Data Protection

Purpose and scope

MC TRANS SA and now defined as “Organization”, undertakes to comply with applicable laws and regulations relating to the protection of personal data in countries where this work, in this case to the nLPD Switzerland. This policy 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 services and its employees in the processing of personal data.

The principles of nLPD

The data protection principles outline the basic responsibilities (accountability) for organizations dealing with the processing of personal data. “the controller is competent for compliance with these principles and must be able to demonstrate the conformity of its processing to these principles.”

Liceity, fairness and transparency

Personal data must be processed in a fair, transparent manner in relation to the data subject.

Limitation of the purpose

Personal data must be collected for specific, explicit and legitimate purposes and not further processed incompatible with such purposes.

Minimization of data

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 to data subjects, the organization must apply anonymization or pseudonymization to personal data.

Exact

Personal data must be accurate and, where necessary, updated; reasonable measures must be taken to ensure that inaccuracies personal data, in relation to the purposes for which they are processed, are deleted or rectified in a timely manner.

Limitation of the retention period

Personal data must be stored for a period not exceeding the one necessary for the purposes for which personal data is processed.

Integrity and confidentiality

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

Responsibility

The controller shall be competent for compliance with these principles and must be able to demonstrate the conformity of his/her processing to these principles.

Collection

The organization must 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 according to the legal forecasts.

Use, storage and disposal

The organization must maintain the accuracy, integrity, confidentiality and relevance of personal data according to the purpose of processing. You must use appropriate security mechanisms to protect your personal data to prevent it from being stolen or used improperly and prevent violations of your personal data. the Data Controller is responsible for compliance with the requirements listed in this section.

Disclosure to third parties

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

The supplier or business partner must process personal data only to fulfil their contractual obligations about the organization or instructions of the latter and not for other purposes. When the organization processes personal data jointly with a third party, the organization must explicitly specify their respective responsibilities in the respective contract or in any other legally binding document, such as the Data Processing Agreement of the supplier.

Cross-border transfer of personal data

Before transferring personal data from Switzerland and the European Economic Area (EEA) appropriate safeguard measures must be used, including signing an agreement on data transfer, as required by the European Union and, if necessary, the authorization by the data protection authority must be obtained. The entity receiving personal data must comply with the principles of the processing of personal data established in the Transfrontier Data Transfer Procedure.

Access rights of data subjects

When acting as data controller, the organization is required to provide the data subject 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 necessary or required by law. The access mechanism will be further detailed in the Request for access to data of the data subject.

Data portability

The data subjects have the right to receive a copy of the data they provided, in a structured format and to transmit this data to another data holder free of charge. the Data Controller is responsible for ensuring that such requests are processed within a month, are not excessive and do not prejudge the rights on personal data of other persons.

Right to oblivion

On request, the data subject has the right to obtain from the organization, the erasure of his personal data. When the organization acts as the controller, the Data Controller must take the necessary actions (including technical measures) to inform third parties that use or process those data to adapt to the request.

Organization and responsibility

The responsibility to ensure proper processing of personal data is for anyone working within the organization or on their behalf and having access to the personal data processed by it.

The Board of Directors takes decisions and approves the general strategies of the organization regarding the protection of personal data.