Danish Crown

Group Data Protection Compliance Policy

May 2023 – Version 4.0

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

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.

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.

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 can be divided into two overall groups: sensitive personal data and ordinary personal data.

Sensitive personal data is information on e.g. health, sexual orientation, religious belief, political view or trade union membership.

Ordinary personal data is information on e.g. name, address, performance measures and information on bank accounts.

2.2 Processing of sensitive 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.

2.3 Processing of ordinary personal data

Processing of ordinary personal data must:

- be in accordance with certain "data protection principles" defined in the data protection legislation. The data protection principles are described below in section 2.3.1.
- have a "legal basis" as defined in the data protection legislation. The constitution of a legal basis is described below in section 2.3.2.

2.3.1 Data protection principles

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

- **Principle 1:** Processed lawfully, fairly and transparently
- **Principle 2:** Processed only for a specific, explicit and legitimate purpose
- **Principle 3:** Adequate, relevant and not excessive
- **Principle 4:** Kept accurate and up to date
- **Principle 5:** Not kept for longer than necessary
- **Principle 6:** Kept secure
- **Principle 7:** Transferred or disclosed with anadequate level of protection

2.3.2 Legal basis for processing of personal data

Besides the fulfilment of the above-mentioned data processing principles (section 2.3.1) any processing must have a so-called legal basis. The necessary legalbasis can be obtained if processing of personal data is either:

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

2.4 Data protection guidelines

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

The Guidelines are an integral partof 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.

2.5 – IT security and breach of security

Danish Crown's employees are required to read Danish Crown's Information Security Policy, which describes the technical and organisational security measures that each individual employee must know and observe.

Danish Crown has established a process to be followed by all employees in the event of a breach of security. A breach of security can be defined as an incident which may compromise an individual person's data or Danish Crown's IT infrastructure.

Examples of breaches of security:

- Personal data are transferred to the wrong external recipient
- Physical documents containing personal data have been lost
- A phishing email is clicked (this is an email intended to lure a person to click a link to obtain information)
- Unapproved third-party software is used
- There are signs that a person's computer has been compromised by a virus or the like

Danish Crown is under obligation to assess whether a breach must be reported to the authorities within a period not exceeding 72 hours from the time when Danish Crown becomes aware of the breach.

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.