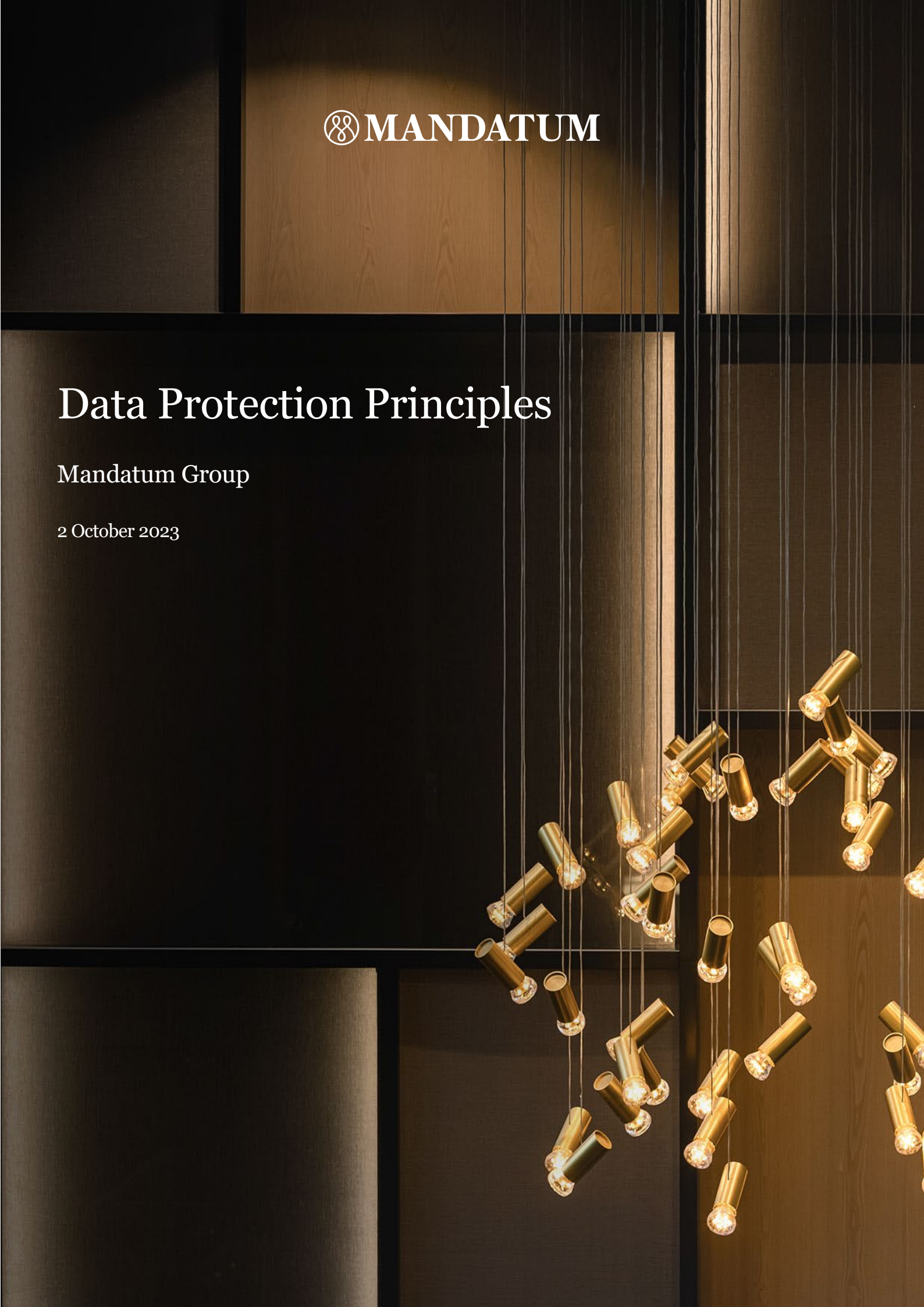
MANDATUM

Data Protection Principles

Mandatum Group

2 October 2023



Contents

1 INTRODUCTION

1.1 Background and Purpose

Processing of personal data is a necessary part of providing financial services. As an inseparable part of personal data processing is data protection – the measures to protect the personal data and to safeguard the rights and freedoms of data subjects when personal data is processed.

The purpose of these Data Protection Principles (the "**Principles**") is to set forth the key rules and principles concerning data protection at Mandatum Group. Mandatum Group is committed to protecting individuals' rights and to keeping their personal data safe while it is processed by a Mandatum Group company. When processing data, Mandatum Group companies are to ensure a high level of data protection by operating in compliance with all applicable regulations, laws and rules regarding data protection and privacy.

The key regulatory requirements stem from the Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, the "**GDPR**"), and the national data protection laws specifying and supplementing the GDPR and its national application. In addition to this, there are several provisions in the sectoral legislation regulating the financial industry and therefore applicable to Mandatum Group companies, which are to be complied with when conducting the Group companies' business activities.

1.2 Scope

These Principles apply to all Mandatum Group companies. Mandatum Group companies are committed to implementing the principles laid down in this document and in the regulation on data protection, as further elaborated below.

2 DATA PROTECTION PRINCIPLES

Mandatum Group shall comply with the principles of processing personal data set forth below in all its operations and ensure that it is also able to demonstrate compliance with the said principles and applicable data protection legislation.

Lawfulness, fairness and transparency

Mandatum Group is committed to processing personal data in a lawful, fair and transparent manner in relation to the data subject. Personal data is processed in compliance with the GDPR and other applicable legislation, and the processing is communicated to the data subjects clearly and in an intelligible manner. Mandatum Group companies are committed to processing the personal data appropriately and fairly with regard to the purposes of the processing.

In order to transparently provide information on the processing of personal data by the Mandatum Group companies, a privacy notice has been published and is available at all times via Mandatum Group's public website. Further information is also provided when using Mandatum Group companies' services.

Purpose limitation

Mandatum Group companies collect personal data only for specified, explicit and predefined legitimate purposes that are deemed necessary for the business of the Group company in

question. The collected personal data shall not be further processed in a manner that is incompatible with those purposes.

Data minimisation

Mandatum Group companies shall not process other personal data than what is adequate, relevant and limited to necessary in relation to the purposes for which they are processed.

Accuracy

Mandatum Group companies shall take all reasonable measures to ensure that personal data processed is accurate and kept up to date and that data inaccurate for the processing purposes are erased or rectified without delay.

Storage limitation

Mandatum Group companies are to ensure that the personal data are kept in a form which permits identification of data subjects for no longer than what is necessary for the purposes of the processing. Personal data are stored in accordance with predefined rules and criteria for retention, after which they are erased or anonymised.

Integrity and confidentiality

Mandatum Group companies have set in place wide technical and organisational measures to always ensure the appropriate security and confidentiality of personal data. Mandatum Group companies are committed to secure the personal data from unauthorised or unlawful processing, accidental loss, destruction or damage.

Furthermore, in accordance with the key integrative principles of Data Protection by Design and by Default, Mandatum Group companies consider the issues of data protection and privacy at the design of any system, service, product or process, and throughout the whole lifecycle of it, and ensures that only such data that is necessary to achieve a specific purpose is being processed. Mandatum Group companies are to put in place appropriate technical and organisational measures designed to implement the previously mentioned core principles effectively and to integrate necessary safeguards to meet the GDPR requirements and to protect the data subjects' rights and freedoms.

Further principles on information security, which are followed by Mandatum Group companies to ensure the confidentiality, integrity and availability of systems, services and data, are defined in Mandatum Group's Information Security Policy.

3 PROCESSING OF PERSONAL DATA

All Mandatum Group companies have established internal policies, guidelines, procedures and controls tailored to their business profile to ensure compliance with all applicable obligations and requirements regarding the protection of personal data.

In accordance with the regulatory requirements and the risk-based approach stemming from the GDPR, Mandatum Group companies shall carefully assess the risks that their processing of personal data may cause to data subjects and determine the likelihood and severity of the risks to the rights and freedoms of the data subject by reference to the nature, scope, context and purposes of the processing. The extent of the internal technical and organisational measures necessary to protect the individual rights is adapted to the risk concerned.

Mandatum Group companies shall not disclose personal data to third parties without a valid legal basis pursuant to the GDPR. Processing activities may only be outsourced to external

data processors providing sufficient guarantees to implement technical and organisational measures to ensure that all personal data are processed in compliance with data protection legislation and Mandatum Group's internal policies. Processing by a data processor shall be governed by a written data processing agreement, which is binding on the processor with regard to the Mandatum Group company concerned and sets forth the terms and conditions for all processing activities.

Should personal data be transferred outside the EU/EEA, the transfer is to be done in accordance with the applicable regulation and ensuring that the level of the protection guaranteed for personal data by the GDPR is not compromised.

Detailed information on the processing activities conducted by the Mandatum Group companies is provided in Mandatum Group's privacy notice available on the Group website.

4 DATA SUBJECT RIGHTS

Data protection regulation provides the data subjects with several data protection rights in relation to personal data processed about them, such as the right to obtain information on the processing, the right of access and the right to rectification.

Mandatum Group companies are committed to facilitate the exercise of the data subject rights. When Mandatum Group companies process personal data, they take appropriate measures to ensure that the data protection rights of data subjects are fulfilled. Further guidance for the data subjects on how to exercise their rights is provided e.g., in Mandatum Group's privacy notice.

5 PERSONAL DATA BREACHES

A personal data breach means an event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Mandatum Group has defined procedures and measures to take in order to react and report on data breaches as required by the regulation.

Should a personal data breach occur, Mandatum Group shall without undue delay and, where feasible, not later than within 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authorities, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Mandatum Group shall communicate the personal data breach also to the data subjects without undue delay.

6 DISTRIBUTION OF RESPONSIBILITIES

In order to efficiently ensure the adequate implementation of data protection requirements, Mandatum Group has organised the distribution of responsibilities by establishing a model of three lines. Each line represents a defined role in:

1. daily operation activities and risk management (the first line);
2. ensuring, monitoring and reporting on the companies' overall risk management and compliance with regulation and internal guidelines (the second line); and
3. independently assessing and assuring by an internal audit function that the procedures and controls set in place by the first and second lines of defence are adequate and efficient (the third line).

The first line refers to the business units and functions supporting the business units in their daily operations. The management of each unit is responsible for ensuring that the data protection requirements, including accountability, are met and all potential risks concerning their processing of personal data are identified, assessed, measured, monitored, and reported as required in accordance with the Group's internal policies.

Mandatum Group has also designated a Group Data Protection Officer, an independent role responsible for monitoring compliance with the legislation and Mandatum Group's internal guidelines on the protection of personal data, for providing advice to the organisation of their obligations pursuant to the data protection requirements, as well as for other tasks stemming from the GDPR or otherwise appointed to them. The Data Protection Officer reports directly to the Board of Directors in line with Group's internal policies.

The overall responsibility for compliance with the applicable regulation lies with the Boards of Directors of the Mandatum Group companies. The Board of Directors and the Chief Executive Officer of each Mandatum Group company are responsible for ensuring that Mandatum Group's data protection is at a sufficient level and that sufficient resources are allocated to ensure data protection.

7 TIMELINESS AND REVISION OF THE PRINCIPLES

These Principles shall be reviewed annually and always when deemed necessary due to amendments in the regulatory framework or other material changes in Mandatum Group's operating environment, or changes within Mandatum Group affecting the subject issue.

Any updates or amendments to these Principles shall be approved by the Board of Directors of Mandatum plc.

Mandatum's Group Legal unit is responsible for the said review and update process.

MANDATUM

Mandatum plc

Registered domicile and address:
Bulevardi 56, FI-00120 Helsinki, Finland

Business ID: 3355142-3

www.mandatum.fi