SAFEROAD®

Data Protection Manual

for Saferoad Group

Table of Contents

1. Introduction to Data Protection

The term data protection refers to laws and regulations imposed by countries to ensure that personal data (that is information relating to a natural person) is collected, made available, and otherwise processed in a fair and lawful way. The European Regulation of Personal Data, referred to as GDPR (General Data Protection Regulation) is applicable for all EU and EC states.

Processing of Personal Data in Saferoad within EU and EC should only be conducted in accordance with GDPR. Each company within Saferoad is obliged to ensure that its employees have sufficient knowledge of GDPR and other local laws and regulations applicable to its processing of Personal Data.

Data protection laws prohibit the processing of certain categories of personal data other than in exceptional circumstances, and set out prerequisites, which must be fulfilled in order for the processing of personal data to be lawful.

The Saferoad Group (from now on referred to as "Saferoad") processes personal data on a daily basis. Individuals' privacy and the security of personal data is important for Saferoad. Therefore, Saferoad has adopted this manual to ensure that the processing of personal data within Saferoad is in compliance with applicable data protection legislation. The purpose of this manual is to provide Saferoad's employees with a basic understanding of situations, which typically are governed by data protection laws, and thereby enable Saferoad's employees to comply with those laws.

This manual applies to everyone at Saferoad – all employees, managers, executive officers, and members of the board of directors (the "employees").

In addition to the general guidelines, detailed requirements in local data protection laws must be followed by employees who are responsible for activities involving processing of personal data.

2. Executive Summary

- Data protection laws set out limitations on the categories of personal data which may be collected, under which circumstances that data may be collected, and for how long the data may be stored.

- Proposed acts of collection (such as collection of employee or customer personal data, purchase of customer data for marketing purposes, and collection of personal data through websites) must be analysed closely to ensure they would not result in violation of data protection laws.

- The need for proportionality and transparency is key, and individuals must be informed of Saferoad's processing of their personal data.

- Personal data may only be disclosed to third parties when a legitimate basis for doing so has been established, and only provided that appropriate measures have been undertaken, such as a data processing agreement.

- Transfers of personal data to entities outside the European Economic Area (EEA) or access to personal data by entities outside the EEA should occur only when there is a legal basis for transfer (such as consent or a standard contract).

- Violations can result in damage claims, monetary penalties, or imprisonment as well as administrative sanctions imposed by the supervisory authority.

3. Data Collection

“Personal data” is any information, which, directly or indirectly, relates to an identified or identifiable natural person. Personal data may only be collected for specified, explicit, and legitimate purposes, and not further processed in a way incompatible with those purposes. Unless there is a legal basis for transfer (such as consent or a standard contract), personal data may not becollected.

“Processing of personal data” is any operation or set of operations which is performed upon personal data, whether or not by automatic means, including but not limited to collection, organisation, storage, adaptation, disclosure, blocking, or erasure.

It is only legal to process personal data if:

- the individual to whom the personal data relates to has given consent;
- the processing is necessary for the performance of a contract to which the individual is party, or in order to take steps at the request of the individual prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which Saferoad is subject;
- the processing is necessary in order to protect the vital interests of the individual;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority put on Saferoad or in a third party to whom the data are disclosed; or
- the processing is necessary for purposes of a legitimate interest pursued by Saferoad or by the third party or parties to whom the data are disclosed, except where such interest is overridden by the privacy interest of the individual to whom the personal data relates to.

Where required by applicable law or otherwise deemed reasonably practical and appropriate, collection of personal data should be done with the consent of the individual concerned. Consents from individuals whose personal data are being processed should be unambiguous, explicit, and possible to revoke by the individual in question.

When collecting personal data, the need for proportionality and transparency should be considered. Accordingly, the personal data collected should be adequate, relevant, and not excessive in relation to the purposes for which the data are collected and/or further processed.

4. Sensitive Personal Data and Special Categories Of Personal Data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

5. Notice

Where personal data relating to a data subject are collected from the data subject or a third party, he/she should be provided with the following information:

- the name of the legal entity which alone or jointly with others determines the purposes and means of the processing of personal data (sometimes referred to as the data controller);
- the purposes for which the personal data are intended to be processed;
- any further information which is necessary in order for the individuals to be able to exercise their rights in connection with the processing, such as the types of personal data, the recipients or categories of recipients of the data, and the nature of any access rights under applicable law, as described in Section 6 and applicable by GDPR articles 13 and 14.

6. Access Requests

If an individual makes a request to receive information regarding Saferoad's processing of personal data, to object to the processing of personal data, or to have errors in such personal data corrected, Saferoad should respond in the manner required by applicable law or otherwise deemed reasonably practical and appropriate in consultation with the VP Risk Management.

7. Data Quality, Confidentiality and Security

Processed personal data must be accurate and, to the extent necessary, up to date. Personal data that is inaccurate or incomplete should be erased or corrected.

An employee who has access to personal data must only process the data in accordance with the purpose of the processing, and may not share, distribute, or otherwise disclose the personal data to a third party unless instructed to do so by Saferoad.

Appropriate technical and organisational measures should be implemented to protect personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorised disclosure or access, and any other unlawful forms of processing. The extent of such measures should be appropriate to the risks represented by the processing, and nature of, the personal data.

Security breaches, which jeopardize the confidentiality or security of personal data processed by Saferoad should be reported immediately to a supervisor and to the VP Risk Management.

8. Storaging

Personal data should only be stored for as long as is necessary, considering the purposes for which it was collected and applicable legal storing periods.

When the storing period of personal data has expired, it should be erased in a permanent and secure way.

9. Disclosure

Personal data may only be disclosed to third parties, such as Saferoad's subcontractors, partners, and affiliates, when there is a legal basis. When disclosing personal data to a third party, a written determination should be made as to whether the third party is considered a data controller or a data processor of the personal data disclosed.

The term "data processor" refers to a legal entity which processes personal data on behalf of the data controller. The term "data controller" refers to a legal entity which alone or jointly with others determines the purposes and means of the processing of personal data.

Where required by applicable law, a data processing agreement must be entered into with each data processor, for example in connection with the use of cloud services or outsourcing of IT services. Such agreements should require the data processor to protect the personal data from further disclosure and only process personal data in accordance with Saferoad's instructions.

A data processing agreement should also require the data processor to implement appropriate security measures to protect the personal data and keep it confidential and include procedures for data breach notifications.

10. Data Transfers

Transfers of personal data to entities outside the European Economic Area (or EEA), or access to personal data by entities outside the EEA, are only allowed when the exporting entity has received assurances that the personal data will be adequately protected by the importing entity.

This may be accomplished by using one of Saferoad's standard data transfer agreements, as set out in Appendix 1 (for transfers to a non-EEA data controller) or Appendix 2 (for transfers to a non-EEA data processor) to this manual.

Saferoad's standard data transfer agreements are based on templates adopted by the EU Commission and need to be completed with details of the transfer at hand.

11. Marketing Measures and Websites

The use of personal data for marketing measures, such as direct marketing campaigns, marketing through social websites, or the purchase of personal data for marketing purposes, must fulfil the requirements of applicable law. Unless a legitimate purpose allowing the collection and use of personal data for marketing purposes can be established, personal data may not be used for these purposes. Direct marketing by use of emails, require a consent from the receiver.

Individuals are entitled to give notice that they oppose the processing of their personal data for purposes concerning direct marketing. If an individual gives such a notice, it must be honoured.

Each of Saferoad's external websites must include an online privacy statement, including procedures for accepting cookies, fulfilling the requirements of applicable law.U.S. authorities have aggressively used various theories to expand the jurisdictional reach of U.S. trade sanctions and frequently pursue non-U.S. companies for violations of U.S. sanctions, even when such transactions do not violate applicable local law.

12. Notification of Data Processing Activities

Each company within Saferoad is obliged to notify its data processing activities to the applicable supervisory authority, unless an exception from the notification obligation applies.

If the data processing activities change, an assessment should be made as to whether notifications made to the applicable supervisory authority should be updated or amended.

Each company within Saferoad is obliged to establish and maintain a record of processing activities under its responsibility. That record shall contain all of the following information;

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organization,
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures ensured.

13. Penalties

Penalties for violations of data protection laws include claims for damages by individuals whose personal data has been unlawfully processed, fines, and imprisonment. In addition, the supervisory authority may prohibit individual companies within Saferoad from engaging in certain acts of processing and impose other administrative sanctions.

The European Union is considering proposals for increased penalties for breaches of data protection laws, such as administrative penalties of up to 5% of the data controller's annual worldwide turnover or EUR 100 million.

14.Do's and Don'ts

DO:

- Exercise particular care in collecting and processing sensitive personal data and other special categories of personal data.
- Provide information to individuals and respond to access requests to the extent required by applicable law or as otherwise deemed reasonably practical and appropriate in consultation with the VP Risk Management.
- Keep personal data confidential, and implement a level of security appropriate to the risks presented by the processing, and nature, of the personal data.

DON'T:

- Collect personal data without having established the purpose of the processing and the time period during which the purpose is relevant.
- Collect personal data on a "nice to have"-basis.
- Disclose or transfer personal data, even to Saferoad's affiliates, without implementing appropriate measures, such as a data processing agreement.

15. Reporting

Employees who suspect that a violation of this policy or of relevant data protection laws has occurred within Saferoad should contact the VP Risk Management.

16. Training

Saferoad provides adequate training for all employees consistent with Saferoad's risk profile and appropriate to employee responsibilities.

17. Internal Audit

The VP Risk Management is responsible for conducting objective, comprehensive audits of the Corporate Compliance Program, including data protection, on a periodic basis in light of Saferoad's specific areas of operations, geographic locations, and legal obligations.

18. Division of responsibility for personal data within Saferoad

Each group company within Saferoad is the data controller in respect of the processing of personal data that occurs within such group company. As such, the relevant group company is responsible for treating the personal data in compliance with this manual and applicable data protection legislation.

Each group company is further responsible for keeping an updated internal register in respect of the processing of personal data for which the group company is responsible.

19. Contact information for Responsible Officers

The CEO is responsible for the overall oversight and implementation of the Corporate Compliance Program.

The VP Risk Management is responsible for Saferoad's day-to-day compliance with this manual and data protection laws.

20. Related Information

This manual should be read in connection with the following documents:

- Corporate Compliance Program Description
- Code of Conduct