Versie: 1.2 / november 2026

Verwerkers-overeenkomst IT aanspreekpunt

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

NLdigital versie maart 2025

Deel 1: Data Pro Statement

Dit Data Pro Statement vormt, tezamen met de Standaardclausules voor verwerkingen, de verwerkersovereenkomst voor het product of de dienst van de organisatie die dit Data Pro Statement heeft opgesteld.

Begrippen in gewone taal

Dit Data Pro Statement gebruikt een aantal begrippen uit de privacywetgeving. Hieronder staat in gewone taal wat ze betekenen.

Opdrachtgever: de klant van IT aanspreekpunt. In de Overeenkomst Managed Services heet opdrachtgever "jij"; het gaat om dezelfde partij.

Overeenkomst: de hoofdovereenkomst tussen opdrachtgever en IT aanspreekpunt, meestal de Overeenkomst Managed Services.

AVG: de Algemene verordening gegevensbescherming, de Europese privacywet.

Verwerkingsverantwoordelijke: de partij die bepaalt waarom en hoe persoonsgegevens worden gebruikt. Dat is meestal opdrachtgever.

Verwerker (data processor): de partij die persoonsgegevens verwerkt in opdracht van de verwerkingsverantwoordelijke. Dat is hier IT aanspreekpunt.

Subverwerker (sub-processor): een andere partij die IT aanspreekpunt inschakelt en die daarbij persoonsgegevens van opdrachtgever verwerkt, bijvoorbeeld een leverancier van cloudopslag. Alle subverwerkers staan in de Lijst van subverwerkers.

Betrokkene: de persoon over wie de persoonsgegevens gaan, bijvoorbeeld een medewerker of klant van opdrachtgever.

EU/EER: de Europese Unie en de Europese Economische Ruimte (de EU plus IJsland, Liechtenstein en Noorwegen). Daar geldt overal de AVG.

Doorgifte: het verwerken van persoonsgegevens buiten de EU/EER, of het beschikbaar maken ervan voor een partij daar.

Passende waarborg: een wettelijk erkende manier om persoonsgegevens buiten de EU/EER te beschermen: een adequaatheidsbesluit, het EU-VS Data Privacy Framework (DPF) of standaardcontractbepalingen (SCC's). Deze staan uitgelegd in de Lijst van subverwerkers.

DPIA: Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling): een risicoanalyse die de AVG in sommige gevallen verplicht stelt.

Datalek: een inbreuk in verband met persoonsgegevens, bijvoorbeeld wanneer persoonsgegevens verloren gaan of bij onbevoegden terechtkomen.

Technische termen: RBAC is rolgebaseerde toegang: medewerkers kunnen alleen bij wat voor hun rol nodig is. TLS is versleuteling van verbindingen. EDR is software die verdachte activiteit op apparaten opspoort en direct reageert. ITDR bewaakt inlogs en accounts op misbruik. SIEM controleert logbestanden centraal op verdachte patronen. IDS/IPS spoort verdacht netwerkverkeer op en houdt het tegen. Een NAS is een apparaat voor netwerkopslag en back-ups.

Algemene informatie

1. **Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):**
   IT aanspreekpunt B.V.
   Jaargetijdenweg 3D
   7532 SX te Enschede

   Voor vragen over dit Data Pro Statement of over gegevensbescherming kan opdrachtgever contact opnemen met:
   De heer Tom Koelemij
   053 203 21 53
   info@itaanspreekpunt.nl

2. **Dit Data Pro Statement geldt vanaf 5 juni 2026 (herzien november 2026, versie 1.2)**
   Wij passen dit Data Pro Statement en de daarin beschreven beveiligingsmaatregelen periodiek aan, zodat deze in lijn blijven met actuele wet- en regelgeving, technologische ontwikkelingen en onze dienstverlening. Nieuwe versies communiceren wij via onze gebruikelijke kanalen.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van IT aanspreekpunt**
   a **Managed Services (alle modules uit de Overeenkomst Managed Services, waaronder het pakket Totale ontzorging)**: inclusief support, monitoring, proactief beheer en onderhoud van de IT-infrastructuur
   https://itaanspreekpunt.nl/totale-ontzorging/
   https://itaanspreekpunt.nl/diensten/onbeperkte-ict-helpdesk/
   https://itaanspreekpunt.nl/diensten/monitoring-en-updates/
   b **Cloud- en werkplekdiensten**: Microsoft 365-beheer, cloudbeheer, licentiemanagement, migratie en optimalisatie
   https://itaanspreekpunt.nl/diensten/microsoft-365-abonnement/
   https://itaanspreekpunt.nl/sharepoint-specialist/
   https://itaanspreekpunt.nl/diensten/automatische-email-handtekening/
   c **Securitydiensten**: endpoint protection, EDR, bewaking van Microsoft 365-identiteiten (ITDR), logmonitoring (SIEM), e-mailbeveiliging, antivirus, content filtering en wachtwoordmanager
   https://itaanspreekpunt.nl/ict-beveiliging-mkb/
   https://itaanspreekpunt.nl/microsoft-365-beveiliging/

https://itaanspreekpunt.nl/diensten/cybersecurity/
https://itaanspreekpunt.nl/diensten/wachtwoordmanager/

d **Back-up en recovery**: Microsoft 365 back-up (NinjaOne SaaS-back-up, voorheen Dropsuite), back-up van servers op een Synology-NAS met een kopie naar cloudopslag (Backblaze of Impossible Cloud) en disaster-recoveryoplossingen
https://itaanspreekpunt.nl/diensten/cybersecurity/
https://itaanspreekpunt.nl/diensten/monitoring-en-updates/

e **Netwerk- en connectiviteitsdiensten**: netwerkbeheer, internetverbindingen, technisch beheer van camerasystemen, monitoring en updates
https://itaanspreekpunt.nl/diensten/beveiligd-bedrijfsnetwerk/

f **Telefonie**: zakelijke telefonie (Microsoft Teams of een hosted telefooncentrale) en mobiele telefonie

g **Webhosting**: websitehosting, domein- en DNS-beheer en back-ups
https://itaanspreekpunt.nl/diensten/webhosting-domeinregistratie/

h **Digital signage en digitale receptie**: technische inrichting, installatie en ondersteuning van schermen en platform; de bezoekersgegevens van de digitale receptie worden opgeslagen bij de platformleverancier (FrontAssist, zie de Lijst van subverwerkers); IT aanspreekpunt gebruikt die zelf niet, maar kan er bij technische ondersteuning toegang toe hebben

i **Hardwarelevering en onderhoud**: levering van laptops, desktops en randapparatuur met fabrieksgarantie
https://itaanspreekpunt.nl/diensten/zakelijke-werkplek/

j **Advisering en consultancy**: IT-advies, ISO 27001-begeleiding, optimalisatie van IT-omgevingen en SharePoint, en Teamleader CRM-optimalisatie
https://itaanspreekpunt.nl/diensten/versnel-jouw-bedrijfsgroei/
https://itaanspreekpunt.nl/iso-27001-begeleiding/
https://itaanspreekpunt.nl/it-scan/
https://itaanspreekpunt.nl/teamleader-crm-implementatie/

k **Managed Print Services**: IT aanspreekpunt treedt hierbij alleen op als tussenpersoon en verwerkt geen persoonsgegevens

4. **Omschrijving product(en)/dienst(en)**
IT aanspreekpunt levert complete IT-ontzorging aan mkb-organisaties en non-profitinstellingen. De dienstverlening omvat onder meer het beheer, onderhoud, de beveiliging en de optimalisatie van de volledige IT-infrastructuur van opdrachtgever, zowel on-premises als in cloudomgevingen.

Daaronder vallen onder meer de volgende werkzaamheden en diensten:

- **Microsoft 365-beheer**: licentiebeheer, configuratie, gebruikersbeheer en ondersteuning.
- **Endpoint management**: geautomatiseerde updates van Windows- en third-partysoftware, monitoring en ondersteuning op afstand.
- **Beveiliging**: antivirus, content filtering, multifactor-authenticatie en e-mailbeveiliging, en afhankelijk van het afgenomen pakket EDR, bewaking van Microsoft 365-identiteiten (ITDR) en logmonitoring (SIEM).
- **Back-up**: dagelijkse back-ups van Microsoft 365-omgevingen, waaronder SharePoint, OneDrive, Exchange en Teams; bij een eigen server ook back-ups op een Synology-NAS, met een kopie naar cloudopslag.
- **Netwerkbeheer**: beheer en monitoring van UniFi-netwerkapparatuur, firewallconfiguratie en IDS/IPS, en technisch beheer van camerasystemen.
- **Helpdesk en support**: incidentoplossing, reparatie en gebruikersondersteuning via telefoon, e-mail en het selfserviceportaal.

- **Telefonie**: inrichting en beheer van zakelijke en mobiele telefonie, inclusief gebruikersbeheer en nummerbehoud.

Een nadere beschrijving van de dienstverlening is opgenomen in de Overeenkomst Managed Services (Totale ontzorging is daarin een pakket van modules) of in de andere tussen partijen geldende hoofdovereenkomst.

5. Beoogd gebruik

   Product/dienst is ontworpen en ingericht voor de verwerking van de volgende categorieën persoonsgegevens:

   a **NAW-gegevens** (naam, adres, woonplaats)
   b **Contactgegevens** (e-mailadressen, telefoonnummers)
   c **Bedrijfsinformatie en gebruikersgegevens** (gebruikersnamen, functietitels, organisatiestructuur)
   d **Technische gegevens** (IP-adressen, computernamen, serienummers, hardwarespecificaties en geïnstalleerde software)
   e **Log- en monitoringgegevens** (systeemlogboeken, antivirus- en EDR-detecties, netwerkactiviteit)
   f **Aanmeld- en identiteitsgegevens** (aanmeldingen bij Microsoft 365 met tijdstip, IP-adres, apparaat en locatie, bij bewaking van identiteiten)
   g **Communicatiegegevens** (e-mailcommunicatie, helpdesktickets en supportcorrespondentie)
   h **Back-upgegevens** (bestandsopslag, e-mail en SharePoint-documenten, en bij een eigen server de bestanden op die server)
   i **Verkeers- en gespreksgegevens** (bij telefoniediensten: telefoonnummers, datum, tijdstip en duur van gesprekken en dataverbruik)
   j **Contentbestanden** (bij digital signage: door opdrachtgever geüploade afbeeldingen, video's en presentaties)
   k Bezoekersgegevens (bij digitale receptie: zoals naam, bedrijf, contactpersoon en tijdstip van bezoek)
   l **Camerabeelden** (alleen bij incidentele toegang voor technische storingsoplossing, na uitdrukkelijke toestemming van opdrachtgever)

- Bij deze diensten is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, of door de overheid uitgegeven identificatienummers.
- Slaat opdrachtgever toch bijzondere persoonsgegevens op in Microsoft 365 of in een back-up, dan beheert IT aanspreekpunt die omgeving technisch zonder de inhoud te gebruiken; aanvullende maatregelen spreken partijen op verzoek af.
- Opdrachtgever blijft te allen tijde verantwoordelijk voor de beoordeling of het gebruik van de diensten van IT aanspreekpunt passend is voor de persoonsgegevens die via die diensten worden verwerkt.

6. Privacy by design/privacy by default

Bij de inrichting van haar producten en diensten heeft IT aanspreekpunt onder meer de volgende maatregelen toegepast:

a Dataminimalisatie: wij verwerken uitsluitend persoonsgegevens die noodzakelijk zijn voor de uitvoering van onze dienstverlening. Opdrachtgever bepaalt zelf welke gegevens worden aangeleverd.

b Toegangsbeperking: toegang tot persoonsgegevens is beperkt tot geautoriseerde medewerkers voor zover dit noodzakelijk is voor de uitvoering van hun werkzaamheden.
c Encryptie: persoonsgegevens worden, waar passend, versleuteld opgeslagen en verzonden via beveiligde verbindingen (TLS/SSL).
d Multifactor-authenticatie (MFA): waar mogelijk maken wij gebruik van MFA voor toegang tot portalen en systemen.
e Zero Trust: waar mogelijk maken wij gebruik van het Zero Trust principe.

7. **IT aanspreekpunt gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn.**

8. **IT aanspreekpunt verwerkt de persoonsgegevens van zijn opdrachtgevers zoveel mogelijk binnen de EU/EER. Een aantal subverwerkers verwerkt persoonsgegevens (ook) buiten de EU/EER, vooral in de Verenigde Staten. Dat is per subverwerker vermeld in de Lijst van subverwerkers, inclusief de toepasselijke waarborg.**

Indirecte doorgifte buiten de EU/EER via subverwerkers:

Bepaalde door ons ingeschakelde subverwerkers kunnen persoonsgegevens geheel of gedeeltelijk buiten de EU/EER verwerken. Voor zover daarvan sprake is, wordt per subverwerker in de Lijst van subverwerkers IT aanspreekpunt (bijlage bij de Overeenkomst Managed Services en bij deze verwerkersovereenkomst) vermeld of verwerking buiten de EU/EER plaatsvindt en op basis van welke passende waarborg dit gebeurt.

a Adequaatheidsbesluit van de Europese Commissie (de Europese Commissie heeft vastgesteld dat een land buiten de EU/EER, zoals het Verenigd Koninkrijk, persoonsgegevens voldoende beschermt)
b EU-VS Data Privacy Framework (DPF: afspraken tussen de EU en de VS; geldt voor Amerikaanse bedrijven die zich daarbij hebben aangesloten)
c Standard Contractual Clauses (SCC's): standaardcontractbepalingen van de Europese Commissie, afgesloten met subverwerkers buiten de EU/EER

Per subverwerker is in de Lijst van subverwerkers IT aanspreekpunt (bijlage bij de Overeenkomst Managed Services en bij deze verwerkersovereenkomst) opgenomen of persoonsgegevens binnen of buiten de EU/EER worden verwerkt en welke passende waarborgen daarop van toepassing zijn.

9. **IT aanspreekpunt maakt gebruik van subverwerkers:**

Onze subverwerkers staan in de Lijst van subverwerkers IT aanspreekpunt (versie 1.2, november 2026). Die lijst is een bijlage bij de Overeenkomst Managed Services en bij deze verwerkersovereenkomst. De actuele versie stuurt IT aanspreekpunt op verzoek toe.

10. **IT aanspreekpunt ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**

IT aanspreekpunt ondersteunt opdrachtgever hierbij op redelijke verzoeken en binnen de mogelijkheden van de gebruikte systemen.

a Doorverwijzing: indien een betrokkene zich rechtstreeks tot IT aanspreekpunt wendt, sturen wij het verzoek door aan opdrachtgever. Opdrachtgever onderhoudt vervolgens zelf de verdere correspondentie met de betrokkene.
b Technische ondersteuning: via de systemen van IT aanspreekpunt kan opdrachtgever, voor zover de functionaliteit dit toelaat, zelfstandig gegevens exporteren, aanpassen of verwijderen.
c Helpdeskondersteuning: op verzoek van opdrachtgever kunnen wij ondersteuning bieden bij het exporteren, aanpassen of verwijderen van persoonsgegevens. Hiervoor kunnen administratieve kosten in rekening worden gebracht conform de gebruikelijke tarieven.
d Instructietoetsing: indien een instructie van opdrachtgever naar ons oordeel in strijd is met de AVG of andere privacywetgeving, informeren wij opdrachtgever daarover onverwijld voordat wij de instructie uitvoeren.
e Verzoeken van autoriteiten: ontvangen wij een wettelijk bindend verzoek van een (buitenlandse) autoriteit tot verstrekking van persoonsgegevens van opdrachtgever, dan informeren wij opdrachtgever voorafgaand aan de verstrekking, tenzij dit wettelijk verboden is.

11. **IT aanspreekpunt zal op de volgende wijze medewerking verlenen aan Data Protection Impact Assessments (DPIA):**

Indien opdrachtgever daartoe op grond van de AVG verplicht is, verleent IT aanspreekpunt op redelijk verzoek medewerking aan een Data Protection Impact Assessment (DPIA).
Deze medewerking omvat onder meer:

a Het verstrekken van relevante informatie over de aard van de verwerkingen, de getroffen beveiligingsmaatregelen en de ingeschakelde subverwerkers.
b Het beantwoorden van redelijke vragen met betrekking tot risico's en getroffen waarborgen.
c Het meedenken over eventuele aanvullende maatregelen, voor zover dit redelijkerwijs van ons kan worden verlangd.

Indien uitgebreide DPIA-ondersteuning substantiële inspanningen vergt, kan IT aanspreekpunt hiervoor kosten in rekening brengen conform de gebruikelijke tarieven.

12. Na beëindiging van de overeenkomst verwijdert IT aanspreekpunt de persoonsgegevens die zij voor opdrachtgever verwerkt binnen 3 maanden. Back-ups van Microsoft 365 en van servers bewaart IT aanspreekpunt tijdens de overeenkomst volgens het bewaarschema uit de Overeenkomst Managed Services (artikelen 4.3.3 en 4.3.6) of, als die overeenkomst niet geldt, volgens de tussen partijen afgesproken bewaartermijnen, met jaarlijkse back-ups tot 7 jaar. Na beëindiging draagt IT aanspreekpunt de back-ups op verzoek van opdrachtgever over in een gangbaar formaat en verwijdert zij ze daarna binnen dezelfde termijn van 3 maanden. Voor gegevens die door subverwerkers worden verwerkt, geeft IT aanspreekpunt binnen deze termijn opdracht tot verwijdering; daarop is het retentiebeleid van de betreffende subverwerker van toepassing. Een en ander tenzij een wettelijke bewaarplicht of andere geldende verplichting zich daartegen verzet.

13. **Retourneren van persoonsgegevens na beëindiging van de Overeenkomst**

Voorafgaand aan verwijdering stelt IT aanspreekpunt opdrachtgever gedurende een redelijke termijn in de gelegenheid de persoonsgegevens zelf veilig te stellen. Op verzoek ondersteunt IT aanspreekpunt opdrachtgever daarbij tegen de gebruikelijke tarieven. Overige afspraken over het retourneren van persoonsgegevens zijn niet gemaakt.

Beveiligingsbeleid

14. IT aanspreekpunt heeft passende technische en organisatorische beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst.

a Fysieke beveiliging

- Het kantoor van IT aanspreekpunt is voorzien van digitale codesloten.
- Er is cameratoezicht aanwezig.
- Toegang wordt beheerst en waar relevant geregistreerd.

b Toegangsbeveiliging:

- Computers, systemen en webportalen zijn uitsluitend toegankelijk voor geautoriseerde gebruikers.
- Waar mogelijk wordt multifactor-authenticatie (MFA) toegepast.
- Schermen van laptops en computers worden bij inactiviteit automatisch vergrendeld.
- Voor interne systemen wordt gebruikgemaakt van rolgebaseerde toegangscontrole (RBAC).

c Dataopslag en verwerking:

- Er wordt gebruikgemaakt van beveiligde verbindingen (TLS 1.2 of hoger) en van encryptie van opgeslagen gegevens, waaronder persoonsgegevens, waar passend.
- Back-ups worden dagelijks geautomatiseerd uitgevoerd en versleuteld opgeslagen en verzonden.

d Software en patchmanagement:

- Er wordt gebruikgemaakt van actuele software, waaronder antivirus en EDR.
- Windows-systemen ontvangen wekelijks automatische kritieke updates en beveiligingsupdates.
- Third-partysoftware wordt wekelijks geactualiseerd waar dit technisch mogelijk en passend is.
- Content filtering wordt toegepast ter beperking van malware- en ransomware-risico's.

e Monitoring en detectie:

- Endpoints en netwerkapparatuur worden continu gemonitord.
- Beveiligingsincidenten worden waar mogelijk automatisch gedetecteerd.
- Periodieke systeemherstelpunten ondersteunen een doelmatig herstelproces.
- IDS/IPS is ingericht op firewalls voor detectie en preventie van netwerkdreigingen.

f Vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht:

- Vertrouwelijkheid: toegangscontrole, encryptie en geheimhoudingsverplichtingen voor medewerkers.
- Integriteit: logregistratie, versiebeheer en geautomatiseerde back-ups.
- Beschikbaarheid: redundante systemen, monitoring en serviceafspraken waar van toepassing.
- Veerkracht: disaster-recoveryprocedures, periodieke tests van back-ups en een incidentresponsproces.

g Herstel bij incidenten:

- Bij incidenten kunnen beschikbaarheid en toegang tot persoonsgegevens tijdig worden hersteld via back-upsystemen, waaronder NinjaOne SaaS-back-up (voorheen Dropsuite), Synology-NAS-oplossingen en cloudopslag bij Backblaze of Impossible Cloud.
- Herstel van Microsoft 365-data is, afhankelijk van omvang en complexiteit, in beginsel mogelijk binnen 24 tot 48 uur.
- Systeemherstelpunten op laptops en werkstations ondersteunen snel herstel waar dit technisch mogelijk is.

Een samenvatting van ons beveiligingsbeleid is voor opdrachtgevers op aanvraag beschikbaar; inzage in het volledige interne beveiligingsbeleid is uitsluitend mogelijk onder geheimhouding.

15. IT aanspreekpunt heeft een Information Security Management System (ISMS) ingericht en geborgd via:

- ISO/IEC 27001

IT aanspreekpunt beschikt over een actief ISO/IEC 27001:2022-certificaat voor informatiebeveiliging. Dit certificaat wordt periodiek geauditeerd door een onafhankelijke certificerende instelling.

Het ISMS van IT aanspreekpunt omvat onder meer:

- Een Plan-Do-Check-Act (PDCA)-cyclus voor continue verbetering.
- Periodieke risicoanalyses en passende risicobehandelingsmaatregelen.
- Periodieke interne en externe audits.
- Managementreviews en evaluatie van beveiligingsmaatregelen.
- Incidentmanagement en een gedocumenteerd datalekkenprotocol.

16. IT aanspreekpunt heeft de volgende verificaties en certificeringen:

- ISO/IEC 27001:2022

Datalekkenprotocol

17. In geval er toch iets misgaat, hanteert IT aanspreekpunt het volgende datalekkenprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:

IT aanspreekpunt beschikt over een gedocumenteerd datalekkenprotocol in overeenstemming met de AVG. Hieronder is beknopt opgenomen hoe opdrachtgever over relevante incidenten wordt geïnformeerd.

Interne detectie en melding:

- Er geldt een interne procedure voor het melden van (vermoedelijke) beveiligingsincidenten.
- Medewerkers zijn geïnstrueerd om beveiligingsincidenten onverwijld te melden aan de privacycontactpersoon (Tom Koelemij).
- Monitoring- en detectiesystemen signaleren waar mogelijk automatisch potentiële incidenten.

Melding aan opdrachtgever:

Indien IT aanspreekpunt een inbreuk in verband met persoonsgegevens constateert, wordt opdrachtgever daarvan zonder onredelijke vertraging en uiterlijk binnen 48 uur na ontdekking op de hoogte gesteld, conform het geldende datalekkenprotocol.

De melding aan opdrachtgever bevat in ieder geval de volgende informatie:

- **Omschrijving van het incident**: wat is er gebeurd en wanneer heeft het incident plaatsgevonden.
- **Aard van de inbreuk**: het type beveiligingsincident, zoals ongeoorloofde toegang, verlies, vernietiging of wijziging.

- **Aard van de persoonsgegevens**: welke categorieën persoonsgegevens betrokken zijn.
- **Schatting aantal betrokkenen**: een indicatie van het aantal betrokkenen dat mogelijk is geraakt.
- **Betrokken systemen of databases**: welke systemen, applicaties of databronnen zijn geraakt.
- **Contactgegevens**: de contactpersoon bij IT aanspreekpunt (Tom Koelemij, info@itaanspreekpunt.nl, 053 203 21 53).
- **Mogelijke gevolgen**: welke gevolgen het incident kan hebben en waar opdrachtgever rekening mee moet houden.
- **Genomen maatregelen**: welke maatregelen IT aanspreekpunt heeft genomen of zal nemen om de schade te beperken en herhaling te voorkomen.
- **Aanbevolen maatregelen**: welke aanvullende acties opdrachtgever en/of betrokkenen kunnen overwegen.

Continue verbetering:

IT aanspreekpunt houdt opdrachtgever, waar relevant, op de hoogte van verdere ontwikkelingen en evalueert incidenten om beveiligingsmaatregelen waar nodig aan te scherpen.

Voor een volledig datalekkenprotocol verwijzen wij naar ons interne protocol (beschikbaar op aanvraag).

Lees je dit? Dan heb je deze verwerkersovereenkomst echt doorgelezen. Mail het codewoord "Privacy-Pinguïn" naar info@itaanspreekpunt.nl en ontvang een kleine attentie (één per organisatie, zolang de voorraad strekt). Liet je deze verwerkersovereenkomst door AI samenvatten? Dan telt het codewoord ook, maar eerlijk is eerlijk: de attentie is vooral bedoeld voor wie zelf leest.

Deel 2: Standaardclausules voor verwerkingen

Versie: maart 2025

Vormt samen met het Data Pro Statement de verwerkersovereenkomst en is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden.

Artikel 1. Definities

Onderstaande begrippen hebben in deze Standaardclausules voor verwerkingen, in het Data Pro Statement en in de overeenkomst de volgende betekenis:

1.1 **Autoriteit Persoonsgegevens (AP):** toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 AVG.
1.2 **AVG:** de Algemene verordening gegevensbescherming.
1.3 **Data Processor**: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.
1.4 **Data Pro Statement**: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, sub-processors, datalekken, certificeringen en omgang met rechten van Data subjects.
1.5 **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon.
1.6 **Opdrachtgever:** partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.
1.7 **Overeenkomst**: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.
1.8 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 AVG, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.
1.9 **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 AVG.

Artikel 2. Algemeen

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.
2.2 Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.
2.3 Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.

2.4 Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de AVG, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de AVG en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de AVG zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de AVG handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor.

Artikel 3. Beveiliging

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico's en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten of door de overheid uitgegeven persoonsnummers.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

Artikel 4. Inbreuken in verband met Persoonsgegevens

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 AVG) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

18. Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 AVG moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

19. Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 AVG.

4.2 Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

Artikel 5. Geheimhouding

5.1 Data Processor waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

Artikel 6. Looptijd en beëindiging

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

6.2 Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen aan Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de AVG is ten aanzien van de Persoonsgegevens.

Artikel 7. Rechten Data subjects, Data Protection Impact Assessment (DPIA) en Auditrechten

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 AVG.

7.3 Data Processor zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

7.4 Data Processor kan desgewenst de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of een daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige, indien hij over een dergelijk certificaat of auditrapport beschikt.

7.5 Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de AVG of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.6 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.7 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

Artikel 8. Sub-Processors

8.1 Data Processor heeft in het Data Pro Statement vermeld of, en zo ja welke derde partijen (sub-processors of subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere sub-processors in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

8.3 Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

Artikel 9. Overig

Deze Standaardclausules voor verwerkingen vormen tezamen met het Data Pro Statement een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst.