Data Management Practices

1. Introduction

This document is a description of how data is collected, used, deleted, or otherwise processed in the Verso Vision fall prevention software (“Solution”). The Solution is used as assistance and support for care work in healthcare and social services in hospitals and elderly care to improve the safety of patients and customers. Personal data, as defined in General Data Protection Regulation (“GDPR”), is processed in the Solution. In addition, the Solution produces anonymous data from which individuals are not identifiable.

Care providers (“Customer”) who use the Solution under a separate service agreement are data controllers for any personal data processed when using the Solution whereas the processor of the personal data is typically Verso Vision Ltd., a company organized and existing under the laws of Finland, registered under number FI31288246, address Kympinkatu 3 C , FI-40320 Jyväskylä, Finland (“Verso Vision”). If the Customer acquires the Solution from a distributor or another service provider, Verso Vision acts as a subprocessor.

2. Processing of Personal Data and Types of Personal Data

The Solution uses camera sensors and AI analytics to detect risky situations in the monitored area, such as the Customer’s patient rooms. The original images from the camera sensor are not stored but only processed in real time and transformed into pose and movement analysis on the servers at the Customer’s premises.

The Solution is not connected to patient data management systems and only provides alerts based on place and room information. The Solution does not process, identify, or by any means try to identify any personal characteristics in the human figures it has detected, such as the gender, age, or ethnicity. Room information is processed in order to provide useful alerts for the medical and care personnel. By default, the Solution does not provide access for the Customer’s personnel to the camera sensor video streaming for remote monitoring of patient rooms. By the Customer’s request, anonymized real-time but not recorded mobile video streaming can be enabled from predefined events such as alarms generated by the Solution.

Data generated by the Solution is pseudonymous data because it includes place and date information, but not directly identifiable personal information about the individuals who have been in the monitored areas. Data is personal data because the Customer’s nursing personnel (i.e., persons authorized by Customer) can link data generated by the Solution with place and date information to a specific patient. Practically, the same data is anonymous data for Verso Vision’s support team since they don’t have any access to patient data. The Verso Vision support team is unable to attribute the generated data to any individuals.

From certain events, such as detected risky situations and for the monitoring of possible software failures, the Solution stores non-identifiable data on the Customer’s on-premise server with anonymous or pseudonymous metadata (date and place). Pseudonymous data is used for software failure monitoring, and anonymous data for software failure correction and product development purposes. The Solution’s actual processing of personal data takes place on the Customer’s premises.

Pseudonymous metadata (date, place, alarm type) is sent to a nurse call system and nursing personnel are notified of the detected risky situations. Nurse call systems are typically hosted on the Customer’s premises or on public cloud.

Pseudonymous data

Pseudonymous data is processed and stored for the Solution’s performance, maintenance and failure monitoring purposes only from certain events in the database in the servers located at the Customer’s premises. The pseudonymous data is stored for a limited storage period agreed with the Customer (for example, five working days) so that possible problems can be fixed, and the Solution maintained. When the agreed storage period has expired and/or the required support actions are completed, the pseudonymous data containing date and place is deleted permanently from the Solution.

Anonymous data

For product development and failure correction purposes, pseudonymous data is anonymized by Verso Vision on the servers on the Customer’s premises. Anonymized data is not personal data.

To obtain anonymized data, all the metadata of the anonymized images, which may contain information that can be used to identify an individual, is removed or made inaccurate. Then anonymous data is saved and transferred using a secure connection to the Verso Vision servers located in the EU. After the transfer, Verso Vision permanently deletes the anonymized data from the Customer’s server and database. Anonymous data is not transferred continuously but typically during the Solution’s installation phase and later if needed for software failure corrections in product development.

3. Sharing Personal Data

Any personal data processed by Verso Vision on the Customer’s behalf will not be publicly displayed or shared. Verso Vision employees have access to personal data only to the extent necessary for the performance of their work duties to provide the Solution to Customer. Third party processors who help Verso Vision to provide the Solution do not have access to personal data. Hence, Verso Vision does not use any sub-processors in this context.

4. Ensuring the Security of Personal Data

Verso Vision constantly works to protect the security of personal data and has taken necessary technical and organizational security measures to protect the personal data against accidental or unlawful destruction, loss, or alteration and against the unauthorized disclosure, abuse, or other processing in violation of applicable law. Data security of the servers at the Customer’s premises depends also on the data security measures applied by the Customer on its premises.

The measures taken include for example identity and access management; preventing unauthorized viewing of personal data; deliberately set password requirements; structurally safe network design; encryption; data loss prevention and other relevant continuously updated security measures. All Verso Vision personnel have committed themselves to confidentiality.