POLICY

Data Protection Policy

Document Information

Document Holder (name and title)	Sara Edlund, Group General Counsel
Related Documents (governing document/s)	Information Security Policy Data Protection Guideline Risk Management Guideline

Distribution, Confirmation and Implementation

This steering document shall be distributed to the following functions or roles and shall be confirmed in accordance with the table below.

Confirmation required for the steering document	Read	Implemented
ICA Gruppen Board of Directors	X	X
IMT	X	X

IMT means the ICA Management Team. IMT+1 means an employee with managerial function reporting directly to an IMT Member.

By confirming that the steering document has been **READ**, the recipient acknowledges having read and understood the contents of the steering document.

By confirming that the steering document has been **IMPLEMENTED**, the recipient:

- has informed all pertinent persons within his/her respective unit of the content of this steering document; and
- has established a process to ensure that the principles and the minimum requirements of the steering document will be followed within his/her respective unit.

Versions

This steering document has been updated since implementation and the most important changes are listed below.

Version (20XX:X)	Major changes since last version
2024:1	General review to adopt new structure. The role names/titles are updated due to the reorganization within the Swedish ICA companies. We replaced the term 'data privacy' with 'data protection' as it aligns better with the Swedish translation and ICA's data protection efforts.

1 Introduction

In today's digitalized world, we all share more information online and as a result exposing our integrity. Recognizing this, the European Union established the General Data Protection Regulation (GDPR) to ensure a consistent and high level of protection of personal data across Europe.

ICA Gruppen AB and its subsidiaries ("ICA") are fully committed to processing personal data in a responsible manner in accordance with law and stakeholders' expectations. Our culture values responsibility, trust and professionalism. We want everyone who trusts us with their personal data to do so with confidence. We are transparent with why and how ICA processes personal data, ensuring that data subjects understand why we need it and how it benefits them.

We strive to embed data protection governance and management activities throughout the ICA organization so that we can demonstrate accountability and compliance.

This policy is applicable for all companies within ICA for which the GDPR is applicable. The policy applies to both employees and consultants. We will also ensure that our partners comply with this policy.

2 Data Privacy Vision and Guiding Principles

ICA always puts the individual's personal integrity at heart to build trust and protect their personal data.

We then build on the vision with five supporting guiding principles.

- **Be honest** - actively provide the data subject with the information needed at the right time.
- **Be mutual** - show the data subject the benefits of sharing data and explain how we protect it.
- **Be reliable** - set realistic commitments, keep promises and advertise changes .
- **Be human** – provide direct contact for the data subject and give faces to what we do, listen to the data subject, and give the data subject the possibility to object.
- **Be innovative yet respectful** – strive to innovate with respect for personal integrity.

3 Data Protection Processing Principles

ICA stands for a respectful processing of personal data, considering the personal integrity as well as efficiency in its business operation. ICA believes that achieving sustainable data protection

management requires striking a balance between business needs and efforts to ensure data protection compliance. ICA aims to meet business needs and maintain good ethical standards when processing personal data. ICA shall be, and be perceived to be, responsible and transparent in how ICA processes personal data and communicates with data subjects.

This policy is an expression of ICAs long-term ambition and fundamental approach to comply with applicable data protection legislation where the GDPR data protection principles shall serve as a basis for processing of personal data at ICA.

In its operations, ICA shall comply with applicable data protection laws and further strive to follow EU guidelines, industry practices, standardization, and any leading practices. As part of our commitment to data protection, we adhere to the following principles when processing personal data:

1. We process personal data lawfully, fairly and in a transparent manner (principle on lawful, fair and transparent processing)
2. We only process personal data for specified and lawful purposes and only process personal data for the purposes for which it was collected (principle on purpose limitation)
3. We only collect personal data that is adequate, relevant, and limited to what is necessary (principle on data minimization)
4. We ensure that personal data is correct and up to date (principle on accuracy)
5. We only keep personal data for as long as necessary for the purposes for which the personal data is processed (principle on storage limitation)
6. We protect personal data in terms of confidentiality and integrity (principle on integrity and confidentiality)
7. We must be able to demonstrate data protection accountability (principle on accountability)

4 Governance and Organisation

ICA has established a data protection governance and organization structure as well as a systematic data protection management to enable compliance with our data privacy principles as well as delivering on data subjects rights.

- **Processing Responsible** has an overall responsibility to ensure that a purpose of processing is carried out in accordance with the data protection principles.
- **Privacy Office** is a group-wide data protection expert function led by the Chief Privacy Officer.
- **Data Protection Officers (DPO)** have an independent role to monitor and advise data protection processing.
- **Data Protection Program Steering Committee** is responsible for long term strategy, setting and following up on goals, advising on risks and mitigation strategies as well as high level decisions elevated from the Chief Privacy Officer or any of our DPOs.

In addition to the roles mentioned here, we also have specialist roles further described in ICA data protection steering documentation, such as Data Protection Managers and Data Protection Guardians.

The Group CEO is responsible for issuing guidelines on roles and responsibilities, management of data subject rights, personal data breaches and data processing record.

5 Guidance, Compliance and Reporting

If you have any questions regarding this steering document, please consult the Privacy Office.

Each ICA Company CEO is responsible for implementation of and compliance with this steering document within its company. Compliance with applicable data protection laws resides with the highest management body within the organization, irrespective of whether a data protection officer has been appointed or not.

Enforcement and compliance follow-up is part of every manager's responsibility. According to the GDPR, there are several corrective measures that can be taken in case of violations of the GDPR. Some of those measures include warnings, reprimands, limitation of processing (including ban of processing) and administrative fines.

Each DPO shall, in collaboration with and guidance from the Privacy Office, monitor the compliance with applicable data protection laws, including internal policies and guidelines in the area. The DPO shall report any breaches of this policy to the ICA company's highest management level and Chief Privacy Officer. The Chief Privacy Officer shall report any breaches of this policy to the Board of Directors and/or IMT, where relevant.

Any deviations from this steering document shall be reported to Chief Privacy Officer (privacyoffice@ica.se) with a copy to Group General Counsel.

6 Updates and Reviews

This document shall be reviewed and updated annually or as needed based on the recommendations of Chief Privacy Officer, in consultation with Group General Counsel.