DATA ETHICS POLICY

SDC A/S

FEBRUARY 2024

CONTENT

1 Introduction

Data has great value and has great potential to influence strategic and commercial decisions for companies in the financial sector. An essential element of SDC's strategy is to enable our customers to create increased growth and business value based on their data.

SDC has an important role as an IT supplier to financial companies in the Nordic countries and processes large amounts of data on behalf of our customers. It is therefore of paramount importance to SDC that we process data correctly, securely and in an ethically responsible manner in all respects.

SDC takes its responsibility as a data processor seriously. We want to be perceived as a respected, competent and conscientious partner who complies with the legislation in force at any time and observes the development of proper data behavior and ethics. This policy aims to contribute to this.

SDC's processing of data extends beyond GDPR, as SDC as a full-service IT supplier collects and stores a lot of valuable data on behalf of our customers. Data ethics is therefore relevant to SDC's processing and use of all types of data and goes beyond compliance with legislation regarding the protection of personal data.

SDC's data ethics policy applies to all of SDC, including SDC's branch in Poland.

This policy shall be applied in accordance with and as part of SDC's IT Security Policy, SDC's Privacy Policy, SDC's Outsourcing Policy and SDC's IT Risk Management Policy.

2 SDC's use of data

SDC processes large amounts of data on behalf of our customers. This involves both personal data and other types of data belonging to our customers. We process our customers' data securely and confidentially and in accordance with the agreed requirements and standards, including requirements for processing personal and financial data.

Therefore, SDC has implemented a wide range of technical and organizational measures to demonstrate an appropriately high and adequate level of data protection. Privacy and data protection are key elements in maintaining the trust of SDC's customers, employees and partners. SDC ensures that our customers can add their data in SDC's systems with data from other partners and from their own systems as needed. Data from this helps qualify our customers' business management and customer-oriented activities.

Any processing of data must take place in compliance with the requirements of SDC's IT Security Policy. The purpose of this is to ensure that there is effective control of access for employees and external users to SDC's premises, facilities and data, as well as prevent

and/or reduce the disadvantages of malfunctions and ensure data and information confidentiality based on the concepts of Confidentiality, Integrity and Availability.

Through compliance with the IT Security Policy, SDC ensures that both customer data and SDC's own data are correct, consistent and complete.

SDC has implemented processes and systems for access management, which ensures that access to data in SDC is based on a work-related need.

Both during and after employment with SDC, SDC's employees are obliged to observe an unconditional duty of confidentiality with regard to information about SDC's internal conditions, systems and customers. This is specified in the individual's employment contract as well as in SDC's Personal Data Policy for employees.

SDC does not collect data for its own independent needs or purposes, e.g. profiling of individuals. Thus, this is not part of the current business strategy or current business activities.

SDC processes our customers' data solely for the purpose of providing the agreed services to our customers.

3 Governance in the organization

SDC's management is responsible for ensuring that every business area in SDC takes into consideration reliable and correct use of data in the development and maintenance of systems and processes. System ownership is uniquely located in the organization. SDC's organizational structure is de-centralized, corresponding to the division of responsibilities, and ensures effective internal control, reporting and follow-up.

Activities to ensure sound use of data are part of the daily work routines, so that the desired level can be achieved with the fewest possible administrative and organizational resources, as well as with a focus on avoiding challenges in relation to key persons, etc.

The daily work with data ethics takes place in SDC's individual business areas. Relevant internal processes and guidelines for documentation and handling of data, including personal data, are continuously implemented and reviewed. Furthermore, SDC has a large number of underlying policies, processes and guidelines on the use of personal data, etc., which are continuously reviewed or updated as needed. They are all part of the organizational steps to ensure that appropriate measures are taken and to document the requirement for accountability under GDPR and IT security.

All internal policies, processes and guidelines are available to all employees on SDC's intranet. There is ongoing education and security training of all employees, including onboarding of new employees and consultants.

4 Cooperation with suppliers

SDC imposes a number of requirements on its suppliers. Several of these requirements originate from the legislation and regulation that the financial sector is subject to, including requirements for financial companies' outsourcing. Other requirements originate from SDC's customers.

Among other things, SDC's outsourcing policy stipulates that there must be a prior investigation (due diligence) of all outsourcing suppliers. In addition, SDC imposes a wide range of contractual requirements of a data protection and outsourcing-related nature.

SDC monitors its suppliers. This is implemented widely across SDC's organization with associated processes and ownership. There is a special focus on monitoring in relation to GDPR and outsourcing.

5 Use of new technologies

SDC has established both internal and external boards, which are involved in decisions on the application of new technology. These boards also advise other departments in SDC on cross-cutting issues of IT architecture.

The IT Security Manager is responsible for the security aspect of data protection in SDC. The task is to ensure an appropriate technical and organizational level of security measures in SDC, and to assist the business with ongoing sparring on appropriate technical and organizational security measures.

SDC's DPO must be involved if the use of new technologies results in the processing of personal data.

SDC updates its policies continuously and adds guidelines when new technology so requires. In 2023, SDC has added a guideline for using Public AI engines.

SDC's customers, as data controllers, must carry out an analysis of the consequences of the intended processing activities for the protection of personal data, i.e. an impact assessment, before initiating a new processing of data that may involve a high risk to the rights and freedoms of natural persons As data processor, SDC assists our customers in ensuring compliance with the obligations in relation to conducting impact assessments, and SDC provides the agreed contributions, taking into account the nature of the processing and the information available to SDC.

6 Maintenance

This Data Ethics Policy has been updated on 1 February 2024 and has been approved by SDC's Executive Board.

Legal & Compliance reviews the guidelines at least once a year and provides the necessary adjustments with involvement of relevant areas in SDC's organization. Updates are submitted to the Executive Board for approval.