VERWERKERSOVEREENKOMST

Versie: 1 oktober 2026

Inleiding

Deze Verwerkersovereenkomst met haar bijlagen is een bijlage bij de overeenkomst (de "Overeenkomst") tussen Epassi Nederland B.V. ("Epassi Nederland") en Epassi NL Platform Transactions B.V. ("Epassi Platform Transactions"), ieder als dienstverlener, en de klant (de "Klant") zoals vermeld in de Overeenkomst.

De Verwerkersovereenkomst wordt gebruikt door zowel Epassi Nederland als Epassi Platform Transactions. Dit betekent dat de Verwerkersovereenkomst afzonderlijk van toepassing is op de Overeenkomst tussen de Klant en Epassi Nederland en op de Overeenkomst tussen de Klant en Epassi Platform Transactions. Epassi Nederland en Epassi Platform Transactions zijn ieder zelfstandige contractspartijen die niet aansprakelijk zijn voor het handelen van de ander.

Bij het uitvoeren van de in de Overeenkomst omschreven diensten kunnen Epassi Nederland en Epassi Platform Transactions persoonsgegevens verwerken ten behoeve van de Klant. In dat geval treden Epassi Nederland en Epassi Platform Transactions op als Verwerker en de Klant als Verwerkingsverantwoordelijke. Verwijzingen in deze Verwerkersovereenkomst naar "Verwerker" gelden als verwijzingen naar Epassi Nederland dan wel Epassi Platform Transactions (afhankelijk van de Overeenkomst die in het betreffende geval van toepassing is), en verwijzingen naar "Verwerkingsverantwoordelijke" gelden als verwijzingen naar de Klant.

Artikel 1. Definities

In deze Verwerkersovereenkomst hebben de met een hoofdletter geschreven begrippen de volgende betekenis:

- **Autoriteit Persoonsgegevens:** de Nederlandse toezichthoudende autoriteit op het gebied van gegevensbescherming, belast met het toezicht op de naleving van de toepasselijke privacywet- en regelgeving.
- **AVG:** de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679 van 27 april 2016).
- **Betrokkene(n):** de natuurlijke persoon of personen op wie de Persoonsgegevens betrekking hebben.
- **Bijlage(n):** iedere bijlage bij deze Verwerkersovereenkomst. De bijlagen zijn onlosmakelijk verbonden met deze Verwerkersovereenkomst.
- **Derde(n):** iedere natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of ander orgaan, niet zijnde de Verwerker
- **EER:** de Europese Economische Ruimte.
- **Incident:** iedere gebeurtenis waarbij of als gevolg waarvan Persoonsgegevens worden vernietigd, gewijzigd, verloren gaan en/of ongerechtvaardigd aan een Derde worden verstrekt, of die een Derde in staat stelt zich onbevoegd toegang tot de Persoonsgegevens te verschaffen.
- **Log:** het (computer)bestand of de (computer)bestanden waarin de verwerkingsactiviteiten automatisch worden vastgelegd.

- **Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de Betrokkene) die door de Verwerker ten behoeve van de Verwerkingsverantwoordelijke wordt verwerkt.
- **Subverwerker:** een partij die door de Verwerker wordt ingeschakeld voor de uitvoering van zijn verplichtingen uit de Overeenkomst. De Subverwerker is (hoofdzakelijk) belast met de verwerking van Persoonsgegevens.
- **Toepasselijk Gegevensbeschermingsrecht:** de AVG, de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) en alle overige toepasselijke nationale en Europese wet- en regelgeving inzake de bescherming van persoonsgegevens.
- **Verwerkersovereenkomst:** de onderhavige verwerkersovereenkomst inclusief haar Bijlagen.

Artikel 2. Algemene bepalingen

2.1 De Verwerkingsverantwoordelijke stelt het doel van en de middelen voor de verwerkingsactiviteiten vast. De Verwerkingsverantwoordelijke valt daarmee onder artikel 4 lid 7 AVG. De Verwerker wordt uitsluitend ingeschakeld om Persoonsgegevens te verwerken ten behoeve van en op schriftelijke instructie van de Verwerkingsverantwoordelijke. De Verwerker valt daarmee onder artikel 4 lid 8 AVG.

2.2 De Verwerker verstrekt de Verwerkingsverantwoordelijke alle informatie die nodig is om aan de toepasselijke privacywet- en regelgeving te voldoen.

Artikel 3. Verwerking van Persoonsgegevens

3.1 De Verwerker verwerkt de Persoonsgegevens ten behoeve van de Verwerkingsverantwoordelijke in overeenstemming met de toepasselijke privacywet- en regelgeving. Bijlage 1 bevat een overzicht van de soorten Persoonsgegevens die worden verwerkt, de categorieën Betrokkenen op wie de Persoonsgegevens betrekking hebben en het doel waarvoor en de middelen waarmee de Persoonsgegevens worden verwerkt.

3.2 De Verwerker verwerkt Persoonsgegevens uitsluitend overeenkomstig de instructies van de Verwerkingsverantwoordelijke. De Verwerker wijkt alleen van deze instructies af indien hij daartoe wettelijk verplicht is, of indien het opvolgen van een instructie zou leiden tot een schending van wet- of regelgeving.

3.3 Bij de verwerking van Persoonsgegevens wijkt de Verwerker niet af van het doel waarvoor de Persoonsgegevens oorspronkelijk door de Verwerkingsverantwoordelijke zijn verstrekt, tenzij hij daartoe op grond van een wettelijk voorschrift verplicht is.

3.4 De Verwerker verstrekt de Persoonsgegevens niet aan een Derde, tenzij deze verstrekking plaatsvindt op schriftelijke instructie en/of met schriftelijke toestemming van de Verwerkingsverantwoordelijke. Het is de Verwerker eveneens toegestaan de Persoonsgegevens aan een Derde te verstrekken indien dit noodzakelijk is om aan een wettelijke verplichting te voldoen.

3.5 De Verwerker draagt er zorg voor dat de Persoonsgegevens niet buiten de EER worden verwerkt, tenzij de Verwerkingsverantwoordelijke daarvoor schriftelijke toestemming heeft gegeven.

3.6 Indien de Verwerker van de Verwerkingsverantwoordelijke toestemming heeft gekregen om de Persoonsgegevens buiten de EER te verwerken, treft de Verwerker passende waarborgen ter bescherming van de Persoonsgegevens, waaronder het gebruik van de door de Europese Commissie vastgestelde standaardcontractbepalingen (Uitvoeringsbesluit (EU) 2021/914) en/of het uitsluitend

verwerken of doorgeven van Persoonsgegevens op basis van een adequaatheidsbesluit (artikel 45 AVG) en/of goedgekeurde certificeringsmechanismen (artikel 42 AVG).

Artikel 4. Technische en organisatorische maatregelen

4.1 Overeenkomstig artikel 32 AVG treffen en handhaven Partijen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bijlage 2 bevat een overzicht van de door de Verwerker getroffen technische en organisatorische maatregelen. Deze maatregelen worden periodiek geëvalueerd en zo nodig aangepast.

4.2 Bij het implementeren van beveiligingsmaatregelen houdt de Verwerker rekening met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de doeleinden van de verwerking en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van de Betrokkene.

4.3 De Verwerker houdt een audittrail bij van relevante verwerkingsactiviteiten (bijvoorbeeld systeemlogs) die voldoende is om de naleving van deze Verwerkersovereenkomst aan te tonen. Op verzoek van de Verwerkingsverantwoordelijke verleent de Verwerker zonder onredelijke vertraging toegang tot deze logs.

Artikel 5. Bijstand

5.1 De Verwerker verleent, voor zover vereist op grond van artikel 28 lid 3 onder f AVG, alle redelijke bijstand aan de Verwerkingsverantwoordelijke om deze in staat te stellen aan zijn verplichtingen uit de AVG te voldoen, zoals ten aanzien van beveiliging, datalekken en gegevensbeschermingseffectbeoordelingen, rekening houdend met de informatie waarover de Verwerker beschikt en de rol van de Verwerker, en voor zover de Verwerkingsverantwoordelijke zelf geen toegang heeft tot de relevante informatie. De Verwerker is gerechtigd de redelijke interne kosten en uitgaven die hij maakt in verband met de nakoming van dit artikel in rekening te brengen.

5.2 Zodra de Verwerker een verzoek van een Betrokkene ontvangt, zoals een verzoek om informatie, inzage, rectificatie, verwijdering, beperking van de verwerking en/of gegevensoverdraagbaarheid (artikelen 13 tot en met 20 AVG), of een beroep op enig ander recht van de Betrokkene, stuurt de Verwerker dit verzoek zonder onredelijke vertraging door aan de Verwerkingsverantwoordelijke.

5.3 De Verwerker verleent alle redelijke bijstand aan de Verwerkingsverantwoordelijke nadat deze een verzoek van een Betrokkene heeft ontvangen, zodat de Verwerkingsverantwoordelijke kan voldoen aan zijn wettelijke verplichtingen op grond van de toepasselijke privacywet- en regelgeving.

Artikel 6. Audits

6.1 De Verwerkingsverantwoordelijke heeft het recht om op eigen kosten audits uit te voeren van de systemen, processen en registraties van de Verwerker die rechtstreeks betrokken zijn bij de verwerking van de Persoonsgegevens van de Verwerkingsverantwoordelijke op grond van deze Verwerkersovereenkomst. Audits vinden maximaal eenmaal per kalenderjaar per Verwerkingsverantwoordelijke plaats, behalve bij een vermoedelijk Incident, een wettelijke verplichting of indien schriftelijk anders is overeengekomen. De Verwerkingsverantwoordelijke kondigt een audit ten minste dertig (30) dagen van tevoren schriftelijk aan. De Verwerker verleent redelijke medewerking aan dergelijke audits, waaronder, na overleg met de Verwerkingsverantwoordelijke, het verlenen van toegang tot relevant personeel, systemen en registraties die rechtstreeks betrekking hebben op de onder deze Verwerkersovereenkomst vallende verwerkingsactiviteiten.

6.2 De kosten van de audit komen voor rekening van de Verwerkingsverantwoordelijke. Indien uit de audit blijkt dat de Verwerker deze Verwerkersovereenkomst op wezenlijke punten niet naleeft, komen de redelijke kosten van de audit voor rekening van de Verwerker.

6.3 De Verwerker verleent alle redelijke medewerking aan een onderzoek van de Autoriteit Persoonsgegevens of een andere bevoegde toezichthoudende autoriteit naar de verwerkingsactiviteiten van de Verwerker. De Verwerker stelt de Verwerkingsverantwoordelijke zonder onredelijke vertraging op de hoogte zodra hij van een dergelijk onderzoek kennis heeft genomen, tenzij dit wettelijk verboden is.

Artikel 7. Incidenten

7.1 Zodra de Verwerker kennis heeft genomen van een beveiligingsincident dat heeft geleid, of redelijkerwijs waarschijnlijk heeft geleid, tot een inbreuk in verband met persoonsgegevens (zoals gedefinieerd in de AVG), stelt de Verwerker de Verwerkingsverantwoordelijke daarvan zonder onredelijke vertraging op de hoogte en in ieder geval uiterlijk aan het einde van de eerstvolgende werkdag.

7.2 De Verwerker treft alle redelijke maatregelen om de gevolgen van het Incident te beperken en/of een nieuw Incident te voorkomen. De Verwerker verleent tevens alle redelijke medewerking aan de Verwerkingsverantwoordelijke bij de beoordeling van het Incident, zodat deze kan voldoen aan zijn wettelijke verplichtingen tot melding aan de bevoegde toezichthoudende autoriteiten en/of het informeren van de Betrokkenen.

Artikel 8. Subverwerkers

8.1 De Verwerkingsverantwoordelijke geeft de Verwerker hierbij toestemming om Subverwerkers in te schakelen voor de uitvoering van de Overeenkomst. De actuele lijst van door de Verwerker ingeschakelde Subverwerkers is beschikbaar op www.epassi.nl/static/subverwerkers. Welke Subverwerkers worden ingezet kan verschillen afhankelijk van de door de Verwerkingsverantwoordelijke gekozen Diensten en functionaliteiten; niet alle vermelde Subverwerkers zijn op iedere Verwerkingsverantwoordelijke van toepassing.

8.2 Indien de Verwerker een Subverwerker wenst in te schakelen of te vervangen, informeert hij de Verwerkingsverantwoordelijke daarover. De Verwerkingsverantwoordelijke kan binnen veertien (14) dagen na ontvangst van de kennisgeving bezwaar maken tegen dit voornemen. Maakt de Verwerkingsverantwoordelijke niet binnen veertien (14) dagen na ontvangst van de informatie over de voorgenomen wijziging bezwaar, dan wordt hij geacht met de voorgenomen wijziging te hebben ingestemd.

8.3 De Verwerker sluit een overeenkomst met de door hem ingeschakelde Subverwerkers. Deze overeenkomst moet in overeenstemming zijn met de toepasselijke privacywet- en regelgeving. De Verwerker legt de Subverwerker voorwaarden op die in wezen gelijkwaardig zijn aan die van deze Verwerkersovereenkomst.

Artikel 9. Geheimhouding

9.1 De Verwerker houdt alle Persoonsgegevens die hij ten behoeve van de Verwerkingsverantwoordelijke verwerkt geheim. De bepalingen over geheimhouding in de op de Overeenkomst toepasselijke algemene voorwaarden zijn van toepassing.

9.2 De Verwerkingsverantwoordelijke behandelt alle informatie over de beveiligingsmaatregelen, IT-systemen, Subverwerkers en interne processen van de Verwerker die hij op grond van deze

Verwerkersovereenkomst verkrijgt, met inbegrip van informatie die in het kader van een audit wordt verstrekt, als vertrouwelijk en maakt deze niet aan derden bekend, behalve voor zover een wettelijke verplichting dat vereist.

Artikel 10. Duur en beëindiging

10.1 Deze Verwerkersovereenkomst treedt in werking op het moment dat de Overeenkomst tot stand komt en blijft van kracht zolang de Overeenkomst van kracht is. De Verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst. Verplichtingen die naar hun aard bestemd zijn om voort te duren, blijven tussen Partijen van kracht nadat de Verwerkersovereenkomst is beëindigd en/of (van rechtswege) is geëindigd.

10.2 De verplichtingen van de Verwerker met betrekking tot het teruggeven en verwijderen van Persoonsgegevens bij beëindiging zijn opgenomen in Bijlage 1 (Details van de verwerking).

10.3 In geval van faillissement blijft deze Verwerkersovereenkomst onverkort van kracht tussen Partijen, teneinde de continuïteit van de verwerking te waarborgen binnen de context waarin de Persoonsgegevens oorspronkelijk zijn verstrekt.

Artikel 11. Slotbepalingen

11.1 De bepalingen over toepasselijk recht en bevoegde rechter in de Overeenkomst zijn van toepassing op deze Verwerkersovereenkomst.

11.2 In geval van strijdigheid tussen deze Verwerkersovereenkomst en de Overeenkomst prevaleert deze Verwerkersovereenkomst voor zover het de verwerking van Persoonsgegevens betreft.

Bijlage 1: Details van de verwerking

1. Categorieën Betrokkenen

De personen op wie de Persoonsgegevens betrekking hebben zijn:

- Werknemers van de Verwerkingsverantwoordelijke.

2. Soorten Persoonsgegevens

De door de Verwerker verwerkte soorten Persoonsgegevens zijn:

Indien Epassi Nederland B.V. de Verwerker is:

De volgende Persoonsgegevens worden altijd door Epassi Nederland B.V. verwerkt:

- Voornaam;
- Achternaam;
- Geboortedatum;
- Datum indiensttreding;
- Einddatum contract;
- IP-adres;
- Globale locatie op basis van IP-adres;
- Zakelijk e-mailadres;
- Privé e-mailadres op verzoek van de Verwerkingsverantwoordelijke;
- Verrichte benefit-transacties;
- Personeelsnummer;
- Indien sportabonnementen (bedrijfsfitness) worden aangeboden:
  - Geslacht
  - Volledig adres
  - Telefoonnummer
  - IBAN-gegevens

Indien Epassi NL Platform Transactions B.V. de Verwerker is:

De volgende Persoonsgegevens worden altijd door Epassi NL Platform Transactions B.V. verwerkt:

- Voornaam;
- Achternaam;
- Zakelijk e-mailadres;
- Privé e-mailadres (indien verzocht door de Verwerkingsverantwoordelijke);
- Verrichte benefit-transacties;
- Indien sportabonnementen (bedrijfsfitness) worden aangeboden:
  - Geslacht
  - Volledig adres
  - Telefoonnummer
  - IBAN-gegevens

3. Aard en doel van de verwerking

De Verwerker verwerkt de Persoonsgegevens voor de volgende doeleinden:

Indien Epassi Nederland de Verwerker is:

- Het leveren van de diensten zoals overeengekomen in de Overeenkomst, waaronder in het bijzonder het aanbieden van het Epassi Platform aan de Verwerkingsverantwoordelijke voor het beheer van diens employee benefits, het aanmaken en beheren van werknemersaccounts in het Epassi Platform, en het aanmaken en inkopen van benefits van derden (met inbegrip van het doorgeven van Persoonsgegevens aan derde partners die dergelijke benefits aanbieden);
- Opslag van de Persoonsgegevens in de back-end van het Epassi Platform;
- Toegang tot de Persoonsgegevens in de back-end via het Epassi Platform om de Persoonsgegevens in de front-end aan gebruikers te tonen;
- Het bieden van ondersteuning aan werknemers van de Verwerkingsverantwoordelijke bij hun gebruik van het Epassi Platform;
- Het communiceren met werknemers van de Verwerkingsverantwoordelijke over de functionaliteiten van en updates van het Epassi Platform;
- Het analyseren van gebruikspatronen en het verbeteren van de prestaties, gebruikerservaring en dienstverlening van het Epassi Platform;
- Het bewaken en waarborgen van de beveiliging en integriteit van het platform, waaronder het voorkomen van onbevoegde toegang en het afhandelen van beveiligingsincidenten;
- Het aan de Verwerkingsverantwoordelijke ter beschikking stellen van een webportaal voor het analyseren van het gebruik door werknemers van de Verwerkingsverantwoordelijke en het beheren van het Epassi Platform.

Indien Epassi Platform Transactions de Verwerker is:

- Toegang tot en verwerking van alle gegevens over benefits die ten behoeve van de Verwerkingsverantwoordelijke zijn aangeschaft, om de waarde van de benefits overeenkomstig de Overeenkomst te factureren dan wel te verrekenen.

De Persoonsgegevens worden **niet verwerkt** voor de volgende doeleinden:

- Het uitvoeren van analyses en/of het opstellen van rapportages over het gebruik van benefits op niet-geanonimiseerde wijze;

Bewaartermijn van de Persoonsgegevens

- Na beëindiging van de zakelijke relatie heeft de Verwerkingsverantwoordelijke dertig (30) dagen (de "Bewaartermijn") om te verzoeken om export of verwijdering van de Persoonsgegevens. Gedurende de Bewaartermijn kan de Verwerkingsverantwoordelijke de Verwerker opdragen om: a. de Persoonsgegevens te exporteren in een gangbaar, machineleesbaar formaat, of b. de Persoonsgegevens te verwijderen.
- Na ontvangst van een verzoek van de Verwerkingsverantwoordelijke tot verwijdering van de Persoonsgegevens of na afloop van de Bewaartermijn, afhankelijk van wat zich het eerst voordoet, zal de Verwerker binnen maximaal dertig (30) dagen: a. alle Persoonsgegevens definitief verwijderen of vernietigen, of b. alle Persoonsgegevens anonimiseren zodat de betrokkenen niet langer identificeerbaar zijn, tenzij langere opslag wettelijk verplicht is. Daarnaast draagt de Verwerker er zorg voor dat ook de bij zijn Subverwerkers aanwezige Persoonsgegevens worden verwijderd, vernietigd of geanonimiseerd.

- De Verwerker bevestigt binnen tien (10) dagen na afronding van deze handelingen schriftelijk aan de Verwerkingsverantwoordelijke dat alle Persoonsgegevens overeenkomstig deze bepaling zijn verwijderd, vernietigd of geanonimiseerd.

4. Verwerking buiten de EER

De Persoonsgegevens worden hoofdzakelijk binnen de Europese Economische Ruimte (EER) verwerkt. Hoewel de Verwerker gebruikmaakt van Subverwerkers die hun hoofdkantoor buiten de EER kunnen hebben, vindt iedere doorgifte van Persoonsgegevens buiten de EER uitsluitend plaats in overeenstemming met hoofdstuk V van de AVG, waaronder het gebruik van passende waarborgen zoals standaardcontractbepalingen of andere rechtmatige doorgiftemechanismen.

Contactgegevens

Voor vragen of opmerkingen over deze Verwerkersovereenkomst en haar Bijlagen kunt u contact opnemen met de vertegenwoordiger van de Verwerker:

S. Cune, DPO, privacy@epassi.nl

Bijlage 2: Technische en organisatorische maatregelen

Deze Bijlage bevat de technische en organisatorische maatregelen die de Verwerker heeft getroffen ter bescherming van Persoonsgegevens. De in deze Bijlage opgenomen maatregelen kunnen zo nodig worden gewijzigd en/of uitgebreid. De Verwerkingsverantwoordelijke beschouwt de hieronder vermelde maatregelen als passend om het risico te beperken dat gepaard gaat met het uitbesteden van bepaalde verwerkingsactiviteiten aan de Verwerker.

1. Technische maatregelen

- De Verwerker is ISO/IEC 27001:2022 gecertificeerd. De Verwerker verstrekt op verzoek een kopie van het certificaat en de verklaring van toepasselijkheid.
- De Verwerker gebruikt Amazon Web Services als cloudprovider. Amazon Web Services is onder meer gecertificeerd volgens ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015 en CSA STAR CCM v4.0.
- De Verwerker past versleuteling toe van gegevens in rust en tijdens transport voor zijn opslagsystemen, te weten AWS RDS en AWS S3, beveiligd met AES-256.
- Beperking van risico's door menselijke fouten
  - De wachtwoorden en inloggegevens voor de interne systemen worden opgeslagen in een wachtwoordmanager die aan audits is onderworpen.
  - Ieder verzoek om gegevens, ook van interne teamleden, wordt eerst getoetst en beoordeeld om vertrouwelijke gegevens te beschermen en een audittrail van de handeling te hebben.
- Toegang tot clouddiensten
  - De diensten zijn niet direct via internet bereikbaar, maar bevinden zich achter een Virtual Private Cloud die alleen met de juiste inloggegevens toegankelijk is.
- Hardeningbeleid
  - De Verwerker gebruikt een CVE-scanner (Common Vulnerabilities and Exposures) voor alle softwarepakketten en images en brengt alleen veilige builds naar zijn productieomgeving.
- Auditing en monitoring
  - Om automatisch een aanvaardbaar beveiligingsniveau te handhaven, monitort de Verwerker zijn platform doorlopend op het volgende: SSL-certificaten voor de API; AWS-audittrail voor toegang tot resources; toegang tot resources op serverniveau; toegang tot databaseverbindingen.
- De gegevens zijn alleen toegankelijk voor de systeemengineers en medewerkers die uitdrukkelijk toegang hebben gekregen en zijn getraind om de gegevens in te zien.
- De communicatie tussen de mobiele applicatie en de API van het Epassi Platform verloopt via een HTTPS-verbinding en het authenticatie- en autorisatieproces is beveiligd met JWT (JSON Web Token).
- Hardware van medewerkers is aangemeld in JAMF MDM en is versleuteld, op afstand toegankelijk en kan bij verlies of schade worden vergrendeld en gewist. De Verwerker gebruikt voor zijn klantgerichte diensten een doorlopende kwetsbaarheidsscanner via intruder.io in plaats van periodieke pentests. Dit biedt realtime bescherming tegen nieuwe en zich ontwikkelende CVE's.

2. Organisatorische maatregelen

- Er is een Incident Response Plan dat richting geeft aan medewerkers of incident responders die menen een beveiligingsincident te hebben ontdekt of daarop reageren.
- De Verwerker biedt medewerkers begeleiding en training om phishing en social engineering te herkennen.
- Medewerkers van de Verwerker hebben alleen toegang tot persoonsgegevens indien en zodra daarvoor toestemming is verleend.
- Er is een exitprocedure. Deze beschrijft de stappen om de toegang tot de verschillende systemen en kantoren technisch te blokkeren, zodat een voormalig medewerker zich geen ongewenste toegang tot deze systemen kan verschaffen.
- Intern informatiebeveiligingsbeleid. De volgende beveiligingsrichtlijnen gelden voor alle medewerkers:
  - Google Workspace 2FA / MFA is verplicht en moet binnen 24 uur na aanmaak van het medewerkersaccount zijn ingesteld;
  - Gebruik altijd Google SSO om in te loggen op andere accounts en schakel 2FA / MFA in;
  - Beveilig je werklaptop en telefoon met een wachtwoord en laat deze niet ontgrendeld/open en onbeheerd achter;
  - Laat geen wachtwoorden of belangrijke notities op papier in het kantoor achter;
  - Sta geen onbevoegde toegang tot het kantoor toe;
  - Sla alle wachtwoorden en gevoelige gegevens op in 1password;
  - Wees alert op phishing- en oplichtingspogingen. Klik niet op verdachte links;
  - Deel wachtwoorden niet in leesbare tekst via e-mail, sms of Slack. Gebruik in plaats daarvan 1password;
  - Sla geen gevoelige klantgegevens (e-mailadressen, namen, andere persoonsgegevens) op op je persoonlijke apparaten.