TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Access controls to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication: anti-virus protection; stateful inspection firewalls; internal and external vulnerability scans; intrusion detection and prevention systems; least-privilege access to IT systems based on job role and segregation of duties; password procedures (incl. special characters, minimum length, periodic changes); no access for guest Users or anonymous accounts; two-factor authentication for privileged IT administrators who access the Platform.

2. Access controls to Customer Data

Measures must be taken to prevent authorized Users from accessing Customer Data beyond their authorized access rights. These measures shall include: least-privilege access rights based on job role and segregation of duties; management approval required for new or modified access prior to provisioning or change; terminated User access disabled within 72 hours of notification from human resources; monthly logical and physical access review for workforce members with access to production; quarterly administrator access revalidated by management; physical access to the data centers restricted to appropriate individuals; two-factor authentication for privileged IT administrators who access production.

3. Disclosure controls

Measures must be taken to prevent the unauthorized access, alteration, or removal of Customer Data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include: encryption using a VPN for remote access; secure File Transfer Protocol (SFTP) for transport and communication of Customer Data; prohibition of portable media; media sanitization and destruction procedures.

4. Change management controls

Measures must be put in place to ensure all changes to Systems are logged, tested, and approved. Measures must include: change request and approval required prior to implementation into production; critical application changes tested and approved prior to implementation into production; access to migrate changes into production restricted to appropriate individuals; critical changes reviewed monthly basis to confirm appropriateness and authorization.

5. Data processing controls

Measures must be put in place to ensure that Customer Data is processed strictly in compliance with the data exporter's instructions under the GDPR. These measures must include: unambiguous wording of contractual instructions; monitoring of contract performance; monitoring of Service Level Agreements (SLAs).

6. Availability controls

Measures must be put in place to ensure that Customer Data is protected against accidental destruction or loss. These measures must include: Customer Data backup procedures; uninterruptible power supply (UPS); business continuity procedures; 24x7 Network Operations Centre (NOC) monitoring; critical jobs monitored for successful completion and error resolution; problem and incident management and response procedures; Incident Issue management and response procedures; root cause analysis required for problems and incidents affecting production.

7. Segregation controls

Measures must be put in place to allow Customer Data collected for different purposes to be processed separately. These must include: restriction of access to Customer Data according to job role and segregation of duties; segregation of business IT systems; segregation of IT testing and production environment.