ANNEX III

Technical and organisational measures, including those designed to ensure data security

Table of Contents

Background and Objectives

Perseus Technologies GmbH (“Perseus”) implements appropriate technical and organisational measures (“TOMs”) to safeguard the confidentiality, integrity and availability of personal data and to ensure the resilience of its systems. “Appropriate” in this context means that the measures are suitable and proportionate in relation to the risks to be managed.

When planning, implementing and carrying out the measures, Perseus takes into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons. These measures include the following:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the systems and services relating to the processing;

- the ability to swiftly restore the availability of, and access to, personal data following a physical or technical incident;
- a procedure for regularly reviewing, assessing and evaluating the effectiveness of the technical and organisational measures to ensure the security of the processing.

When assessing the appropriate level of protection, Perseus takes particular account of the risks associated with the processing (e.g. destruction, loss, alteration or unauthorised disclosure of, or unauthorised access to, personal data).

The requirements are reflected and documented in the following categories of TOM:

- Confidentiality (Art. 32(1)(b) GDPR)
- Integrity (Art. 32(1)(b) GDPR)
- Availability and resilience (Art. 32(1)(b) GDPR)
- Procedures for regular review, assessment and evaluation (Article 32(1)(d) of the GDPR, Article 25(1) of the GDPR)

This document serves, in particular, to fulfil the contracting parties' obligation to provide evidence under data protection law.

In addition to the technical and organisational measures (TOMs) within the meaning of data protection law, in particular in accordance with Article 32 of the GDPR, Perseus has implemented an information security management system (ISMS) based on the requirements of the international standard ISO/IEC 27001:2013.

Scope and field of application

Perseus implements data security measures both for its own data processing activities and for the data processing carried out in order to provide the various Perseus Cyber Security Services. To provide these services, Perseus engages data processors who, on the basis of agreed data processing agreements (Article 28 of the GDPR), process personal data on its behalf in accordance with its instructions. These data processing relationships and the corresponding agreements constitute sub-processing relationships for the purposes of this agreement. The sub-processors thus engaged meet at least the security standards set by Perseus. Perseus's own technical and organisational measures (TOMs), as well as those of the data processors, complement one another seamlessly in the provision of services and together ensure an appropriate level of data security.

This document describes the data security measures relevant to the provision of the various Perseus Cyber Security Services.

Description of the individual measures

Confidentiality (Art. 32(1)(b) GDPR)

Access control – protection against unauthorised access to data processing facilities

Technical	Organisational
• Electronic access control system for the premises used by Perseus (smart cards/transponders) • Mechanical security locks • Motion detectors • CCTV monitoring of access points • Appropriate measures in the event of	• the definition of security zones for the premises used by Perseus • Role-based and documented assignment and management of access rights ("Role-Based Access Control – RBAC") with an integrated Joiner-Mover-Leaver process • Visitor policy governing access to

Perseus's sub-processors	Perseus's business premises, in particular assignment to a Perseus employee, logging of the visit, and the requirement to wear visitor badges • security guards • Appropriate measures at the sub-processors

Access control – protection against unauthorised system use

Technical	Organisational
• Authentication using user ID + password • Two-factor authentication • Firewalls • Virtual Private Network (VPN) • Anti-virus protection • Automatic screen lock • appropriate measures in relation to the sub-processors	• Role-based and documented assignment and management of access rights ("Role-Based Access Control, RBAC") with an integrated Joiner-Mover-Leaver process • Password policy and reset procedures • Appropriate measures in place for the sub-processors

Access control – protection against unauthorised reading, copying, modification or removal of data within an IT system

Technical	Organisational
• Logging of access to applications, in particular when entering, amending and deleting data • Hard disk encryption on end devices • Encryption of data storage media • Use of document shredders	• Classification of information (public/internal/confidential) • Granting of authorisations in accordance with the 'need-to-know' principle • Role-based and documented assignment and management of access rights ("Role-Based

• Appropriate measures in place for the sub-processors	Access Control RBAC") with an integrated Joiner-Mover-Leaver process • Password policy and reset procedures • Use of service providers for document and data destruction in accordance with DIN 66399 • Appropriate measures in place for the sub-processors

Principle of separation – separate processing of data

Technical	Organisational
• Separation of development, test and production environments • Appropriate measures in place for the sub-processors	• Physical or logical client segregation • Appropriate measures in relation to the sub-processors

Pseudonymisation — Article 32(1)(a) GDPR, Article 25(1) GDPR — Personal data cannot be attributed to a specific data subject without the use of additional information

Technical	Organisational
• Separation of the allocation file and its storage on a separate, secure IT system • Appropriate measures in relation to the sub-processors	• Assessment for all processing activities as to whether pseudonymous data processing is possible • Appropriate measures in relation to the sub-processors