Data Privacy Policy

Contents

1. Data Privacy Policy

This data privacy policy (hereinafter the "policy") of OPR-Finance (hereinafter "OPR") sets forth the main principles to be applied in the collection, use, registration, transfer as well as other processing of personal data of natural persons by automatic means or structured filing (the "processing"). This policy shall be applied by whole OPR and is intended to highlight OPR due commitment to protect the privacy of natural persons.

Personal data as referred herein covers information such as name, address, telephone number, date of birth, nationality etc. on an identifiable natural person.

2. Responsibilities

The controller is the entity which determines the purpose and means of the processing of personal data, e.g. what information, from whom and for what purpose the information is collected. The controller is always ultimately responsible for the lawful processing of personal data. OPR or its subsidiaries shall be regarded as a controller when it determines the purpose and the way in which the information is collected and processed.

The owner of the information shall be responsible for the classification, integrity, confidentiality and availability of the information, the rights of use and the processing of personal data in accordance with the law and the OPR policies and guidelines. In the case of a breach of data protection or any deviation from the policy or guidance, the owner of the data shall report this to his supervisor and/or the Data Protection Officer.

The management of the OPR is responsible for the overall management of the registers and organizing and resourcing the data protection function and its development.

The staff of the OPR shall be responsible for the processing of personal data in accordance with the General Data Protection Regulation, personal data legislation, this privacy policy, the security policy and the OPR's other instructions. It is the responsibility of each person to report on a breach of the privacy that he/she detects, or any deviation from the policy or other instructions to the Data Protection Officer.

Superiors are responsible for that their subordinates have adequate knowledge, guidance and appropriate tools for the lawful processing of personal data. They are responsible for monitoring the privacy work and for reporting security breaches and for deviations from policies or guidelines to the Data Protection Officer.

The Processor of personal data is an entity which processes personal data in accordance with the instructions given by the Controller and on behalf of the Controller.

OPR's **Data Protection Officer** acts as a privacy expert in support of Managing Director, management and staff and assists OPR to ensure a high level of data protection and the lawfulness of the processing of personal data.

The data protection officer's tasks include, for example,

– Take part in the planning activities for the processing of OPR's personal data,

– Participate in the preparation and maintenance of the OPR privacy guidelines,

– Monitor and control the processing of personal data and their security methods;

– Contribute to the implementation of the data protection training for staff;

– Support staff and OPR customers on data protection issues;

– Acts as a liaison with the supervisory authorities,

– Monitor the development of legislation relating to the processing of personal data;

– Report to the OPR management on data protection status and development needs, and

– Take care of other data protection tasks indicated by the OPR management.

3. Objectives and Definitions

The aim of the data protection policy and the data protection work is to ensure the confidentiality of the OPR's data, personnel data and other confidential information, and to limit access to data only to persons who should have access to it based on their duties or other authorization.

The implementation of the data protection objectives will be assured by processes and practices based on staff training, guidance, minimizing the handler district and monitoring the processing of personal data. In addition, the protection of confidential information is ensured through technical security measures. The measures necessary for the protection of data are implemented through solutions that are cost-efficient relative to the risks and the security needs of the classified information.

Privacy refers to the implementation of personal data and the protection of privacy in the processing of personal data. In this policy, it also refers to the protection of other classified or highly classified information.

Data security means the technical and administrative measures designed to ensure the integrity, confidentiality and availability of information.

Personal data refers to all kinds of natural persons or characteristics describing their characteristics or living conditions which can be identified by him or his family or with those living in the same household as living with them. Identification can also be based on data aggregation.

A registered person is a natural person who is subject to personal data and whose processing of personal data is subject to policy/guidance.

Processing of personal data means the collection, deposit, organization, use, transfer, disclosure, retention, modification, aggregation, protection, deletion, destruction and other measures focused on personal data.

The personal data register means a set of data, consisting of a coherent set, and processed partly or completely by automatic data processing.

4. Processing Confidential Information

4.1. Data classification

The data processed by the OPR is classified in three categories: public, internal and confidential. A more detailed information about the classification of information and the processing of classified information is in the security practice document (Tietoturvakäytännöt).

4.2. Principles of processing personal data

Personal data must be processed in accordance with the data protection regulation and the law, in accordance with the diligence and good practice of data processing, without limiting privacy if not based on law. The processing of personal data must be planned and may not be processed for lawful purposes other than those previously defined and clearly defined. The personal data processed must be necessary for the intended use and as accurate as possible.

OPR staff must periodically review the personal data they hold and delete unnecessary data after statutory or OPR mandatory rules or other intentional activity no longer require data retention. Changes to personal data that have become known to OPR staff must be corrected without delay.

4.3. Accuracy

Personal data must be kept accurate and up-to-date. In assessing the obligation of OPR to keep the information accurate, account is taken of the purpose of the processing of personal data and of the importance of processing for the protection of the privacy.

4.4. Security

Personal data shall be adequately protected against accidental or abusive destruction or loss, alteration or unauthorized access to personal data. Technical, physical and organizational security measures must be proportionate to the sensitivity of the information in hand and the risk associated with the processing of the data. The precautions to be taken will be given more detailed guidance in the OPR security policy and other security guidelines of OPR.

If the third party processes personal data on behalf of the OPR, security, contractual arrangements and other appropriate measures shall ensure that the third parties do not disclose personal data to outsiders in violation of the OPR’s instructions or without the prior written consent of the OPR, and that the third party undertakes to protect the personal data of the OPR in a manner consistent with the OPR's own security level and the OPR's guidance on the processing of personal data.

4.5 Rights of the data subject

In the circumstances required by the regulation and the law, the registrant must be able to obtain information on the purpose for which personal data relating to them are collected and used and who is responsible for processing the data. In addition, any other data required by law should be provided to the data subject.

The data subject should have the right to know about the register data relating to them to the extent required by the regulation and the law, or where the discomfort and costs of providing the information do not exceed the interests of the data subjects. This is necessary because a person can check and, if necessary, ask for correction of information about him.

4.6. Transfer of personal data

According to the Data Protection regulation and the Personal Data Act, personal data may be transferred outside the territory of the Member States or the European Economic Area of the European Union only if the country in question ensures an adequate level of protection.

The transfer of personal data to another subsidiary of the OPR-Finance is permitted in accordance with the data Protection regulation and other applicable legislation. The Data protection regulations, personal data laws and other OPR guidelines are applied to the disclosure of personal data abroad.

4.7. Obligation of confidentiality

The employee of the OPR signs a certificate of secrecy in connection with the contract. The staff shall have a professional secrecy regarding personal data processed at work and other confidential information.

4.8. Policy approval and updating

The privacy policy is approved by the OPR management and its updating is the duty of the OPR-Finance Oy data protection officer Jouni Selin.