Appendix III

TECHNICAL AND ORGANISATIONAL MEASURES

IN ACCORDANCE WITH ART. 28 OF THE GDPR: THE FOLLOWING ARE APPLIED TECHNICAL AND ORGANISATIONAL MEASURES IN ALL EU AND NON/EU SUBSIDIAIRIES OF THE CHAMP GROUP

DECEMBER 2022

1. Pseudonymization and encryption of personal data (Art. 32 para. 1 (a) of the GDPR)

- **Pseudonymization**

  Processing personal data in a manner such that personal data can no longer be attributed to any specific data subject without consulting additional information, provided that this additional information is kept in a separate location and is subject to technical and organizational measures.
- **Encryption**

  Encryption is used to protect corporate assets by signing executables developed by CHAMP or communications with any application programming interfaces exposed. CHAMP owns a corporate public key infrastructure but also works with world's premier high-assurance digital certificate providers.

2. Measures to ensure confidentiality (Art. 32 para. 1 (b) of the GDPR)

- **Physical access control**

  Accesses are limited to authorized datacentre personnel. Periodic controls are performed audited for SOC compliance (ISAE 3402 SOC 1 Type II), from herein referred to solely as SOC to ensure that physical access to data centres is restricted to authorized and appropriate personnel.
- **System and Data access control**

  CHAMP invest significant effort to keep accesses to all the systems managed following a Role-Based Access Control principle. Roles, privileges, and permissions are periodically audited for SOC compliance.

- **Separation control**

  Separate environments for development, test and production are audited regulalry for SOC compliance.

3. Measures to ensure integrity (Art. 32 para. 1 (b) of the GDPR

- **Transfer control**

  All network accesses are protected by two level of firewalls operating in a deny-all mode in conjunction additional security components including, but not limited to, Intrusion Detection and Prevention Systems. Encrypted connections protect data in transit over public networks. Network security is audited regularly for SOC compliance.
- **Input control**

  Logical access to system infrastructure is restricted to authorized and appropriate personnel. Security-related events are monitored 24/7. Automated tool raises alerts in case of privileged-level access modification. Technical and organizational controls are audited regularly for SOC compliance.

4. Availability and resilience of systems and services (Art. 32 (b) of the GDPR)

- **Availability control**
  Redundant Data Centers are located in Luxembourg and audited regularly for SOC compliance.
- **Availability of IT systems used**
  IT systems are hosted in Tier 4 and Tier 3-equivalent Data Centers
  - Tier 4 - A completely fault-tolerant data center with redundancy for every component
  - Tier 3-equivalent - A data center with multiple paths for power and cooling, and redundant systems that allow the staff to work on the setup without taking it offline

5. Measures to restore availability and access to personal data in the event of a technical incident (Art. 32 (c) of the GDPR)

- **Recovery/backup systems**
  Online backups are maintained at separate data centers within Luxembourg. CHAMP backup systems are audited regularly for SOC compliance.
  Back-up on disks and tapes are replicated weekly between data centers to always ensure that a recent and complete copy of the backup is available in each DC.

6. Procedures for the regular review, assessment, and evaluation of technical and organizational measures (Art. 32 para. 1 (d) of the GDPR; Art. 25 para. 1 of the GDPR)

- **Data protection management**

  Description of measures taken:

  - Register of processing activities is maintained and regular risk assessment and inventory management is conducted to ensure that measures remain compliant and up-to-date.
  - Data Protection Agreements, Policies and Procedures, Privacy Notices, Consent Forms, and other related documents are periodically reviewed. Ongoing training and awareness programs for employees and contractors are conducted.

- **Data protection-friendly default settings (privacy by default)**

  Description of measures taken:

  Privacy by design Policy and process implemented and training to key divisions delivered;

  Pre-DPIA and full DPIA forms and Decommissioning forms established.

- **Contract control**

  (Technical/organizational) measures to define the respective competencies of Controller and Processor.

  Description of measures taken:

  Data Protection Amendment for customers and suppliers implemented;

  Amendment of Employee contracts;

  Vendor Management project work in progress.