PRIVACY POLICY AND PERSONAL DATA PROTECTION POLICY

Visage Technologies AB („VTAB “), seeks to comply in the course of its business with all relevant legal provisions and regulations concerning personal data in all countries in which the Office operates. This document determines the fundamental principles by which the Office processes the personal data of the customers, users, suppliers, business associates, employees and others, establishing the roles and responsibilities in all departments of the company when processing personal data.

This policy concerns the VTAB which operates in the European Economic Area (EEA) or processes personal data of the subjects in the European Union.

Users of this document are all employees for an indefinite or fixed-term employment period, as well as all contractors engaged by the VTAB.

Definitions

The definitions set in this document are defined in Article 4. of the General Data Protection Regulation:

Personal data: any information relating to an identified or identifiable natural person;

Data subject: an identifiable natural person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Sensitive personal data: personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, merit specific protection as the context of their processing could create significant risks to fundamental rights and freedoms. Those personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, 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;

Controller: a natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Anonymization: irreversibly de-identified personal data in a way that the person cannot be identified in reasonable time, costs or technology, either by the controller or by any other person who could identify that individual. The personal data processing principles do not apply to anonymized data;

Pseudonymization: processing of personal data in a way that the personal data can no longer be assigned to a particular data subject without using additional information, provided that such additional information is kept apart and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. Pseudonymization decreases but does not entirely exclude the associating of personal data with data subject. Since pseudonymization still represents personal data, processing of the pseudonymizated data should be in accordance with the Personal Data Processing principles;

Cross-border processing: processing of personal data taking place among the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one member state; or processing of personal data taking place among the activities of a single establishment of a controller or processor in the EU but which substantially impacts or is likely to substantially impact data subjects in more than one Member State;

Supervisory authority: an independent public authority established by a Member State, pursuant to Article 51. General Data Protection Regulation;

Lead supervisory authority: the supervisory authority primarily responsible for dealing with a cross-border data processing, for example when a data subject makes a complaint about the processing of his or her personal data. It is responsible also for receiving the data breach notifications and risky processing activities, having full authority to ensure compliance with the provisions of the General Data Protection Regulation;

Local supervisory authority: responsible on its own state territory, monitoring any local data processing which has an impact on data subjects, or which is performed by an EU or non-EU controller or processor when their processing targets data subjects reside on its state territory. Their duty and powers involve undertaking of investigations and employing administrative measures and fines, strengthening awareness of the risks, rules, security and rights regarding personal data processing, as well as ensuring access to facilities of the controller and the processor with entire data processing equipment and assets;

Main establishment of a controller: with establishments in more than one Member State, the place of its central administration in the EU, unless the decisions on the purposes and means of the personal data processing are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions should be considered to be the main establishment.

Main establishment of a processor: with establishments in more than one Member State, the place of its central administration in the EU, or, if the processor has no central administration in the EU, the establishment of the processor in the EU where the main processing activities in the context of the activities of an establishment of the processor are taking place to the extent that the processor is subject to specific obligations in accordance with this Regulation.

Group of undertakings: an undertaking with a dominant position over the other subsidiary undertakings.

Basic Principles of the Personal Data Processing

The data protection principles define the main responsibilities within an organization managing personal data. Article 5(2) of the General Data Protection Regulation sets that "controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Lawful, Fair and Transparent Processing

Personal data in VTAB shall be processed in a lawful, fair and transparent manner regarding the data subject.

Purpose Limitation

Personal data are collected according to the statutory obligations and legitimate interests of VTAB and shall not be processed in a way incompatible with those purposes.

Minimum Data Quantity

Personal data correspond and are limited to what is necessary for the purposes for which they are processed. When processing personal data, VTAB uses anonymization and pseudonymization of personal data if possible, in order to decrease the risk to data subjects.

Accuracy

Personal data are accurate and kept up to date if needed. Should, in the course of processing, any inaccurate personal data appear, VTAB as the controller takes steps without delay to erase or rectify those personal data.

Storage Period Limitation

Personal data must be stored only as long as it is necessary for the purposes for which they have been processed. Time-limits and procedure of data retention are defined in the Data Retention Policy of VTAB.

Integrity and Confidentiality

Taking into account the technological achievements, available security measures, implementation costs and a possibility of a serious data protection risk, VTAB has implemented suitable technical and organizational measures in order to process personal data in a way that provides security of personal data, as well as protection from accidental or unlawful destruction, loss, alternation, unauthorized disclosure or access to.

Accountability

VTAB is a highly responsible entity capable to prove compliance with the above-mentioned principles.

Notification to Data Subjects

The General Data Protection Regulation sets ways of notifying and communicating with the data subject about his/her personal data (Articles 12, 13, 15-22) and notification on the violation of the data (Article 34).

It is particularly requested in Article 12 that notification and communication with the data subject must be carried out as follows:

-must be precise, transparent, unambiguous and easily understandable

-communicated using clear and plain language

-must be in written form (electronic or paper)

-where requested by the data subject, the information must also be provided by oral

-must be free of charge

Data Subject's Choice and Consent

Article 4(11) demands that the consent of the data subject must be given in a free, specific, informed, and unambiguous way, indicating the data subject's agreement to the processing of personal data related to him or her.

Collection

The Office collects the minimum quantity of personal data possible. In case a third party collects personal data, the CEO of VTAB must provide that personal data is collected in a lawful manner.

Use, Storage and Removal

Purposes, methods, storage limitation and retention period must correspond to Privacy Notice information. VTAB is able to keep the accuracy, integrity, confidentiality and relevance of personal data founded on the purposes in its business processes.

Relevant security mechanisms which protect personal data are used for prevention of theft, infringement of rights or misuse of personal data. The CEO of VTAB is responsible for the protection of the provisions set in this chapter.

Disclosure to Third Parties

Should VTAB engage a third-party supplier or a partner to process personal data, the CEO shall ensure that this processor takes security measures for the protection of personal data corresponding to the possible risks that may appear during the processing activities. The GDPR Compliance Questionnaire is used for this purpose.

By a contract, VTAB defines and requests the supplier or business partner to ensure the equal level of data protection as set in the course of business activities. When VTAB processes personal data together with an independent third party, the Office will explicitly specify its own and the third party's responsibilities by an appropriate contract or any other legally binding document.

Rights of Access by Data Subjects

When acting as a controller, VTAB shall ensure data subjects an acceptable access mechanism to their personal data. Data subjects have opportunity to update, rectify, erase or transfer their personal data, if applicable or required by law.

Data Portability

Upon request, data subjects have the right to receive a copy of the data which is processed by VTAB, in a structured format, as well as to transfer those data to another controller, free of charge.

The CEO of VTAB shall ensure that such requests are processed within 30 days that they are not extreme, and they do not affect the rights of personal data protection of other individuals.

Right to Be Forgotten

Upon request, data subjects have the right to demand the erasure of their personal data kept by VTAB. When VTAB acts as a controller, the CEO must take the steps and use technical measures to inform the third parties who use or process those data, about the necessary compliance with the request.

Fair Processing Guidelines

Personal data must be processed only with explicit authorization given by the CEO of VTAB. While defining the processing activities, VTAB must decide if the Data Protection Impact Assessment for each data processing activity, according to the Data Protection Impact Assessment Guidelines, will be used.

Notices to Data Subjects

During or prior to collecting personal data for any type of processing, including but not limited to selling goods, services or marketing activities, the CEO of VTAB is responsible to accurately inform data subjects about the following: the type of personal data collected, the purpose of processing, the method of processing, the data subjects' rights regarding his or her personal data, the retention period, possible international data transfer, possible sharing the data with third parties and the

security measures within the Office for the protection of personal data. This information is set in the Privacy Notice.

Depending on the processing activities and categories of personal data collected, VTAB creates a range of notices which vary depending on the processing activities (e.g. for mailing purposes or delivery of goods).

If personal data are shared with a third party, the CEO of VTAB must ensure that data subjects have been informed about that through the Privacy Notice.

If personal data are transferred to a third country according to the Cross-Border Data Transfer Policy, VTAB will clearly indicate through the Privacy Notice to where and to which institution personal data is being transferred.

When collecting sensitive personal data, Data Protection Coordinator needs to ensure that the Privacy Notice explicitly indicates for whom the sensitive personal data is being collected.

Obtaining Consents

When personal data processing is founded on the data subject's consent or other legal basis, the CEO of VTAB is responsible to ensure an appropriate record of those consents. Data subject should be presented by the CEO of VTAB with an option to provide the consent, informing and ensuring him or her that their consent (whenever consent is being used as the legal basis for processing) can be withdrawn at any moment.

If personal data are collected for a child under the age of 16, the CEO of VTAB is responsible to obtain parental consent prior to the collection, through the Parental Consent Form.

If a correction, additional information or destruction of personal data records is requested, the CEO of VTAB must ensure that such requests are managed in a reasonable time limit. Further, the CEO of VTAB must keep a log of such requests.

Personal data in VTAB are processed only for the purpose for which they were originally collected. Should VTAB wish to process collected personal data for another purpose, VTAB shall request consent by its data subjects, in a clear and unambiguous written form. Every such request includes the original purpose for which the data was collected, as well as the new or additional purpose (or purposes). The request should also state the reason for the change in purpose (purposes). The Data Protection Coordinator is responsible to comply with the rules indicated in this chapter.

The CEO of the Office has ensured that the collecting methods are in compliance with relevant law, best practices and applicable security standards.

Organization and Responsibilities

The responsibility for providing appropriate personal data processing falls on each individual working for or with VTAB and has access to personal data processed by VTAB.

The main scope of responsibilities for processing personal data is found in the following organizational units:

- **Directorate or other decision-making entity** takes decisions or approves general strategies of VTAB on personal data protection;
- **The Data Protection Coordinator or any other relevant employee is** responsible for managing the personal data protection as well as for development and promotion of end-to-end personal data protection policies, as defined in Data Protection Coordinator Job Description;
- **Head of Office** monitors and analyses personal data laws and changes to regulations, creates compliance requests and helps other departments in reaching their goals in regard to personal data;

Visage Technologies AB is not responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

The **Data Protection Coordinator** is responsible for:

- Improving all employees' awareness of user personal data protection.
- Organizing Personal data protection expertise and awareness training for employees working with personal data.
- End-to-end employee personal data protection. It must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.

Procedure in the Case of Personal Data Breach

If VTAB suspects or detects that there has come to personal data breach, the CEO of VTAB must undertake an internal investigation and take corrective remedial measures. In case of any risk to the rights and freedoms of data subjects, VTAB must without delay and, if possible, within a maximum of 72 hours from detection of the risk or incident, notify AZOP as the supervisory body.