personal data

2.1 What is personal data?

Personal data means any information which can be related to an identified or identifiable physical person ("Data Subject").

Personal data must be processed in accordance with the General Data Protection Regulation ("GDPR").

Personal data is divided into three categories ordinary personal data, sensitive personal data and confidential personal data:

Ordinary personal data includes all personal data that is not classified as sensitive personal data or confidential personal data.

Sensitive personal data is information classified by law as sensitives, such as personal information on health, trade union affiliation, racial and ethnic origin, sexual and political beliefs and biometric data.

Confidential personal data is information that is classified as ordinary, but the general opinion of society would deem it inappropriate if data is not adequately secured. Confidential personal data can be social security number, passport, financial income, criminal records etc.

2.2 Processing of personal data

Processing of personal data is basically everything you can do with personal data, both automated processing and manual handling, such as collection, structuring, storing, disclosure, making available, erasure and destruction.

Processing of all personal data must:

- be in accordance with Data Protection Principles described below in section 2.2.1;
- have a Legal Basis as defined in the data protection legislation described below in sections 2.2.2 and 2.2.3; and
- be in accordance with the GDPR guideline for all employees.

2.2.1 Data Protection Principles

The data protection principles applicable under the data protection legislation stipulate that personal data must be:

- **Principle 1:** Personal data must be processed lawfully, fairly and transparently, by ensuring a privacy notice is given to the Data Subject;
- **Principle 2:** Personal data must be processed only for a specific, explicit, and legitimate purpose;
- **Principle 3:** Personal data, that is processed for a purpose, must be adequate and relevant for the purpose for which it is processed. Excessive data should not be processed;
- **Principle 4:** Personal data processed must be kept accurate and up-to-date;
- **Principle 5:** Personal data that is processed must be deleted when data is no longer needed; and
- **Principle 6:** Personal data that is stored or transferred must be kept secure using appropriate technical and organisational measures.

2.2.2 Legal Basis for processing of ordinary and confidential personal data

Besides the fulfilment of the Data Processing Principles (section 2.2.1) any processing must have a legal basis ("Legal Basis"). The necessary Legal Basis can be obtained, if processing of personal data is:

- based on the Data Subject´s consent;
- necessary for the performance of a contract;
- necessary for complying with a legal obligation; or
- necessary for the purpose of a legitimate interest provided such processing is not considered to be harmful towards the Data Subject.

2.2.3 Legal Basis for processing of sensitive personal data

It is generally forbidden to process sensitive personal data in Danish Crown, however, there are some cases where it is necessary to process sensitive personal data

e.g., in relation to health and safety and HR. In these cases, it must be considered if processing of sensitive personal data is:

- based on the Data Subject´s consent; or
- necessary for adherence to employment, social security or social protection rules and regulations.

2.3 GDPR guidelines

In order to comply with the data protection legislation a number of practical guidelines have been developed.

The guidelines are an integral part of this Group Data Protection Compliance Policy and provided to all relevant employees as part of the mandatory training conducted under our Data Protection Compliance Programme.

Further information and the guidelines on the GDPR can be found on the Danish Crown´s data protection intranet page, which can be found here: *Link*

2.4 Suppliers that process personal data on our behalf

In order to comply with the data protection legislation a number of practical guidelines have been developed.

Danish Crown is responsible for safeguarding the personal data of its Data Subjects. This also applies when a supplier processes our data.

In order to comply with the GDPR, it is mandatory to ensure that a data processing agreement is in place with a supplier whose main service is to process personal data on behalf of Danish Crown.

Danish Crown may be subject to severe fines and sanctions if Danish Crown does not put in place adequate security measures for data protection including data processing agreements. More guidance can be found in the GDPR guideline found here: *Link*

2.5 IT security

Danish Crown's employees are required to adhere to Danish Crown's IT Security Guideline, which describes the technical and organisational security measures that every employee must know and observe. The IT Security Guideline can be found on the Danish Crown's data protection intranet page, which can be found here: *Link*

2.6 Data security breach

Danish Crown has established a process to be followed by all employees in the event of a breach of security. A data security breach can be defined as an incident which may compromise the confidentiality, integrity or availability of a Data Subjects personal data or Danish Crown's IT infrastructure where personal data is processed.

Examples of breaches of security:

- An email containing confidential or sensitive personal data is sent to one or more wrong recipients (both internally and externally).
- An email with confidential or sensitive personal data is displayed while sharing screen during online meetings.
- A laptop is stolen or forgotten / left unattended.
- Physical documents containing confidential or sensitive personal data are lost/mislaid.
- Cyber security attacks involving personal data.
- A document including confidential or sensitive personal data was inadequately masked/concealed.

In the event of a breach of security, such breach must be reported as soon as possible via IT Service Desk. Danish Crown's IT Department will subsequently help contain the damage and assess whether the breach is to be reported to the authorities.

Click here to report a breach of security: *Link*

Danish Crown is under obligation to assess whether a breach must be reported to the relevant authority no later than 72 hours after Danish Crown becomes aware of the breach.

2.7 How to seek further advice

In Danish Crown we recognize that an open and honest dialogue is a precondition to maintain and continuously strengthen our integrity.

As an employee in Danish Crown, it is your right and responsibility to obtain guidance regarding any business decision you are uncertain about. The first point of contact in relation to GDPR matter for guidance should be to reach out to *GDPR@danishcrown.com*