

DATA PROTECTION POLICY

GOVERNING POLICIES: SECURITY POLICY AND IT POLICY

Decision instance: GD

Document owner: Johan Damell

Applies as of: 25 May 2018

DATA PROTECTION POLICY

CONTENTS

| | | |
|-----|---|---|
| 1. | PURPOSE..... | 1 |
| 2. | SCOPE..... | 1 |
| 3. | FUNDAMENTAL PRINCIPLES..... | 1 |
| 4. | RECORD | 2 |
| 5. | REQUEST FOR ACCESS..... | 2 |
| 6. | REQUEST FOR RECTIFICATION AND REGISTRATION..... | 2 |
| 7. | DATA PROCESSOR AGREEMENT | 2 |
| 8. | SECURITY MEASURES AND ACCESS | 3 |
| 9. | PERSONAL DATA BREACHES | 3 |
| 10. | DATA PROTECTION OFFICER | 3 |

1. PURPOSE

The Swedish Export Credits Guarantee Board (EKN) cares about the privacy of its counterparties, partners and employees, and abides by current data protection regulations. This document provides overall guidance on how EKN processes personal data.

2. SCOPE

All processing of personal data must be carried out in accordance with current data protection regulations. Current data protection regulations include Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), which has the force of law in Sweden, as well as national provisions supplementing the regulation.

This Policy applies to all employees and consultants.

3. FUNDAMENTAL PRINCIPLES

3.1 Lawful ground

All processing of personal data by EKN must be based on a lawful ground. Lawful grounds include performing a task in the public interest, and consent. The applicable lawful ground is communicated to the data subject, e.g. by reference to information on the EKN website. If a lawful ground cannot be identified, personal data processing must not be carried out.

3.2 Purpose limitation

If EKN is considering processing personal data for purposes other than the purpose for which the personal data were collected, the subsequent purpose must be compatible with the original one.

3.3 Data minimisation

Personal data that are processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. It must be ensured that the data that are collected are in fact needed, and personal data must not be requested merely because they might be good to have. Copies of data and storage in multiple systems must be avoided so as to minimise sources of error and to facilitate rectification.

3.4 Accuracy

Personal data that are processed must be correct and, if necessary updated. Take appropriate measures to ensure that inaccurate or incomplete data are rectified.

3.5 Storage limitation

Personal data may not be kept in a form enabling the data subject to be identified for a longer period than necessary, having regard to the purposes of the processing.

3.6 Transfer to third countries

EKN's position is that, if possible, processing of personal data should take place within Sweden's borders. GDPR means that all EU member states and EEA countries provide the same level of protection of personal data and personal privacy, and personal data may therefore be transferred freely within that area.

Personal data may only be transferred to third countries (outside the EU and EEA) in exceptional cases and if justified. Before personal data is transferred to a third country, it must be ascertained that there is an adequate level of protection in the recipient country, or that there are specific guarantees that personal data and the rights of data subjects are protected. Contact Compliance for guidance on investigation of transfers to third countries.

3.7 Impact assessment

EKN has a specific procedure in place to identify and manage specific data protection risks in its operations, and structured monitoring. For instance, particular risks in relation to the rights and freedoms of private individuals may arise in conjunction with a certain type of processing of personal data, particularly sensitive information, processing on a particularly large scale, use of new technology or the like.

Before such processing of personal data begins, Compliance must be contacted so it can be ascertained whether an impact assessment is required. Where necessary, an impact assessment will be made by the person responsible with the help of advice provided by the DPO.

4. RECORD

A record must be kept of the processing of personal data carried out by EKN and for which EKN is responsible. The record must include statutory information and be kept up to date.

5. REQUEST FOR ACCESS

Private individuals have the right to ask whether EKN processes their personal data. At the request of a data subject, EKN must confirm whether or not personal data concerning the data subject are processed, and provide access to the personal data and the information required under GDPR. Appropriate and reasonable identification measures must be taken to ensure that the information is provided to the right person.

6. REQUEST FOR RECTIFICATION AND REGISTRATION

A request for rectification and erasure of personal data must be dealt with in the manner prescribed by law. If inaccurate personal data have been registered, all reasonable measures must be taken without delay so that the data are rectified or erased.

7. DATA PROCESSOR AGREEMENT

If an external party is engaged to process personal data on EKN's behalf, a data processor agreement must be concluded. EKN's instructions to the processor concerning processing of personal data must be set out in the data processor agreement.

A processor may only be engaged if it is able to provide sufficient guarantees that it will carry out appropriate technical and organisational measures to ensure that the rights of data subjects are protected.

If possible, EKN must insert a provision in the data processor agreement to the effect that the processor will pay any costs incurred for an annual check to ascertain compliance with current data protection legislation, the data processor agreement and EKN's instructions.

8. SECURITY MEASURES AND ACCESS

Personal data must be processed so as to ensure appropriate security for the personal data, using technical and organisational measures. EKN's security coordinator must be contacted when an investigation into appropriate technical and organisational measures is evaluated.

9. PERSONAL DATA BREACHES

EKN documents all personal data breaches. EKN's security coordinator must always be notified when personal data breaches have occurred. In addition, an e-mail must be sent to GDPRincident@ekn.se. If there is a likely risk to the rights and freedoms of private individuals, this must be reported to the supervisory authority within 72 hours. EKN may need to notify the data subjects concerned of breaches that have occurred.

10. DATA PROTECTION OFFICER

EKN has a data protection officer (DPO). The DPO provides information and advice about obligations under current data protection regulations, and monitors compliance with them.