ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES

Physical and Environmental Security:

House of Control have 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:

1. Established security areas
2. Protected and restricted access
3. Secured data processing equipment and personal computers
4. All access to data centers where Personal Data is hosted are logged and monitored and secured by restricted access controls, and other appropriate security measures
5. Maintenance and inspections in IT areas and data centers shall only be carried out by authorized personnel.

Endpoint protection:

1. All servers and House of Control clients are set up with automated virus control.
2. Host based firewalls are configured for all servers. Server and application management are only accessible from specific whitelisted IP addresses.

Encryption:

1. Encryption in transit, SSL/TLS termination in the application server
2. Password database is encrypted
3. Backups are encrypted

Access Control (Complete Control and/or IT-application):

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

1. Role-based access control
2. Processes to create, modify and delete accounts
3. Access to Complete Control and applications is protected by authentication mechanisms
4. Access Management procedure and Privileged Access Management Procedure strictly enforced

Measures:

1. All access to data (including personal data) is logged

2. Authorization and logging measures for network connections to Complete Control and applications (including firewalls) implemented
3. Privileged access rights to Complete Control, applications and network are only granted to persons who need access to complete their tasks (last-privilege principle)
4. Privileged access rights to Complete Control and applications are documented and kept up to date
5. Access rights to Complete Control and applications are reviewed and updated on regular basis
6. Automatic time-out of users and blocking when several erroneous passwords are entered, along with log files
7. House of Control maintains log-on procedures on Complete Control and applications with safeguards against suspicious login activity

Availability Control:

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

1. Backup servers are protected against unauthorized access and environmental threats
2. Defined backup intervals
3. The restoration of data from backups is tested regularly (Disaster Recovery) on the criticality of Complete Control
4. Backup is performed on dedicated servers4
5. Datacenters in which Personal Data is stored or processed are protected against natural disasters, physical attacks or accidents
6. IT systems and applications in non-production environments are logically or physically separated from Complete Control 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 perform Continuous Vulnerability Scanning through Argus Continuous Vulnerability Monitoring (ACVM):

1. House of Control logs security-relevant events, such as user management activities, failed logons, changes on the security configuration of Complete Control and applications
2. House of Control analyzes Complete Control and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities
3. House of Control scans and tests Complete Control and applications for security vulnerabilities on a regular basis
4. House of Control have implemented and maintains a change management process for Complete Control and applications
5. House of Control maintains a process to update and implement vendor security fixes and updates for Complete Control and applications

Security Incidents:

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

1. Records of security breaches
2. Customer notification process, and
3. Routines to address the following at time of incident:
    1. Roles, responsibilities, and communication and contact strategies in the event of a compromise
    2. Specific incident response procedures and
    3. Coverage and responses of all critical system components

Penetration testing:

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

1. Complete Control benefits from Mnemonic´s advanced platform built to rapidly detect, analyze, and respond to security threats. House of Control has an ongoing agreement with Mnemonic for security testing. Testing for application vulnerabilities are being done on a regular basis and server configuration testing is done daily. Monitoring systems and automatic procedures for security updates are established.
2. House of Control employees undergo phishing tests at least annually as per our internal security awareness program. We use Secure Practice for phishing tests.

Human Resource Security:

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

1. Employees with access to Personal Data are bound by Confidentiality Agreements
2. Employees with access to Personal Data are trained regularly regarding the applicable data protection and security
3. House of Control have implemented an offboarding process for House of Control employees