

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Inhaltsverzeichnis

Hintergrund und Zielsetzung	1
Scope und Anwendungsbereich	2
Beschreibung der einzelnen Maßnahmen	3

Hintergrund und Zielsetzung

Die Perseus Technologies GmbH ("Perseus") ergreift zur Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sowie zur Sicherung der Belastbarkeit der Systeme angemessene technische und organisatorische Maßnahmen ("TOM"). Angemessen bedeutet dabei, dass die Maßnahmen hinsichtlich der zu steuernden Risiken geeignet und verhältnismäßig sind.

Bei der Planung, Implementierung und Umsetzung der Maßnahmen berücksichtigt Perseus den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Diese Maßnahmen schließen folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus berücksichtigt Perseus insbesondere die Risiken, die mit der Verarbeitung verbunden sind (z.B. Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten).

Die Anforderungen sind in folgenden Kategorien von TOM abgebildet und dokumentiert:

- Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Integrität (Art. 32 Abs. 1 lit. b DSGVO)
- Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

Dieses Dokument dient insbesondere der datenschutzrechtlichen Nachweispflicht der Vertragsparteien.

Perseus hat neben TOM im Sinne des Datenschutzrechts (Art. 32 DSGVO) ein Informationssicherheits-Managementsystem (ISMS) entsprechend der internationalen Norm ISO/IEC 27001:2013 implementiert, welches sich aktuell im Zertifizierungsprozess befindet.

Scope und Anwendungsbereich

Perseus ergreift sowohl für die eigenen Datenverarbeitungen wie auch für die Datenverarbeitungen zur Erbringung der unterschiedlichen Perseus Cyber Security Service Datensicherheitsmaßnahmen. Perseus setzt zur Leistungserbringung Auftragsverarbeiter ein, die auf Grundlage vereinbarter Verträge zur

Auftragsverarbeitung (Art. 28 DSGVO) eine weisungsgebundene Verarbeitung personenbezogener Daten im Auftrag durchführen. Diese Auftragsverarbeitungsverhältnisse und die entsprechenden Vereinbarungen sind Unterauftragsverhältnisse im Hinblick auf die vorliegende Vereinbarung. Die somit eingesetzten Unter-Auftragsverarbeiter erfüllen dabei mindestens die von Perseus gesetzten Sicherheitsstandards. Die eigenen TOM von Perseus wie auch die TOM der Auftragsverarbeiter ergänzen sich nahtlos bei der Leistungserbringung und sorgen gemeinsam für ein angemessenes Datensicherheitsniveau.

Dieses Dokument beschreibt die Datensicherheitsmaßnahmen, die für die Erbringung der unterschiedlichen Perseus Cyber Security Service relevant sind.

Beschreibung der einzelnen Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle – Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

Technisch	Organisatorisch
- elektronisches Zutrittskontrollsystem für die von Perseus genutzten Betriebsstätten (Chipkarten/Transponder) - mechanische Sicherheitsschlösser - Bewegungsmelder - Videoüberwachung der Zugänge - adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern	- Definition von Sicherheitszonen für die von Perseus genutzten Betriebsstätten - rollenbasierte und dokumentierte Zutrittsrechtevergabe und Zutrittsrechteverwaltung ("Role Based Access Control RBAC") mit integriertem Joiner-Mover-Leaver-Prozess - Besucherregelung zum Zutritt zu von Perseus genutzten Betriebsstätten, insbesondere Zuweisung zu einem Perseus-Mitarbeiter, Protokollierung des Besuchs, Pflicht zum Tragen von Besucherausweisen - Wachschutz - adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern

Zugangskontrolle – Schutz vor unbefugter Systemnutzung

Technisch	Organisatorisch
• Authentifikation mit Benutzerkennung + Passwort • Zwei-Faktor-Authentifizierung • Firewalls • Virtual Private Network VPN • Anti-Viren-Schutz • automatische Bildschirmsperre • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern	• rollenbasierte und dokumentierte Zugangsrechtevergabe und Zugangsrechteverwaltung ("Role Based Access Control RBAC") mit integriertem Joiner-Mover-Leaver-Prozess • Passwort-Regelung und Rücksetzungsverfahren • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern

Zugriffskontrolle – Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen von Daten innerhalb eines IT-Systems

Technisch	Organisatorisch
• Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten • Festplattenverschlüsselung Endgeräte • Verschlüsselung von Datenträgern • Einsatz von Aktenvernichtern • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern	• Klassifikation von Informationen (öffentlich/intern/vertraulich) • Vergabe von Berechtigungen nach dem Need-to-know-Prinzip • rollenbasierte und dokumentierte Zugriffsrechtevergabe und Zugriffsrechteverwaltung ("Role Based Access Control RBAC") mit integriertem Joiner-Mover-Leaver-Prozess • Passwort-Regelung und Rücksetzungsverfahren • Einsatz von Dienstleistern zur Akten- und Datenvernichtung nach DIN 66399 • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern

Trennungsgebot – Getrennte Verarbeitung von Daten

Technisch	Organisatorisch
• Trennung von Entwicklung-, Test- und Produktivumgebung • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern	• physische oder logische Mandantentrennung • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern

Pseudonymisierung – Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO – Ohne Hinzuziehung zusätzlicher Informationen können personenbezogene Daten keiner spezifischen betroffenen Person zugeordnet werden

Technisch	Organisatorisch
• Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern	• Prüfung für alle Verarbeitungstätigkeiten, ob eine pseudonyme Datenverarbeitung möglich ist • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern