Vereinbarung zur Auftragsverarbeitung
für
Perseus Cyber Security Service

(basierend auf der Muster-Vertragsanlage des Bitkom e.V.)

Zwischen

[Name Auftraggeber]

[Sitz Auftraggeber]

– Auftraggeber –

und der

Perseus Technologies GmbH

Hagelberger Str. 53 -54, 10965 Berlin

DE-10623 Berlin

- Auftragnehmer -

(gemeinsam auch Vertragsparteien bezeichnet)

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Präambel

Diese Vereinbarung zur Auftragsverarbeitung (»Vereinbarung«) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz und der Auftragsverarbeitung für den Perseus Cyber Security Service (»PCSS«), die als Auftragsverarbeitungen i.S.d. Art. 28 DS-GVO erbracht werden. Der der Auftragsverarbeitung zu Grunde liegende Service ist jeweils im Servicevertrag (»Servicevertrag«) für diesen Service, ggf. in der Leistungsbeschreibung und in den Allgemeinen Geschäftsbedingungen des Auftragnehmers (»AGB«) geregelt. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag im Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem jeweiligen Servicevertrag ergeben sich grundsätzlich Gegenstand und Dauer des Auftrags und damit der Verarbeitung sowie Art und Zweck der Verarbeitung.

Der Zweck der Verarbeitung, die betroffenen Personen sowie die Kategorien personenbezogener Daten werden in der Anlage 1 zu dieser Vereinbarung konkretisiert und sind anwendbar, sofern der jeweilige Service erbracht wird.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Servicevertrag und ggf. in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen (Anlage 3). Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(3) Der Auftragnehmer unterstützt, soweit vereinbart, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der

Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder Daten zu löschen.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist.

(2) Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung, soweit vereinbart.

(4) Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Unterauftragnehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 2 aufgeführten Unterauftragnehmer durchgeführt.

(4) Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Unterauftragnehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

(5) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Servicevertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht.

§9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Auftraggeber	Auftragnehmer
Ort, Datum	Ort, Datum
	
_____	_____
Unterschrift Unterzeichnungsberechtigter	Unterschrift Unterzeichnungsberechtigter

Anlage 1 - DETAILS DER VERARBEITUNGEN

I. Perseus Phishing Check (PPC)s

A. BETROFFENE PERSONEN

Betroffene Personen sind Mitarbeitende des Auftraggebers.

B. KATEGORIEN PERSONENBEZOGENER DATEN

Es werden folgende System- und Anwendungsdaten (zum Teil personenbezogene) verarbeitet:

- Namen
- E-Mailadressen
- Firma
- Ergebnisse der Phishing-Checks

C. ZWECK DER DATENVERARBEITUNG

Die Daten werden für folgende Zwecke verarbeitet:

- zum Zwecke der Wahrung der Informationssicherheit (auch Cybersicherheit) und der Datensicherheit (technisch-organisatorischer Datenschutz) beim Auftraggeber
- Analyse der Sensibilität der Mitarbeiter
- Sensibilisierung der Mitarbeiter

II. Perseus Cyber Security Services (PCSS)

A. BETROFFENE PERSONEN

Betroffene Personen sind Mitarbeitende des Auftraggebers.

B. KATEGORIEN PERSONENBEZOGENER DATEN

Es werden folgende System- und Anwendungsdaten (zum Teil personenbezogene) verarbeitet:

- Dateiinformationen
- Netzwerkinformationen
- Prozessinformationen
- Account-Informationen
- Endpunkt-Netzwerkaktivität
- Geräteidentität
- Teilnahmestatus und Ergebnisse der Online-Trainings

C. ZWECK DER DATENVERARBEITUNG

Die Daten werden für folgende Zwecke verarbeitet:

- Herstellung, Wahrung und Verbesserung der Cybersecurity- und Datenschutz-Compliance bei Kunden und Bezugsberechtigten
- technisch-organisatorischer Datenschutz (Datensicherheit) und Cyber Security (Informationssicherheit) zur Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und personenbezogener Daten
- Durchführung und Auswertung von Online-Trainings
- Malware Scan

III. Incident Response Management (IRM)

A. BETROFFENE PERSONEN

Betroffene der Datenverarbeitung können regelmäßig Beschäftigte der Kunden und Bezugsberechtigten, die Mitarbeiter deren Kunden und Lieferanten und sonstige natürliche Personen

sein, deren personenbezogene Daten von den Kunden und Bezugsberechtigten verarbeitet werden und die im Rahmen der Serviceerbringung von PERSEUS verarbeitet werden oder aber auf die PERSEUS gelegentlich der Serviceerbringung Zugriff hat (beispielsweise Kunden des Auftraggebers bzw. deren Mitarbeiter, Lieferanten des Auftraggebers bzw. deren Mitarbeiter, sonstige natürliche Personen).

B. KATEGORIEN PERSONENBEZOGENER DATEN

Beim Incident-Management besteht potenzieller Zugriff auf alle (personenbezogenen) Daten, die in den Datensätzen des Auftraggebers enthalten sind, auf die im Rahmen des Incident-Managements durch den Auftragnehmer und dessen Unterauftragnehmer zugegriffen werden muss. Das können sein:

- alle personenbezogenen Verbindungs- und Inhaltsdaten (Stamm- und Transaktionsdaten), die in den kompromittierten Systemen des Kunden bzw. Bezugsberechtigten verarbeitet werden, besteht potentieller Zugriff
- alle personenbezogenen Daten, die zur Analyse oder forensischen Beweissicherung in PERSEUS-Systeme übertragen werden

C. ZWECK DER DATENVERARBEITUNG

Ein gezielter Zugriff auf diese Daten erfolgt nicht, der Zugriff kann aber gelegentlich der Leistungserbringung erfolgen.
Die Daten werden für folgende Zwecke verarbeitet:

- Herstellung, Wahrung und Verbesserung der Cybersecurity- und Datenschutz-Compliance bei Kunden und Bezugsberechtigten
- technisch-organisatorischer Datenschutz (Datensicherheit) und Cybersecurity (Informationssicherheit) zur Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und personenbezogener Daten
- Analyse und Rekonstruktion von Sicherheitsvorfällen
- Erteilung von Handlungsempfehlung
- Wiederherstellung der Systeme, Anwendungen, Informationen und Daten
- Dokumentation der Sicherheitsvorfälle
- forensische Beweissicherung
- kontinuierliche Verbesserung („PDCA-Zyklus“)Aufdeckung von Malware in E-Mails und damit verbundene Angriffe und Bedrohungen

Anlage 2 - Unterauftragnehmer

I. Perseus Phishing Check (PPC)

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
Inboxroad, Zekeringstraat 32B, 1014 BS Amsterdam, Niederlande	E-Mail Dienstleister zum Versenden von Test-Phishing-E-Mails
Amazon Web Services, Inc 410 Terry Avenue North Seattle, WA 98109-5210, US	Server Hosting und Cloud Services

II. Perseus Cyber Security Services (PCSS)

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
Google WebRisk, Google Ireland Limited, Gordon House, Barrow Street Dublin 4, Irland	Blacklist-Dienst von Google, der URL-Listen für Webressourcen mit Malware oder Phishing-Inhalten bereitstellt
Amazon Web Services, Inc 410 Terry Avenue North Seattle, WA 98109-5210, US	Server Hosting und Cloud Services

III. Incident Response Management (IRM)

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
SEC Consult Deutschland Unternehmensberatung GmbH, Ullsteinstraße 130, 12109 Berlin	fachliche Unterstützung bei der Leistungserbringung, First-Level-Support
TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen	systemtechnische Unterstützung des Fernzugriffs auf die Benutzeroberfläche von Endgeräten bei Kunden und Bezugsberechtigten durch den Einsatz von TeamViewer

Anlage 3 - Technische und Organisatorische Maßnahmen ("TOM")

Inhaltsverzeichnis

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

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

Weitergabekontrolle - Schutz vor unbefugtem Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Technisch	Organisatorisch
• Virtual Private Network VPN • E-Mail-Verschlüsselung • Verschlüsselung von E-Mail-Anhängen • TLS-Verschlüsselung (https://) • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern	• siehe Zutritts-, Zugangs- und Zugriffskontrolle

Eingabekontrolle - Feststellung, ob und von wem personenbezogene Daten in DV-Systemen eingegeben, verändert oder entfernt worden sind

Technisch	Organisatorisch
• Nutzerbezogene Protokollierung der Zutritte, Zugänge und Zugriffe (Eingabe, Änderung und Löschung von Daten)	• Vergabe von persönlichen Nutzer-Accounts, damit die Eingabe, Änderung und Löschung von Daten einer Einzelperson nachvollziehbar zugeordnet werden kann • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit - Art. 32 Abs. 1 lit. c DSGVO - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust und Vorkehrungen zur schnellen Wiederherstellung

Technisch	Organisatorisch
Da Perseus selbst grundsätzlich keine eigene IT-Infrastruktur betreibt, sondern SaaS (Software-as-a-Service) nutzt, beziehen sie die folgenden Angaben auf die SaaS-Provider und insbesondere auf deren Serverräume: • Brandschutzeinrichtungen • Feuermelde- und Feuerlöschanlagen • Hochwasserschutz • Überspannungsschutz • Klimatisierung • Überwachung von temperatur und Feuchtigkeit • Unterbrechungsfreie Stromversorgung USV • Redundante Netzanbindung • Belastungs- und Wiederanlauftests • Datensicherungen/Backups	• Business-Continuity-Plan • Notfallplan inkl. Meldewege • Backup- und Recoverykonzept • adäquate Maßnahmen bei den durch Perseus eingesetzten Unter-Auftragsverarbeitern

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Technisch	Organisatorisch
n.a.	• Bestellung eines Datenschutzbeauftragten • Bestellung einer Informationssicherheitsbeauftragten • Aufbau, Betrieb und kontinuierliche Verbesserung eines Datenschutz-Managementsystems • Aufbau, Betrieb und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems • Berichtswesen • Audits

Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung - Art. 25 Abs. 2 DSGVO

Technisch	Organisatorisch
n.a.	• Vorabprüfung von zur Einbindung geplanter SaaS auf “Privacy-by-Design” • Vorabprüfung von zur Einbindung geplanter SaaS auf “Privacy-by-Default”

Auftragskontrolle - Auftragsverarbeitung im Sinne von Art. 28 DSGVO

Technisch	Organisatorisch
n.a.	sorgfältige Auswahl des Auftragnehmers (insbesondere hinsichtlich Datensicherheit) • vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation mit Nachweisen • Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller Anforderungen gemäß Art. 28 DSGVO