Cash Management

Nomentia Technical and Organizational Security Measures

Prevent unauthorized persons from gaining access to data processing sites that process and use Personal Data (site access control)

- Personal Data is processed and stored in professionally hosted data centers, which are protected with effective physical access control, including electronic locks, burglar alarms and CCTV monitoring. Only nominated, authorized persons have physical access to data center facilities. All visitors are always accompanied.

Prevent data processing systems from being used without authorization (system access control)

- Each user of data processing systems is authenticated with a personal user account. Shared or group accounts are not used for personal access. Each user account must be approved by a management sponsor, and each user is personally responsible for the user account and the ways in which it is used. User accounts are reviewed regularly, and unnecessary users are removed.

Ensure that persons authorized to use a data processing system have access only to the data they are authorized to access (data access control)

- Access rights to data processing systems are granted to pre-defined roles according to least privilege principle. Access to Personal Data must be justified with a clear and indisputable business need and approved by a management sponsor. Special admin, etc. privileges are granted to an absolute minimum number of users. Access rights are reviewed regularly, and unnecessary rights are removed.

Ensure that Personal Data cannot be read, copied, modified, or removed without authorization during electronic transfer, or when saving to data storage media (transfer control)

- Electronic transfers of Personal Data in public networks are encrypted. Transfers within a data center environment may not be encrypted; however, access to networks and processing systems is strictly limited by site and system access control. It is forbidden to store Personal Data to removable media. Backups of Personal Data are encrypted.

Ascertain and check where and to whom Personal Data can be transferred by means of data transmission facilities (disclosure control)

- Transfer of Personal Data to non-production environments, such as testing, is forbidden without explicit customer approval or sufficient data masking.

Perform checks to establish whether and by whom Personal Data has been entered, modified, or removed in data processing system (input control)

- Access to create, modify and remove Personal Data is logged, and an audit trail is created for all data processing systems. Audit trail logs are stored securely which prevents unauthorized modification or deletion of log events. Audit trail logs are stored in the service according to the service level agreement.

Ensure that Personal Data processed on behalf of a Customer is processed in strict accordance with the service description and service level agreement (order control)

- The scope of Personal Data protection is further described in the Personal Data Processing Appendix.

Ensure that Personal Data is protected against accidental destruction or loss (availability control)

- Personal Data is backed up at regular intervals. Copies of data backups are transferred securely to an offsite location for disaster recovery. Data processing systems and infrastructure utilize redundant technologies, and single points of failure are minimized. Recovery time and point objectives are determined, and every effort is made to adhere to them.

Ensure that data collected for different purposes can be processed separately (separation control)

- Personal Data is processed in dedicated systems that are not shared with other services, applications, or corporate entities. Within individual systems and databases, data is segregated with logical access control. Personal Data will not be

used for different purposes other than what it has been collected for without explicit customer approval.

Ensure that the Customer is notified promptly in the event of a material breach of any of the controls above (notification control)

- Customers will receive a prompt notification in the event of a Personal Data breach, a significant security incident in data processing system, or a material deviation from any of the controls above. In case Personal Data is lost or compromised, Customer will be invited to participate in incident resolution, and can access applicable audit trail logs in the service.