

Overeenkomst inzake Gegevensverwerking

Versie 1.1 - augustus 2026

Deze overeenkomst inzake gegevensverwerking ("**DPA**") wordt aangegaan tussen:

- 1) **De klant**, optredend als **verwerkingsverantwoordelijke**; en
- 2) **Secutec BV**, een vennootschap naar Belgisch recht, met maatschappelijke zetel te Boomsesteenweg 41/11, 2630 Aartselaar, België, ondernemingsnummer 0875.719.463 ("Secutec"), optredend als **verwerker**.

De Klant en Secutec zijn elk een "**Partij**" en samen de "**Partijen**".

Deze DPA vormt een integraal onderdeel van de Overeenkomst tussen de Partijen en regelt de Verwerking van Persoonsgegevens door Secutec namens de Klant.

1 Definities

Alle termen met een hoofdletter die hierin niet worden gedefinieerd, hebben de betekenis die daaraan in de Overeenkomst wordt gegeven.

- "**Gelieerde onderneming**" betekent elke entiteit die zeggenschap heeft over, onder zeggenschap staat van of onder gezamenlijke zeggenschap staat met een Partij.
- **Onder "Overeenkomst"** wordt verstaan de overeenkomst tussen de Klant en Secutec voor de levering van producten en diensten van Secutec.
- "**Persoonsgegevens van de klant**" betekent persoonsgegevens die door Secutec als verwerker namens de klant worden verwerkt in het kader van de overeenkomst.
- "**Gegevensbeschermingswetgeving**" betekent de AVG en alle toepasselijke Belgische en EU-wetgeving die deze aanvult of implementeert.
- "**Verzoek van de betrokkene**" betekent een verzoek van een betrokkene om zijn rechten uit hoofde van de AVG uit te oefenen.
- "**Subverwerker**" betekent elke derde partij die door Secutec is ingeschakeld om persoonsgegevens van klanten te verwerken.
- Termen zoals "**verwerkingsverantwoordelijke**", "**verwerker**", "**verwerking**", "**persoonsgegevens**", "**inbreuk in verband met persoonsgegevens**", "**toezichthoudende autoriteit**", enz. hebben de betekenis die daaraan wordt gegeven in de AVG.

2 Toepassingsgebied van de DPA

Deze DPA is van toepassing op alle verwerkingen die Secutec uitvoert in verband met de door de klant gebruikte diensten. De verwerkingsactiviteiten die van toepassing zijn op alle klanten, ongeacht welke diensten zij afnemen, worden beschreven in **bijlage A – SecureSIGHT-platform en mobiele app**.

In geval van tegenstrijdigheid tussen deze DPA en enig ander contractueel document, prevaleert deze DPA met betrekking tot gegevensbeschermingskwesties. Deze DPA regelt uitsluitend de verwerking van persoonsgegevens van klanten. De verwerking van geanonimiseerde of geaggregeerde gegevens die niet langer betrekking hebben op een identificeerbare persoon valt buiten het toepassingsgebied van deze DPA.

3 Rollen van de partijen

De klant treedt op als verwerkingsverantwoordelijke en bepaalt de doeleinden en middelen van de verwerking van persoonsgegevens van klanten in het kader van de overeenkomst.

Secutec treedt op als gegevensverwerker en verwerkt de persoonsgegevens van de klant uitsluitend op basis van gedocumenteerde instructies van de klant, tenzij de toepasselijke wetgeving anders voorschrijft.

Wanneer Secutec geaggregeerde en/of geanonimiseerde gegevens verwerkt die redelijkerwijs niet opnieuw kunnen worden geïdentificeerd, rekening houdend met de beschikbare middelen, kosten, tijd en technologie, treedt Secutec op als onafhankelijke verwerkingsverantwoordelijke voor doeleinden zoals dreigingsinformatie, statistische analyse, serviceoptimalisatie, beveiligingsonderzoek en platformanalyse.

Een dergelijke verwerking valt onder de eigen privacyverklaring van Secutec en heeft geen betrekking op persoonsgegevens van klanten in de zin van deze DPA.

4 Gedocumenteerde instructies

Secutec zal de persoonsgegevens van de klant strikt verwerken in overeenstemming met de gedocumenteerde instructies van de klant, tenzij anders vereist door de wetgeving van de EU of een lidstaat.

Als Secutec van mening is dat een instructie in strijd is met de wetgeving inzake gegevensbescherming, zal Secutec de klant hiervan op de hoogte stellen en kan Secutec de betreffende verwerking opschorten.

Secutec is niet verplicht om te beoordelen of het gebruik van de diensten door de klant in overeenstemming is met de wetgeving inzake gegevensbescherming.

5 Vertrouwelijkheid

Secutec zorgt ervoor dat alle personen die bevoegd zijn om persoonsgegevens van klanten te verwerken, onderworpen zijn aan passende geheimhoudingsverplichtingen, hetzij contractueel, hetzij wettelijk.

6 Beveiligingsmaatregelen

Secutec implementeert en handhaaft de technische en organisatorische beveiligingsmaatregelen die worden beschreven in **Bijlage B – Technische en organisatorische beveiligingsmaatregelen**, die van toepassing zijn op alle verwerking in het kader van deze DPA.

De Klant erkent dat deze maatregelen een beveiligingsniveau bieden dat in verhouding staat tot het risico, rekening houdend met de stand van de techniek, de implementatiekosten en de aard van de Verwerking (art. 32 AVG).

7 Subverwerking

7.1 Algemene machtiging

De Klant verleent Secutec een algemene machtiging om Subverwerkers in te schakelen voor de Verwerking van Persoonsgegevens van Klanten in verband met de Diensten.

Bijlage C - Subverwerkers beschrijft op categorisch niveau de soorten subverwerkers die door Secutec kunnen worden ingeschakeld, zonder individuele leveranciers te noemen, wat een weerspiegeling is van het leveranciersafhankelijke en evoluerende karakter van cyberbeveiligingstechnologieën. Omwille van de transparantie houdt Secutec een indicatieve lijst van subverwerkers bij met voorbeelden van subverwerkers die momenteel worden gebruikt bij de levering van zijn diensten.

Deze lijst wordt uitsluitend ter informatie verstrekt en maakt geen deel uit van deze gegevensverwerkingsovereenkomst. De lijst van subverwerkers kan van tijd tot tijd worden bijgewerkt om rekening te houden met technologische ontwikkelingen, infrastructuurwijzigingen of serviceverbeteringen.

Subverwerkers worden ingeschakeld en beheerd in overeenstemming met de principes die zijn uiteengezet in dit artikel 7 en bijlage C (Subverwerkers).

Secutec kan subverwerkers aanstellen, vervangen of verwijderen indien dit nodig is om de diensten te leveren, de veiligheid te handhaven, de continuïteit van de dienstverlening te waarborgen of te voldoen aan toepasselijke wettelijke of regelgevende vereisten.

7.2 Kennisgeving en bezwaar

Secutec stelt de Klant informatie ter beschikking over wijzigingen in de categorieën van Subverwerkers die worden ingeschakeld voor de Verwerking van Persoonsgegevens van Klanten.

De Klant kan bezwaar maken tegen dergelijke wijzigingen op redelijke en gedocumenteerde gronden met betrekking tot gegevensbescherming, rekening houdend met de aard van de Diensten en de rol van Subverwerkers binnen de beveiligingsactiviteiten van Secutec.

Wanneer bezwaar wordt gemaakt, zullen de Partijen de kwestie te goeder trouw bespreken. Als er geen redelijk alternatief kan worden overeengekomen, kan de Klant alleen het betreffende deel van de Diensten beëindigen, zonder recht op schadevergoeding, vrijwaring of boetes in verband met een dergelijke beëindiging.

Wijzigingen die nodig zijn om redenen van beveiliging, incidentrespons, continuïteit van de dienstverlening of naleving kunnen onmiddellijk worden doorgevoerd. In dergelijke gevallen zal Secutec de Klant zonder onnodige vertraging op de hoogte brengen.

7.3 Verplichtingen en aansprakelijkheid van subverwerkers

Secutec zorgt ervoor dat elke ingeschakelde subverwerker onderworpen is aan gegevensbeschermingsverplichtingen die niet minder bescherming bieden dan die welke in deze DPA zijn vastgelegd, met inbegrip van passende technische en organisatorische beveiligingsmaatregelen.

Secutec blijft volledig aansprakelijk voor de prestaties van zijn subverwerkers in overeenstemming met deze DPA, in dezelfde mate als wanneer de verwerking rechtstreeks door Secutec zou worden uitgevoerd.

Secutec blijft volledig aansprakelijk voor de handelingen en nalatigheden van zijn subverwerkers in dezelfde mate als wanneer hij de verwerking zelf zou uitvoeren.

8 Internationale gegevensoverdrachten

Persoonsgegevens met betrekking tot verkeer afkomstig uit de EU worden voornamelijk binnen de Europese Unie verwerkt.

Wanneer verwerking buiten de Europese Economische Ruimte vereist is voor het leveren van de diensten, worden dergelijke overdrachten uitgevoerd in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming en onderworpen aan passende waarborgen, waaronder standaardcontractbepalingen of andere geldige overdrachtsmechanismen.

9 Bijstand aan de klant

Secutec zal de klant, voor zover redelijkerwijs mogelijk, bijstaan met:

- het reageren op verzoeken van betrokkenen; Secutec zal niet rechtstreeks reageren op verzoeken van betrokkenen, tenzij de klant hiertoe uitdrukkelijk opdracht heeft gegeven.
- het naleven van de artikelen 32 tot en met 36 van de AVG (beveiliging, melding van inbreuken, DPIA, voorafgaand overleg).

Secutec kan redelijke kosten in rekening brengen wanneer de bijstand het normale serviceniveau overschrijdt, op voorwaarde dat Secutec de klant vooraf op de hoogte stelt van deze kosten.

Deze bijstand omvat niet het uitvoeren van juridische beoordelingen, het nakomen van de wettelijke verplichtingen van de klant of het implementeren van organisatorische maatregelen binnen de omgeving van de klant.

10 Auditrechten

De klant kan audits uitvoeren om na te gaan of Secutec deze DPA naleeft, met inachtneming van:

- een voorafgaande schriftelijke kennisgeving van 60 dagen;
- maximaal één audit per 12 maanden;
- audits die tijdens normale kantooruren worden uitgevoerd;
- geen toegang tot de interne financiële informatie van Secutec, gegevens van andere klanten, interne auditrapporten of handelsgeheimen;

Als alternatief kan Secutec aan de auditverplichtingen voldoen door recente ISO 27001-certificaten of externe ISO 27001-auditsamenvattingen te verstrekken.

De klant zorgt ervoor dat een audit de bedrijfsvoering van Secutec niet onredelijk verstoort en dat er geen auditors bij betrokken zijn die directe concurrenten van Secutec zijn.

11 Melding van inbreuken op persoonsgegevens

Secutec zal de klant onverwijld op de hoogte brengen zodra het kennis neemt van een inbreuk op persoonsgegevens die de persoonsgegevens van de klant betreft.

De kennisgeving omvat de aard van de inbreuk, de categorieën van de betrokken gegevens, de waarschijnlijke gevolgen en de maatregelen die zijn genomen of voorgesteld om de inbreuk aan te pakken.

De klant blijft verantwoordelijk voor alle meldingen aan toezichthoudende autoriteiten en betrokkenen, tenzij anders overeengekomen. De klant stelt Secutec onverwijld in kennis zodra hij kennis neemt van een beveiligingsincident dat:

- betrekking heeft op persoonsgegevens waarvoor Secutec als verwerker optreedt; of
- betrekking heeft op vertrouwelijke informatie, inloggegevens, toegangstokens, bewijsstukken, rapporten of andere gegevens die Secutec aan de klant heeft verstrekt.

Een dergelijke kennisgeving omvat, voor zover bekend, een beschrijving van de aard van het incident en de mogelijke gevolgen ervan voor de gegevens of systemen van Secutec.

Niets in deze clausule verplicht de Klant om Secutec op de hoogte te stellen van inbreuken op persoonsgegevens waarvoor de Klant de Verwerkingsverantwoordelijke is, tenzij de gegevens of systemen van Secutec worden beïnvloed.

12 Teruggave en verwijdering van persoonsgegevens

Bij beëindiging van de Overeenkomst worden Persoonsgegevens van Klanten alleen bewaard zolang dat nodig is in overeenstemming met de bewaarprincipes en toepasselijke bewaartermijnen zoals gedefinieerd in Bijlage D – Bewaarprincipes, tenzij een langere bewaartermijn vereist is door de toepasselijke wetgeving of schriftelijk is overeengekomen.

Na afloop van de toepasselijke bewaartermijnen zal Secutec de persoonsgegevens van de klant binnen een redelijke termijn verwijderen of anonimiseren, met uitzondering van versleutelde back-ups die worden overschreven in overeenstemming met het standaard back-uprotatieschema van Secutec.

De klant kan vóór verwijdering om teruggave van persoonsgegevens verzoeken.

13 Aansprakelijkheid

De aansprakelijkheidsbepalingen van de Overeenkomst zijn eveneens van toepassing op deze DPA.

Niets in deze DPA beperkt de rechten van betrokkenen op grond van artikel 82 van de AVG.

14 Toepasselijk recht en jurisdictie

Deze DPA wordt beheerst door het Belgische recht.

Geschillen worden voorgelegd aan de exclusieve bevoegdheid van de rechtbanken van Antwerpen.

15 Hiërarchie

In geval van inconsistentie:

1. heeft deze DPA voorrang op de Overeenkomst;
2. Bijlagen prevaleren boven deze DPA voor zover zij dienstspecifieke Verwerking beschrijven.

In alle andere opzichten prevaleren de bepalingen van deze DPA boven eventuele tegenstrijdige bepalingen in een bijlage.

Om twijfel te voorkomen: bijlagen waarin verwerkingsactiviteiten, subverwerkers of bewaarprincipes worden beschreven, moeten worden geïnterpreteerd in overeenstemming met en onderworpen aan de bepalende bepalingen van deze DPA.

Deze DPA blijft van kracht zolang Secutec persoonsgegevens van klanten verwerkt in het kader van de overeenkomst.

16 Structuur van de bijlagen

De volgende bijlagen vormen een integraal en onlosmakelijk onderdeel van deze gegevensverwerkingsovereenkomst:

Bijlage A – SecureSIGHT-platform en mobiele app

Beschrijft de verwerkingsactiviteiten die inherent zijn aan het SecureSIGHT-platform en de mobiele applicatie, die van toepassing zijn op alle klanten, ongeacht welke diensten zij afnemen.

Bijlage B – Technische en organisatorische beveiligingsmaatregelen (TOM's)

Beschrijft de ISO27001-conforme beveiligingsmaatregelen van Secutec die van toepassing zijn op alle verwerking in het kader van deze DPA.

Bijlage C – Subverwerkers

Beschrijft op categorisch niveau de soorten subverwerkers die door Secutec kunnen worden ingeschakeld bij het leveren van de diensten, in overeenstemming met het algemene autorisatiemodel zoals uiteengezet in artikel 7.

Bijlage D – Bewaarprincipes

Beschrijft de standaardbewaartermijnen voor de verwerking van persoonsgegevens van klanten voor alle diensten.

Bijlage A – SecureSIGHT-platform en mobiele app

Deze bijlage beschrijft de verwerking van persoonsgegevens die wordt uitgevoerd via het SecureSIGHT-platform en de MySecutec app (samen **'het platform'**). Het Platform biedt authenticatie, gebruikersbeheer, dashboards, waarschuwingen en toegang tot de Diensten van Secutec.

Deze bijlage is van toepassing op alle klanten, ongeacht welke diensten zij afnemen, aangezien alle klanten het platform gebruiken voor toegang en accountbeheer.

Termen die hier niet worden gedefinieerd, hebben de betekenis die daaraan wordt gegeven in de DPA.

1 Reikwijdte van de verwerking

Het Platform fungeert als de uniforme toegangslaag voor alle Secutec-modules.

Het platform verwerkt gebruikersgerelateerde, authenticatie-, technische en toegangsgegevens, terwijl de onderliggende modules operationele cyberbeveiligingsgegevens verwerken.

Het platform neemt geen onafhankelijke beslissingen over de operationele beveiligingsgegevens; het geeft deze alleen weer.

Secutec verwerkt alleen de minimale hoeveelheid persoonsgegevens en technische gegevens die nodig zijn om toegang tot en functionaliteit van het platform te bieden, met inbegrip van authenticatiegegevens, toegangslogboeken en operationele metagegevens, strikt beperkt tot dienstverlening, ondersteuning, beveiliging en controleerbaarheid.

2 Rollen van de partijen

2.1 Rol van de verwerker

Secutec treedt op als verwerker van persoonsgegevens die nodig zijn om klanten toegang te bieden tot en functionaliteit van het platform, waaronder:

- Gebruikersaccounts
- Authenticatie en toegangscontrole
- Logging en sessiemetadata
- Toegang tot het dashboard
- Supportchat

2.2 Controlerende rol

Voor analyse, crashdiagnostiek en prestatiebewaking binnen het platform Secutec als onafhankelijke verwerkingsverantwoordelijke.

Deze verwerking wordt uitgevoerd met het oog op:

- de stabiliteit en prestaties te verbeteren
- het oplossen van fouten of crashes

- de kwaliteit van de dienstverlening te waarborgen

Deze verwerking door de verwerkingsverantwoordelijke heeft geen betrekking op operationele gegevens van klanten.

Voor deze verwerking geldt de privacyverklaring van Secutec.

3 Categorieën van persoonsgegevens

Het platform verwerkt de volgende categorieën persoonsgegevens:

3.1 Gebruikersaccountgegevens

- Volledige naam
- E-mailadres
- Organisatie / huurder
- Gebruikersrollen en machtigingen
- Gekoppelde modules en serviceconfiguratie

3.2 Authenticatie en beveiligingsgegevens

- E-mail + gehashte wachtwoord
- MFA/OTP-verificatiegegevens
- Authenticatietijdstempels
- Sessie-ID's
- Logboeken van inlogpogingen
- IP-adres bij aanmelding

3.3 Technische en apparaatgegevens

- Type apparaat, OS-versie, model van het apparaat
- App-versie
- Metadata van browser of app
- Prestatiestatistieken
- Metadata voor crashdiagnostiek
- Er worden geen geolocatiegegevens verzameld.

3.4 Pushmeldingsgegevens

Het platform kan pushmeldingen versturen. Hiervoor worden meldingstokens verwerkt.

3.5 Gebruiksgegevens

- Schermweergaven
- Navigatiegebeurtenissen
- Gebruik van functies

- Sessieduur

3.6 Ondersteunings- en communicatiegegevens

- In-app chatberichten
- tijdstempels en afzender-ID's

3.7 Doeleinden van de verwerking

Persoonsgegevens worden via het platform verwerkt voor de volgende doeleinden:

1. Gebruikersauthenticatie en veilige toegang
2. Op rollen gebaseerde toegangscontrole
3. Weergave van servicedashboards en operationele inzichten
4. Ondersteuning en communicatie
5. Handhaving van beveiliging, logboekregistratie en controleerbaarheid
6. Monitoring van prestaties en detectie van fouten (controllerrol)

Er worden geen persoonsgegevens gebruikt voor marketing of niet-gerelateerde profilering.

4 Subverwerkers

Bij de verwerkingsactiviteiten in het kader van deze bijlage kan gebruik worden gemaakt van subverwerkers, zoals beschreven op categorisch niveau in bijlage C (Subverwerkers).

Bijlage C identificeert de soorten en categorieën subverwerkers die door Secutec kunnen worden ingeschakeld in het kader van de diensten, zonder individuele leveranciers te vermelden.

Subverwerkers kunnen worden ingeschakeld, vervangen of bijgewerkt in overeenstemming met artikel 7 van de DPA, rekening houdend met het leveranciersafhankelijke en evoluerende karakter van cyberbeveiligingstechnologieën.

5 Bewaartermijnen

Alle bewaartermijnen die van toepassing zijn op persoonsgegevens die in het kader van deze bijlage worden verwerkt, worden uitsluitend geregeld door bijlage D (Bewaarprincipes).

Deze bijlage beschrijft de categorieën persoonsgegevens die via het platform worden verwerkt, maar definieert of wijzigt geen bewaartermijnen.

Bijlage D vormt de enige bron van waarheid voor bewaartermijnen die van toepassing zijn op platformgerelateerde persoonsgegevens.

6 Beveiligingsmaatregelen

Alle verwerkingen in het kader van deze bijlage worden beschermd door de technische en organisatorische maatregelen die worden beschreven in **bijlage B (Beveiligingsmaatregelen)**.

Deze omvatten:

- MFA
- Versleuteling tijdens verzending en opslag
- Veilige hosting en isolatie van tenants
- Logging en detectie van afwijkingen

- RBAC
- Beheer van kwetsbaarheden

7 Verantwoordelijkheden van de klant

De klant moet:

- ervoor zorgen dat zijn geautoriseerde gebruikers veilige inloggegevens bijhouden
- toegangsrechten en rollen te beheren
- ervoor zorgen dat de accounts van werknemers die aan het platform zijn gekoppeld, op wettige wijze worden gecontroleerd
- vermijden dat onnodige of buitensporige persoonlijke gegevens worden opgeslagen in ondersteuningskanalen
- zorgen voor veilig gebruik van apparaten die toegang hebben tot het Platform

8 Aanvullende opmerkingen

- Het platform is uitsluitend bedoeld voor B2B-gebruik en niet voor consumenten.
- De app is een aanvullende interface; deze vervangt niet het volledige SecureSIGHT-webplatform.
- Functies voor identiteitsvervalsing zijn voorbehouden aan geautoriseerde partners.

Bijlage B – Technische en organisatorische beveiligingsmaatregelen

Secutec implementeert de volgende technische en organisatorische maatregelen ("TOM's") om een beveiligingsniveau te waarborgen dat passend is voor het risico dat verbonden is aan de verwerking van persoonsgegevens van klanten, in overeenstemming met artikel 32 van de AVG.

Deze maatregelen zijn van toepassing op alle diensten, tenzij aanvullende dienstmaatregelen worden toegevoegd in aanvullende bijlagen.

1 Informatiebeveiligingsbeheersysteem (ISMS)

1.1 ISO 27001-kader

Secutec hanteert een formeel informatiebeveiligingsbeheersysteem (ISMS) dat is afgestemd op de ISO/IEC 27001-norm.

Het ISMS regelt de aanpak van Secutec met betrekking tot de vertrouwelijkheid, integriteit en beschikbaarheid van informatieactiva.

1.2 Gedocumenteerd beleid

Het ISMS wordt ondersteund door een uitgebreide reeks gedocumenteerde beleidsregels, waaronder (niet-uitputtend):

- Beleid inzake informatiebeveiliging
- Toegangscontrolebeleid
- Beleid inzake netwerkbeveiliging
- Beleid inzake operationele beveiliging
- Beleid inzake cryptografie en sleutelbeheer
- Beleid inzake personeelsbeveiliging
- Beleid inzake activabeheer
- Beleid inzake bedrijfscontinuïteit en noodherstel
- Beleid inzake fysieke beveiliging
- Beleid inzake leveranciers- en derdepartijenbeheer
- Beleid inzake veilige ontwikkeling en veranderingsbeheer
- Beleid inzake incidentbeheer
- Beleid inzake naleving
- Beleid inzake ISMS-governance en risicobeoordeling

Dit interne beleid maakt geen deel uit van de overeenkomst en kan van tijd tot tijd worden bijgewerkt in het kader van voortdurende verbetering volgens ISO 27001.

1.3 Bewijs van naleving

Op verzoek van de klant kan Secutec bewijs van ISMS-implementatie leveren, zoals:

- ISO/IEC 27001-certificaten en scopeverklaringen,
- samenvattende auditrapporten,
- nalevingsverklaringen.

Interne beleidsdocumenten en gevoelige operationele details worden om veiligheidsredenen niet volledig gedeeld.

2 Toegangscontrolemaatregelen

2.1 Principe van minimale rechten

Toegang tot persoonlijke gegevens van klanten wordt uitsluitend verleend op basis van een 'need-to-know'-basis.

2.2 Authenticatie en autorisatie

Voor administratieve toegang is meervoudige authenticatie vereist.

Er worden unieke gebruikersidentiteiten afgedwongen.

Toegangsrechten worden periodiek herzien.

2.3 Onmiddellijke intrekking

De toegang wordt onmiddellijk ingetrokken bij een functiewijziging of beëindiging van het dienstverband.

3 Fysieke en omgevingsbeveiliging

Persoonsgegevens van klanten worden voornamelijk gehost in beveiligde, professioneel beheerde datacenters van gecertificeerde cloudproviders in de EER.

Wanneer verwerking buiten de EER vereist is, worden passende waarborgen toegepast in overeenstemming met de DPA en de toepasselijke wetgeving inzake gegevensbescherming.

Datacenters bieden fysieke toegangscontrole, milieubescherming, branddetectie, redundantie en 24/7 bewaking.

4 Versleuteling en gegevensbescherming

Versleuteling tijdens verzending: alle communicatiekanalen die worden gebruikt om persoonlijke gegevens van klanten over te dragen, zijn beveiligd met TLS 1.2+ of gelijkwaardig.

Versleuteling in rust: logbestanden, DNS-gegevens en servicegegevens worden in rust versleuteld met behulp van algoritmen die aan de industriestandaarden voldoen.

Cryptografische sleutels worden veilig beheerd.

5 Netwerkbeveiliging

Secutec past netwerksegmentatie, firewalls en inbraakdetectie-/preventiesystemen toe.

DNS- en servicespecifiek verkeer wordt gecontroleerd op afwijkingen en kwaadaardige activiteiten.

Anti-DDoS-beveiligingen en mechanismen voor snelheidsbeperking beschermen de beschikbaarheid van de dienst.

6 Operationele beveiliging

Voor intern ontwikkelde componenten worden veilige coderingspraktijken en peer review toegepast.

Alle systemen worden regelmatig gescand op kwetsbaarheden en patches worden toegepast op basis van ernst.

Het loggen van beveiligingsrelevante gebeurtenissen wordt centraal bijgehouden en gecontroleerd. Toegang tot persoonlijke gegevens van klanten wordt gelogd en de logs worden regelmatig gecontroleerd.

Back-upprocedures zorgen ervoor dat gegevens kunnen worden hersteld; back-ups worden versleuteld.

7 Detectie van en reactie op incidenten

Secutec hanteert een incidentresponsplan dat voldoet aan de ISO 27001- en NIS2-normen.

Beveiligingsincidenten worden onmiddellijk onderzocht, gedocumenteerd en ingeperkt.

In geval van een inbreuk op persoonsgegevens die van invloed is op de persoonsgegevens van klanten, zal Secutec de klant zonder onnodige vertraging op de hoogte stellen, zoals vereist op grond van artikel 11 van de DPA.

8 Bedrijfscontinuïteit en noodherstel

De diensten worden voornamelijk geïmplementeerd in een redundante cloudinfrastructuur binnen de EER.

Rampenherstelprocedures worden periodiek getest.

Kritieke systemen worden 24/7 gemonitord op prestaties en beschikbaarheid.

9 Beheer van leveranciers en subverwerkers

Subverwerkers worden vóór hun aanstelling beoordeeld op hun beveiligingsbeleid.

Alleen subverwerkers met de juiste certificeringen (bijv. ISO 27001) worden ingeschakeld.

Contracten met subverwerkers bevatten verplichtingen die gelijkwaardig zijn aan die welke door de DPA worden opgelegd.

10 Gegevensminimalisatie en -bewaring

Secutec verwerkt alleen de minimale hoeveelheid persoonsgegevens en technische gegevens die nodig is om de diensten te leveren in overeenstemming met deze overeenkomst.

Dergelijke gegevens kunnen door de klant verstrekte gegevens, operationele beveiligingsgegevens, authenticatie- en toegangsgegevens, waarschuwingsmetadata en openbaar beschikbare informatie omvatten, strikt beperkt tot wat nodig is voor dienstverlening, onderzoek, rapportage en beveiligingsactiviteiten.

Het bewaren van dergelijke gegevens wordt uitsluitend geregeld door bijlage D (Bewaarprincipes).

11 Testen en voortdurende verbetering

Er worden periodiek beveiligingstests uitgevoerd.

De bevindingen worden bijgehouden en op basis van het risico verholpen.

De TOM's worden ten minste eenmaal per jaar herzien en indien nodig bijgewerkt.

Bijlage C – Subverwerkers

1 Toepassingsgebied

Deze bijlage identificeert de categorieën van subverwerkers die door Secutec worden ingeschakeld voor de verwerking van persoonsgegevens van klanten in het kader van de overeenkomst.

Secutec hanteert een leveranciersafhankelijk, best-of-breed technologiemodel en kan verschillende subverwerkers inschakelen, afhankelijk van de aangeschafte diensten, geactiveerde modules, klantspecifieke configuraties en de ontwikkeling van cyberbeveiligingstechnologieën in de loop van de tijd.

2 Subverwerkers voor kerninfrastructuur

Secutec maakt gebruik van cloudinfrastructuur en hostingproviders voor het leveren van platformcomponenten, logpijplijnen, opslag en rekencapaciteit.

Dergelijke subverwerkers bieden veilige hosting-, opslag- en beschikbaarheidsdiensten en worden geselecteerd op basis van beveiligingscertificeringen, naleving van regelgeving en regionale beschikbaarheid.

De verwerking vindt voornamelijk plaats binnen de Europese Economische Ruimte, voor zover dit operationeel haalbaar is. Wanneer verwerking buiten de EER vereist is, worden passende waarborgen toegepast in overeenstemming met de DPA en de toepasselijke wetgeving inzake gegevensbescherming.

3 MySecutec-platform en mobiele app-subverwerkers

Het SecureSIGHT-platform en de mobiele applicatie zijn afhankelijk van infrastructuur-, analyse- en mobiele serviceproviders voor het leveren van authenticatie, dashboards, meldingen en applicatiefunctionaliteit.

Deze subverwerkers verwerken alleen persoonsgegevens op platformniveau, zoals beschreven in bijlage A, en verwerken geen operationele beveiligingsgegevens die door de diensten worden gegenereerd, tenzij dit uitdrukkelijk is overeengekomen.

Informatie over de categorieën van ingeschakelde subverwerkers wordt beschikbaar gesteld in overeenstemming met artikel 7 van de DPA.

4 SecureDNS-subverwerkers

SecureDNS maakt gebruik van infrastructuurproviders, DNS-resolvercomponenten en beveiligingsanalyse-engines om DNS-beveiligingsdiensten te leveren.

Subverwerkers verwerken DNS-metadata en beveiligingstelemetrie die nodig zijn voor het detecteren, filteren en rapporteren van bedreigingen, in overeenstemming met de overeenkomst en de toepasselijke waarborgen.

5 SecureSIGHT-subverwerkers (modules)

SecureSIGHT-modules kunnen gebruikmaken van externe technologieleveranciers om specifieke functionaliteiten te leveren, zoals detectie-engines, dreigingsinformatie, correlatie of verrijkdiensten.

Dergelijke subverwerkers verwerken beperkte beveiligingsgerelateerde metadata in overeenstemming met de overeenkomst.

De toepasselijke subverwerkers zijn afhankelijk van de geactiveerde modules en de configuratie van de klant en kunnen worden bijgewerkt in overeenstemming met artikel 7 van de DPA.

6 Klant-specifieke subverwerkers

Wanneer de klant integraties met zijn eigen leveranciers aanvraagt of activeert (bijv. door de klant geleverde XDR, SIEM, Darknet-informatie, AD-connectoren):

- kunnen dergelijke tools van derden functioneren als subverwerkers of afzonderlijke verwerkingsverantwoordelijken,
- De klant is ervoor verantwoordelijk dat zijn overeenkomsten met dergelijke leveranciers Secutec toegang en verwerking toestaan.

Secutec neemt geen verplichtingen op zich ten opzichte van door de klant geselecteerde leveranciers.

7 Wijzigingen in subverwerkers

Subverwerkers kunnen worden bijgewerkt in overeenstemming met artikel 7 van de DPA.

De klant erkent dat cybersecuritytechnologiestacks voortdurend evolueren en dat Secutec subverwerkers kan toevoegen, vervangen of verwijderen om de kwaliteit, veiligheid en naleving van de dienstverlening te handhaven.

8 Illustratieve lijst van huidige subverwerkers

De volgende lijst bevat **voorbeelden van subverwerkers die momenteel worden gebruikt** bij de levering van Secutec-diensten.

Deze lijst is indicatief en niet uitputtend. Subverwerkers kunnen in de loop van de tijd veranderen in overeenstemming met artikel 7 van deze DPA.

Categorie	Voorbeelden van subverwerkers	Doel
Cloudinfrastructuur	OVHcloud	Veilige hosting van componenten van het Secutec-platform
Infrastructuur Applicatiehosting	/ DigitalOcean	Hosting van platformdiensten
Leveranciers van cyberbeveiligingstechnologie	SentinelOne	XDR-beveiligingsengine
Mobiele applicatieservices	OneSignal	Pushmeldingsdiensten
Applicatiebewaking	Sentry	Foutbewaking en diagnostiek
Analytics	Google Firebase	Platformanalyse en crashdiagnostiek

Bijlage D – Retentieprincipes

1 Bewaarprincipes

De in deze bijlage gedefinieerde bewaartermijnen zijn indicatief en gebaseerd op operationele noodzaak, vereisten voor dienstverlening en branchepraktijken voor cyberbeveiligingsdiensten.

Bewaartermijnen kunnen per gegevenscategorie verschillen en worden bepaald in overeenstemming met het interne bewaarbeleid van Secutec en de toepasselijke contractuele documentatie.

Indien nodig kunnen de bewaartermijnen in onderling overleg tussen de partijen worden aangepast.

2 Doel en reikwijdte

Deze bijlage beschrijft de standaard bewaartermijnen die van toepassing zijn op de persoonsgegevens van klanten die door Secutec worden verwerkt in het kader van de overeenkomst.

Deze bewaartermijnen zijn van toepassing tenzij in een bestelformulier of werkverklaring uitdrukkelijk een andere termijn is overeengekomen, of een langere bewaartermijn vereist of toegestaan is door de toepasselijke wetgeving.

Secutec verwijdert of anonimiseert persoonsgegevens van klanten na het verstrijken van de toepasselijke bewaartermijnen in overeenstemming met artikel 12 van de DPA.

3 Algemene beginselen

Persoonsgegevens worden alleen bewaard zolang dat nodig is voor detectie, monitoring, onderzoek, rapportage, controleerbaarheid en continuïteit van de dienstverlening.

Bewaartermijnen worden bepaald op basis van operationele noodzaak, wettelijke verplichtingen en erkende praktijken in de sector voor cyberbeveiliging en beheerde beveiligingsdiensten.

Wanneer persoonsgegevens niet langer nodig zijn voor deze doeleinden, worden ze verwijderd of onomkeerbaar geanonimiseerd in overeenstemming met deze bijlage.

4 SecureSIGHT-platform en mobiele app

Platformgerelateerde persoonsgegevens, waaronder gebruikersaccountgegevens, authenticatielogboeken, toegangsmetadata, ondersteuningscommunicatie en applicatiediagnostiek, worden bewaard gedurende de periode die nodig is om de functionaliteit, ondersteuning, beveiliging en controleerbaarheid van het platform te waarborgen.

De bewaartermijnen kunnen variëren afhankelijk van de gegevenscategorie en worden bepaald in overeenstemming met het interne bewaarbeleid van Secutec en de toepasselijke contractuele documentatie.

5 SecureDNS

SecureDNS verwerkt DNS-query-metadata, beveiligingsgebeurtenissen, risicoclassificaties en rapportagegegevens die nodig zijn om DNS-beveiligingsdiensten te leveren.

Operationele DNS-gegevens worden bewaard gedurende een beperkte periode die nodig is voor beveiligingsanalyses, incidentonderzoek en rapportage.

Geaggregeerde rapportagegegevens en incidentgerelateerde artefacten kunnen voor een langere periode worden bewaard ter ondersteuning van serviceraportage, onderzoek en verplichtingen jegens klanten.

6 SecureSIGHT-modules

SecureSIGHT-modules, waaronder maar niet beperkt tot XDR, Leaked Credentials & Darknet Monitoring, Active Threat Hunting, Microsoft 365 Monitoring, Third-Party Risk Management en Attack Surface Management, verwerken beveiligingsgerelateerde metadata, waarschuwingen, bevindingen en contextuele informatie.

Dergelijke gegevens worden alleen bewaard zolang dat nodig is om de dienstverlening, het onderzoek, de rapportage en de nalevingsverplichtingen te ondersteunen, in overeenstemming met het interne bewaarbeleid van Secutec en de toepasselijke contractuele documentatie.

7 Consultancy, pentesting en incidentrespons

Gegevens die worden gegenereerd in het kader van consultancy, penetratietesten en incidentresponsdiensten worden bewaard gedurende de periode die nodig is om de overeengekomen diensten te leveren, onderzoek, rapportage en evaluatie na incidenten te ondersteunen.

Indien nodig kunnen dergelijke gegevens voor een langere periode worden bewaard ter ondersteuning van wettelijke, regelgevende of contractuele verplichtingen, of totdat de zaak is afgesloten plus een redelijke periode na afsluiting.

8 Back-ups

Back-upkopieën kunnen gedurende een beperkte periode worden bewaard in overeenstemming met het standaard back-uprotatieschema van Secutec.

Back-ups bevatten versleutelde kopieën van productiesystemen en kunnen niet selectief worden gewijzigd of verwijderd.

9 Verwijdering na beëindiging van de overeenkomst

Na beëindiging van de overeenkomst zal Secutec de persoonsgegevens van de klant binnen een redelijke termijn verwijderen of anonimiseren, behalve wanneer:

- een langere bewaartermijn vereist of toegestaan is volgens de toepasselijke wetgeving; of
- de gegevens in gecodeerde back-ups blijven bestaan totdat ze worden overschreven in overeenstemming met de standaard back-uprotatieschema's.

Bewaartermijnen kunnen worden verlengd indien dit nodig is om rechtsvorderingen in te stellen, uit te oefenen of te verdedigen.

Indien dit technisch en juridisch haalbaar is, kan Secutec voldoen aan redelijke verzoeken van klanten om specifieke gegevenssets vroegtijdig te verwijderen.