

BIJLAGE III

Technische en organisatorische maatregelen, onder meer om de veiligheid van de gegevens te waarborgen

Inhoudsopgave

Achtergrond en doelstelling	1
Toepassingsgebied en reikwijdte	2
Beschrijving van de afzonderlijke maatregelen	3

Achtergrond en doelstelling

Perseus Technologies GmbH ("Perseus") neemt passende technische en organisatorische maatregelen ("TOM") om de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens te waarborgen en de robuustheid van de systemen te verzekeren. Passend betekent in dit verband dat de maatregelen geschikt en evenredig zijn ten opzichte van de te beheersen risico's.

Bij de planning, implementatie en uitvoering van de maatregelen houdt Perseus rekening met de stand van de techniek, de implementatiekosten, de aard, de omvang, de omstandigheden en de doeleinden van de verwerking, alsmede met de verschillende waarschijnlijkheid van optreden en de ernst van het risico voor de rechten en vrijheden van natuurlijke personen. Deze maatregelen omvatten het volgende:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en diensten in verband met de verwerking op lange termijn te waarborgen;

- het vermogen om de beschikbaarheid van de persoonsgegevens en de toegang daartoe snel te herstellen in geval van een fysiek of technisch incident;
- een procedure voor het regelmatig controleren, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter waarborging van de veiligheid van de verwerking.

Bij de beoordeling van het passende beschermingsniveau houdt Perseus met name rekening met de risico's die aan de verwerking verbonden zijn (bijvoorbeeld vernietiging, verlies, wijziging of ongeoorloofde openbaarmaking van of ongeoorloofde toegang tot persoonsgegevens).

De vereisten zijn weergegeven en gedocumenteerd in de volgende categorieën van TOM:

- Vertrouwelijkheid (art. 32, lid 1, onder b) AVG)
- Integriteit (art. 32, lid 1, onder b, AVG)
- Beschikbaarheid en veerkracht (art. 32, lid 1, onder b, AVG)
- Procedures voor regelmatige controle, beoordeling en evaluatie (art. 32, lid 1, onder d, AVG, art. 25, lid 1, AVG)

Dit document dient met name ter vervulling van de bewijsplicht van de contractpartijen op het gebied van gegevensbescherming.

Naast de technische en organisatorische maatregelen (TOM) in de zin van de wetgeving inzake gegevensbescherming, in het bijzonder overeenkomstig art. 32 AVG, heeft Perseus een informatiebeveiligingsmanagementsysteem (ISMS) geïmplementeerd dat is gebaseerd op de eisen van de internationale norm ISO/IEC 27001:2013.

Reikwijdte en toepassingsgebied

Perseus neemt zowel voor de eigen gegevensverwerking als voor de gegevensverwerking ter uitvoering van de diverse Perseus Cyber Security Service-gegevensbeveiligingsmaatregelen maatregelen. Perseus schakelt voor de dienstverlening verwerkers in die op basis van overeengekomen overeenkomsten inzake verwerking in opdracht (art. 28 AVG) de verwerking van persoonsgegevens in opdracht uitvoeren en daarbij aan instructies gebonden zijn. Deze verwerkingsovereenkomsten en de bijbehorende afspraken vormen onderaannemingsrelaties in het kader van de onderhavige overeenkomst. De aldus ingeschakelde onderverwerkers voldoen daarbij ten minste aan de door Perseus vastgestelde beveiligingsnormen. De eigen TOM van Perseus en de TOM van de verwerkers vullen elkaar naadloos aan bij de dienstverlening en zorgen gezamenlijk voor een passend niveau van gegevensbeveiliging.

Dit document beschrijft de gegevensbeveiligingsmaatregelen die relevant zijn voor de levering van de verschillende Perseus Cyber Security Services.

Beschrijving van de afzonderlijke maatregelen

Vertrouwelijkheid (art. 32, lid 1, onder b) AVG)

Toegangscontrole – bescherming tegen ongeoorloofde toegang tot gegevensverwerkingsinstallaties

Technisch	Organisatorisch
• elektronisch toegangscontrolesysteem voor de door Perseus gebruikte bedrijfsvestigingen (chipkaarten/transponders) • mechanische veiligheidsslots • Bewegingsdetectoren • videobewaking van de toegangen • passende maatregelen bij de door	• definitie van veiligheidszones voor de door Perseus gebruikte bedrijfsvestigingen • Op rollen gebaseerde en gedocumenteerde toekenning en beheer van toegangsrechten ("Role Based Access Control – RBAC") met geïntegreerd Joiner-Mover-Leaver-proces • Bezoekersregeling voor toegang tot de door

Perseus ingeschakelde subverwerkers	door Perseus gebruikte vestigingen, in het bijzonder toewijzing aan een Perseus-medewerker, registratie van het bezoek, verplichting tot het dragen van bezoekersbadges • bewaking • passende maatregelen bij de door Perseus ingeschakelde subverwerkers
-------------------------------------	---

Toegangscontrole – bescherming tegen ongeoorloofd systeemgebruik

Technisch	Organisatorisch
• Authenticatie met gebruikersnaam + wachtwoord • Tweefactorauthenticatie • Firewalls • Virtual Private Network (VPN) • Antivirusbescherming • automatische schermvergrendeling • passende maatregelen ten aanzien van de door Perseus ingeschakelde subverwerkers	• rolgebaseerde en gedocumenteerde toekenning en beheer van toegangsrechten ("Role Based Access Control, RBAC") met geïntegreerd Joiner-Mover-Leaver-proces • Wachtwoordbeleid en procedures voor het resetten van wachtwoorden • passende maatregelen bij de door Perseus ingeschakelde subverwerkers

Toegangscontrole – bescherming tegen het ongeoorloofd lezen, kopiëren, wijzigen of verwijderen van gegevens binnen een IT-systeem

Technisch	Organisatorisch
• Logboekregistratie van toegang tot applicaties, met name bij het invoeren, wijzigen en verwijderen van gegevens • Versleuteling van harde schijven op eindapparaten • Versleuteling van gegevensdragers • Gebruik van papiervernietigers	• Classificatie van informatie (openbaar/intern/vertrouwelijk) • Toekenning van toegangsrechten volgens het 'need-to-know'-principe • rolgebaseerde en gedocumenteerde toekenning en beheer van toegangsrechten ("Role Based

• passende maatregelen bij de door Perseus ingeschakelde subverwerkers	Access Control RBAC”) met geïntegreerd ‘Joiner-Mover-Leaver’-proces • Wachtwoordbeleid en procedures voor het resetten van wachtwoorden • Inschakeling van dienstverleners voor de vernietiging van dossiers en gegevens volgens DIN 66399 • passende maatregelen bij de door Perseus ingeschakelde subverwerkers
--	--

Scheidingsbeginsel – Gescheiden verwerking van gegevens

Technisch	Organisatorisch
• Scheiding van ontwikkel-, test- en productieomgeving • passende maatregelen bij de door Perseus ingeschakelde subverwerkers	• fysieke of logische scheiding van mandanten • passende maatregelen bij de door Perseus ingeschakelde subverwerkers

Pseudonimisering – art. 32, lid 1, onder a) AVG, art. 25, lid 1 AVG – Zonder aanvullende informatie kunnen persoonsgegevens niet aan een specifieke betrokkene worden gekoppeld

Technisch	organisatorisch
• Scheiding van het toewijzingsbestand en de opslag op een afzonderlijk, beveiligd IT-systeem • passende maatregelen ten aanzien van de door Perseus ingeschakelde subverwerkers	• Controle voor alle verwerkingsactiviteiten of pseudonome gegevensverwerking mogelijk is • passende maatregelen bij de door Perseus ingeschakelde subverwerkers