Wellspect's technical and organizational measures

1. Confidentiality

a. Physical access control: Wellspect ensures through appropriate measures that unauthorized persons do not have access to the premises and facilities used for the Processing of Customer Personal Data (in particular telephone systems, databases, application servers, and related hardware).

Physical access control	**Implemented**
24/7 monitoring of premises via security cameras	Yes
Premises protected by a facility security team	Yes
Access to the premises via personalized company ID card or registration at the reception/security desk of the facility. Access rights to certain buildings/premises/times granted individually based on task assignment	Yes
Sensitive areas and security zones protected by electronic access control systems	Yes
Visitors to the premises must register at the reception/security desk of the facility and are then accompanied by a Wellspect employee for the duration of their visit.	Yes
IT rooms protected by video surveillance and intrusion detection systems	Yes

b. Electronic access control: Wellspect ensures that the IT systems used for the processing of customers' personal data only allow authorized users limited access, specified by their individual authorization rights. Wellspect takes appropriate measures to ensure that customers' personal data cannot be read, copied, modified, or deleted without authorization.

Electronic access control	**Implemented**
User authentication via specific username and password using the principles of *least privilege* and role-based access	Yes
Password complexity is defined and enforced based on Wellspect *policies*	Yes
Multi-factor authentication is required for external access to Wellspect hardware and systems.	Yes
Firewalls are used for all external interfaces	Yes
All *workstations* use full disk encryption, and data is encrypted during transfer	Yes
Privileged identity and access management solutions are used for privileged accounts.	Yes
Regular reviews and logging of system access required by Wellspect policy and conducted by system owners.	Yes

c. Segregation control: Wellspect ensures through appropriate measures that Customer Personal Data collected for different purposes is processed separately.

Segregation control	**Implemented**
Established separation between test and production environments	Yes
Organizational separation of departments	Yes
Data collected for different purposes are processed in different systems when deemed appropriate.	Yes

d. Pseudonymization

Pseudonymization	Implemented
Wellspect applies pseudonymization techniques whenever possible in our Personal Data Processing activities.	Yes

2. Integrity

a. Data transfer control: Wellspect takes appropriate measures to ensure that during data transfer, Customers' Personal Data cannot be read, copied, modified, or deleted without authorization.

Data transfer control	Implemented
Secure connections such as Site2Site VPN with suppliers and service providers	Yes
Emails sent by Wellspect are automatically encrypted	Yes

b. Data entry control: Wellspect ensures, through appropriate measures, that it can reconstruct who entered Customer Personal Data into the Data Processing systems or who deleted such data from the Data Processing systems. Wellspect is authorized to process Customer Personal Data only on behalf of its owners and in accordance with the Agreement and/or further instructions from the owners.

Control of data entry	Implemented
Logging mechanisms that record data entry, modification, and deletion	Yes

c. Third parties: Wellspect ensures through appropriate measures that Customer Personal Data Processed on its behalf may only be Processed in accordance with its documented instructions.

Third parties	Implemented
Defined selection process for third parties accessing Customer Personal Data with specific due diligence in relation to privacy and data protection	Yes
Security measures adopted by the Processor confirmed and documented prior to collaboration	Yes
Documented instructions to the Data Processor and continuous monitoring of processing activities	Yes
Agreements to ensure effective control rights for Wellspect, including the commitment of the Processor and its employees to the confidentiality of customers' Personal Data and its deletion at the end of the collaboration	Yes

3. Availability and resilience

Availability control and rapid recovery: Wellspect takes appropriate measures to ensure that customers' Personal Data is protected against accidental loss or destruction and can be restored.

Availability control	Implemented
Business continuity plans to ensure the availability of applicable systems	Yes
Integrated high availability and redundancy for critical services	Yes
Uninterruptible power supply (UPS) including emergency power supply	Yes
Disaster recovery plan for critical infrastructure	Yes
Facilities and server rooms equipped with smoke detectors and fire alarm systems	Yes
Server rooms are air-conditioned	Yes

4. Procedures for periodic testing, evaluation, and verification

a. Data protection and incident response management

Management, testing, evaluation, and analysis	**Implemented**
Centralized data protection organization consisting of the Global Data Protection Officer, Global Privacy Office, local data protection officers, and local data privacy coordinators.	Yes
Annual training and awareness program that educates and informs employees who, due to their role, have access to Customer Personal Data about policies, procedures, and guidelines related to all aspects of data protection.	Yes
Global policies on data protection, data breaches, and data retention	Yes
Global data protection guidelines covering company standards, such as how to process sensitive Personal Data, data subjects' access rights, and data privacy impact assessments	
Incident response processes to enable management and reporting in accordance with applicable law	Yes
Continuous monitoring of the IT environment to detect malicious activity, including incident alerts	Yes
Email filtering to flag and remove any emails containing potentially malicious files or links	Yes

b. *Privacy by Design* and *Privacy by Default*

Privacy by Design and by Default	**Implemented**
Use of Privacy by Design and Privacy by Default principles in the design and development of products and services	Yes
Policies and procedures to ensure the security and storage of customers' Personal Data in approved systems	Yes
Data privacy impact assessments completed for high-risk processing activities	Yes
Automatic deletion of emails based on defined retention periods	Yes