Our Protection Policy

Purpose and scope

NVALUE AG hereinafter referred to as the "Organization", undertakes to comply with the applicable laws and regulations relating to the protection of personal data in the countries where it operates, in this case with the Swiss LPD Law and the European GDPR

This procedure defines the fundamental principles according to which the organization processes the personal data of customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its departments and its employees in the processing of personal data.

This procedure applies to the organization and its subsidiaries (directly or indirectly) which carry out their activity within the European Economic Area or process personal data of data subjects in this area.

The recipients of this procedure are all employees, temporary or permanent.

Personal data must be processed lawfully, fairly and transparently in relation to the data subject.

Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

Data minimization

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. If possible, to reduce the risks for data subjects, the organization should apply anonymisation or pseudonymisation to personal data.

Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data which are inaccurate, in relation to the purposes for which they are processed, are erased or rectified in a timely manner.

Limitation of the retention period

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

Integrity and confidentiality

Taking into account the state of technology and other available security measures, the costs of implementation and the likelihood and severity of personal data risks, the organization shall use appropriate technical or organizational measures to process personal data in such a way as to ensure adequate security of personal data, including protection, by means of appropriate technical and organizational measures, against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Responsibility

The data controller is responsible for compliance with these principles and must be able to demonstrate the compliance of their treatments with these principles.

Collection

The organization should try to collect as little personal data as possible. If personal data is collected by a third party, the Data Controller must ensure that personal data is collected in accordance with the provisions of the law.

Use, storage and disposal

The organization must maintain the accuracy, integrity, confidentiality and relevance of the personal data based on the purpose of the processing. You must use appropriate security mechanisms to protect your personal data to prevent it from being stolen or misused and to prevent personal data breaches. the Owner is responsible for compliance with the requirements listed in this section.

Disclosure to Third Parties

Whenever the organization uses a third-party supplier or business partner to process personal data on its behalf, the Data Controller must ensure that this entity provides adequate security measures to safeguard personal data in relation to the associated risks. To this end, it is necessary to use a specific compliance questionnaire.

The supplier or business partner must only process personal data to fulfill its contractual obligations towards the organization or on the instructions of the organization and not for any other purpose. When the organization processes personal data jointly with an independent third party, the organization must explicitly specify the respective responsibilities in the respective contract or in any other legally binding document, such as the supplier's Data Processing Agreement.

Cross-border transfer of personal data

Before transferring personal data from the European Economic Area (EEA), adequate safeguards must be used, including the signing of a data transfer agreement, as required by the European Union and, if necessary, permission must be obtained from part of the data protection authority. The entity receiving the personal data must comply with the principles of personal data processing set out in the Cross-Border Data Transfer Procedure.

Access rights of data subjects

When acting as a data controller, the organization is required to provide data subjects with a reasonable access mechanism that allows them to access their personal data and must allow them to update, correct, delete or transmit their personal data, if appropriate or required by law. The access mechanism will be further detailed in the Procedure for requesting access to data of the interested party.

Data portability

Data subjects have the right to receive, upon request, a copy of the data they have provided, in a structured format and to transmit this data to another controller free of charge. the Data Controller is responsible for ensuring that such requests are processed within one month, are not excessive and do not affect the personal data rights of other people.

Right to be forgotten

Upon request, the interested party has the right to obtain from the organization the cancellation of his personal data. When the organization acts as a data controller, the Data Controller must take the necessary actions (including technical measures) to inform the third parties who use or process that data to comply with the request.

Organization and accountability

The responsibility for ensuring adequate processing of personal data rests with everyone who works within the organization or on its behalf and has access to the personal data it processes.

The main areas of responsibility for the processing of personal data refer to the following organizational roles:

The Board of Directors or other competent decision-making body makes decisions and approves the general strategies of the organization regarding the protection of personal data.

The Data Protection Officer (DPO), or any other relevant employee, is responsible for managing the personal data protection program and developing and promoting end-to-end personal data protection procedures, as defined in the Data Protection Officer's job description. Protection Officer; Document management and validity

The person responsible for the document is the Data Controller, who has the task of checking it and, if necessary, updating it, at least annually.

Date Updated: 16/01/2024