ANNEX III:

TECHNICAL AND ORGANISATIONAL MEASURES

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

Physical and Environmental Security:

House of Control has implemented suitable measures to prevent unauthorized persons from gaining access to the data processing (including database and application servers and related hardware). This is accomplished by:

a) Established security areas

b) Protected and restricted access

c) Secured data processing equipment and personal computers

d) All access to data centres where Personal Data is hosted are logged and monitored and secured by restricted access controls, and other appropriate security measures

e) Maintenance and inspections in IT areas and data centres shall only be carried out by authorized personnel.

Endpoint protection:

a) All servers and House of Control clients are set up with automated virus control.

b) Host based firewalls are configured for all servers. Server and application management are only accessible from specific whitelisted IP addresses.

Encryption:

a) Encryption in transit, SSL/TLS termination in the application server

b) Password database is encrypted

c) Data at rest and backups are encrypted

Access Control (Complete Control, James and/or IT-application)

House of Control has implemented an authorization and authentication framework including, but not limited to, the following elements:

a) Role-based access control

b) Processes to create, modify and delete accounts

c) Access to Complete Control, James and applications is protected by authentication mechanisms

d) Access Management procedure and Privileged Access Management Procedure strictly enforced

Measures:

a) All access to data (including personal data) is logged

b) Authorization and logging measures for network connections to Complete Control, James and applications (including firewalls) implemented

c) Privileged access rights to Complete Control, James, applications and network are only granted to persons who need access to complete their tasks (last-privilege principle)

d) Privileged access rights to Complete Control, James and applications are documented and kept up to date

e) Access rights to Complete Control, James and applications are reviewed and updated on regular basis

f) Automatic time-out of users and blocking when several erroneous passwords are entered, along with log files

g) House of Control maintains log-on procedures on Complete Control, James and applications with safeguards against suspicious login activity

Availability Control:

House of Control has defined, documented, and implemented a backup concept for Complete Control and James, including the following technical and organizational elements:

a) Backup servers are protected against unauthorized access and environmental threats

b) Defined backup intervals

c) The restoration of data from backups is tested regularly (Disaster Recovery) on the criticality of Complete Control and James

d) Backup is performed on dedicated servers

e) Datacentres in which Personal Data is stored or processed are protected against natural disasters, physical attacks or accidents

f) IT systems and applications in non-production environments are logically or physically separated from Complete Control, James and applications in production environment

Operations Security:

Application servers have managed hosting with power, network and colocation services monitored 24/7/365. System logs and application environment is monitored, and critical incidents create alarms and notifications are followed up during normal office hours. House of Control also performs Continuous Vulnerability Scanning through Visma Application Security Program (VASP).

a) House of Control logs security-relevant events, such as user management activities, failed logons, changes on the security configuration of Complete Control, James and applications

b) House of Control analyses Complete Control, James and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities

c) House of Control scans and tests Complete Control, James and applications for security vulnerabilities on a regular basis. We utilize several tools for security testing and detection of vulnerabilities;

- We utilize a dedicated SAST tool for detection of security flaws in Code repositories during the Development process.

- We utilize dedicated SCA tool for control on Open-Source libraries and features.
- We utilize a dedicated DAST tool for security testing in the Staging/Test environment.
- We utilize a dedicated security tool for monitoring, scanning and detection of security vulnerabilities and activities in the Cloud Infrastructure.

d) House of Control has implemented and maintains a change management process for Complete Control, James and applications

e) House of Control maintains a process to update and implement vendor security fixes and updates for Complete Control, James and applications

Security Incidents:

House of Control has implemented and maintains an Incident Response Plan, including but not limited to:

a) Records of security breaches

b) Customer notification process, and

c) Routines to address the following at time of incident:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise
- Specific incident response procedures and
- Coverage and responses of all critical system components

Penetration testing:

House of Control conduct external penetration testing and phishing testing as two different activities.

a) Complete Control end James benefits from advanced platforms built to rapidly detect, analyse, and respond to security threats. Testing for application vulnerabilities is being done on a regular basis and server configuration testing is done daily.

- We conduct Pentests with manned Visma Pentesting teams every 18 months
- Monitoring systems and automatic procedures for security updates are established.

b) House of Control employees undergo phishing tests several times annually, as per our internal security awareness program and the corporate Visma Security Program. We subscribe to the Visma wide service for regular phishing tests.

Human Resource Security:

House of Control has implemented the following measures in the area of human resource security:

a) Employees with access to Personal Data are bound by Confidentiality Agreements
b) Employees with access to Personal Data are trained regularly regarding the applicable data protection and security
c) House of Control has implemented an offboarding process for House of Control employees