ZORION

PUBLIEK INFORMATIEDOCUMENT

Zorion in de praktijk

Wat wij dagelijks doen met de gegevens die u ons toevertrouwt, en wat u van ons mag verwachten. Geschreven voor wie de verwerkersovereenkomst niet van kaft tot kaft leest, maar wel wil weten hoe het werkt.

Documenttype	Publiek informatiedocument, geen contractueel document
Voor wie	Klanten, prospecten en hun adviseurs
Versie	2.3
Datum	16 augustus 2026
Uitgegeven door	Zorion, Vakenderveld 7.6, 2500 Lier, België, RPR Antwerpen afdeling Mechelen, ondernemingsnummer 1009.162.363
Contact	Luka Stoop, admin@zorion.be

WAT DIT DOCUMENT WEL EN NIET IS

Dit is een toelichting in gewone taal. Het schept geen rechten en geen verplichtingen. Wat bindend is, staat in de offerte, de productfiche, de service level agreement en de verwerkersovereenkomst.

Wijkt dit document af van die documenten, dan gelden zij en niet dit.

De twee petten van Zorion

Bij bijna elke vraag over gegevensbescherming is dit de eerste vraag die beantwoord moet worden, en het is ook de vraag die het vaakst door elkaar wordt gehaald.

Rol	Wat het betekent
Zorion als verwerker	Voor alles wat wij voor u doen. U bepaalt waarom en hoe uw gegevens verwerkt worden, wij voeren uit. Uw klantenbestand, uw mailboxen, uw website: dat blijft van u. Hierop is de verwerkersovereenkomst van toepassing.
Zorion als verwerkingsverantwoordelijke	Voor onze eigen bedrijfsvoering: onze klantenadministratie, onze boekhouding, onze facturatie, onze prospectie en onze eigen website. Daar bepalen wij het doel, en daar hebben wij zelf een privacyverklaring en een eigen register voor.

De praktische toets die wij zelf gebruiken: verwerkt een leverancier gegevens van úw klanten of medewerkers, in het kader van de dienst die wij aan u leveren? Dan staat hij in bijlage 3. Contracteren wij zelf met hem, dan is hij onze subverwerker en zijn wij voor hem volledig aansprakelijk. Contracteert u zelf met hem, zoals bij het Odoo-platform of bij de betaaldienst van uw webshop, dan staat hij in bijlage 3 in een aparte tabel: u ziet hem dus wel, maar hij is niet onze subverwerker en wij kunnen hem ook niet aansturen. Gebruiken wij hem enkel om onze eigen zaak te runnen? Dan staat hij daar niet, en sluiten wij zelf een overeenkomst met hem.

Wat wij doen op de dag dat u klant wordt

1. U ontvangt de offerte met daarbij, in dezelfde zending, de algemene voorwaarden, de algemene dienstverleningsbepalingen, de service level agreement, de verwerkersovereenkomst, de productfiche van uw pakket en de bijlagedocumenten van de modules die op u van toepassing zijn. Nasturen doen wij niet: tussen ondernemingen zijn voorwaarden alleen tegenstelbaar wanneer u er vóór of bij het sluiten kennis van kon nemen.
2. Wij bewaren die zending als bewijs, met datum en inhoud.
3. Bij ondertekening van de offerte aanvaardt u die documenten. Wij vragen daarnaast een afzonderlijk ondertekend exemplaar van de verwerkersovereenkomst, omdat dat bij een controle het sterkste bewijs is.
4. Wij maken u aan in ons verwerkingsregister als verwerkingsverantwoordelijke voor wie wij werken, met de categorieën van verwerkingen die wij voor u doen.
5. Wij zetten uw omgeving op volgens de maatregelen uit bijlage 2 van uw modules, en wij leggen de toegangen vast in onze inventaris.

Wat wij elke dag doen

Toegang en wachtwoorden

- Wij werken met persoonlijke, benoemde accounts. Nooit met een gedeeld account waarop niemand aanspreekbaar is.
- Meervoudige authenticatie staat aan op onze eigen organisatie en op elke beheersomgeving die het ondersteunt.
- Wachtwoorden bewaren wij in een kluis waarvan de aanbieder de inhoud technisch niet kan lezen. Wij sturen nooit een wachtwoord per e-mail of per chatbericht.
- Vraagt u een wachtwoord op dat wij voor u bewaren, dan delen wij dat via de kluis en niet via e-mail.
- Verlaat iemand uw onderneming, dan trekken wij de toegangen in zodra u het meldt. Meld dat daarom altijd, ook wanneer het vertrek in goede verstandhouding gebeurt.

Meekijken op afstand

- Wij kijken enkel mee na uw uitdrukkelijke toestemming, per sessie. De verbinding is versleuteld.
- Wij vragen u om vensters met gevoelige informatie te sluiten voordat u de sessie start. Wat wij niet zien, moeten wij ook niet beschermen.

Uw gegevens in onze systemen

- Wij gebruiken uw gegevens uitsluitend om de afgesproken dienst te leveren. Niet voor onze eigen doeleinden, niet voor analyses over klanten heen, en niet om systemen voor artificiële intelligentie te trainen.
- Wij voeren geen persoonsgegevens van uw klanten of medewerkers in hulpmiddelen in die niet in bijlage 3 staan.
- Moeten wij een uittreksel maken om een fout te onderzoeken, dan beperken wij dat tot de betrokken gegevens en verwijderen wij het na afhandeling.

Waarvoor wij artificiële intelligentie gebruiken

- Wij gebruiken generatieve AI als hulpmiddel bij ons eigen werk: het opstellen van teksten, documenten, scripts en configuratievoorstellen. Een mens beoordeelt altijd het resultaat voordat het bij u terechtkomt.
- Wij voeren daarbij geen persoonsgegevens van u, uw klanten of uw medewerkers in. Artikel 4.5 van de verwerkersovereenkomst verbiedt dat uitdrukkelijk: persoonsgegevens gaan enkel in de hulpmiddelen die in bijlage 3 staan.
- Wij gebruiken uw gegevens niet om AI-modellen te trainen, en wij laten dat ook niet toe bij onze leveranciers.
- Er staat geen AI tussen u en ons. Wanneer u ons contacteert, antwoordt een mens. Wij zetten geen chatbot in die zich als medewerker voordoet.

WAAROM DIT HIER STAAT TERWIJL HET NIET MOET

Er bestaat vandaag geen wettelijke verplichting om u dit te melden. De transparantieplicht van artikel 50 van de Europese AI-verordening, van toepassing sinds 2 augustus 2026, richt zich op wie een AI-systeem aanbiedt en op wie er mensen rechtstreeks mee laat interageren of er synthetische content mee publiceert. Intern gebruik voor eigen teksten valt daar niet onder, en zonder persoonsgegevens komt de AVG er niet aan te pas.

Wij vermelden het toch, omdat u het redelijkerwijs wil weten en omdat het in aanbestedingen en raamovereenkomsten steeds vaker gevraagd wordt. Neemt uw eigen beleid een strengere regel op, laat het ons weten en wij houden ons eraan.

Wat wij met uw meldingen doen om onze dienstverlening te verbeteren

- Wij registreren elke melding, vraag en storing in ons eigen systeem, zodat de opvolging niet van een mailbox afhangt.
- Wij kijken daarnaast naar het geheel van die meldingen om te zien waar het vaak misloopt, hoe snel wij reageren en welke uitleg blijkbaar tekortschiet. Dat gebeurt op geaggregeerd niveau, dus over klanten heen en zonder individuele beoordeling.
- Voor die kwaliteitsanalyse zijn wij zelf verwerkingsverantwoordelijke, niet uw verwerker. De grondslag is ons gerechtvaardigd belang bij een werkende dienstverlening.
- Wilt u dat de meldingen van uw onderneming daar niet in meetellen, laat het weten via admin@zorion.be en wij sluiten ze uit. Dat verandert niets aan de dienst zelf.

Updates en beveiliging

- Wij installeren beveiligingsupdates zodra zij beschikbaar zijn. Loopt een update mis, dan herstellen wij dat: wij bepalen de updatestrategie en dragen dus het risico.
- Wij volgen de meldingen op die de platformen zelf genereren, tijdens de bedrijfsuren.
- Buiten de bedrijfsuren is er geen bewaking. Dat zeggen wij liever te vaak dan te weinig, want het is de verwachting die in de praktijk het meest uiteenloopt.

Wat wij doen wanneer er iets misgaat

Bij een incident met persoonsgegevens

Een incident met persoonsgegevens is bijvoorbeeld: een mailbox die gecompromitteerd is, een bestand dat naar de verkeerde ontvanger is gestuurd, een website die gehackt is, of gegevens die verloren zijn gegaan.

1. Wij melden het u binnen vierentwintig uur na kennisname, per e-mail en telefonisch wanneer wij inschatten dat het risico hoog is.
2. Die melding bevat vier zaken: wat er gebeurd is en over welke gegevens en hoeveel mensen het gaat, bij wie u terecht kan voor meer informatie, wat de waarschijnlijke gevolgen zijn, en welke maatregelen wij al genomen hebben of voorstellen.
3. Wij dijken het incident onmiddellijk in en beperken de gevolgen.
4. Wij melden niet zelf aan de Gegevensbeschermingsautoriteit en niet aan de betrokken personen. Die beoordeling is aan u, en u heeft daar tweeënzeventig uur voor vanaf uw kennisname. Wij leveren u de informatie die u nodig heeft om die beslissing te nemen.
5. Wij noteren elk incident in ons register, ook wanneer het niet gemeld moet worden, met de reden waarom niet.
6. Na afloop krijgt u een korte terugkoppeling: wat er gebeurd is, wat de oorzaak was, en wat er is aangepast.

> **WAAROM WIJ NIET ZELF MELDEN AAN DE TOEZICHTHOUDER**
>
> Dat is geen onwil. De AVG legt die beoordeling uitdrukkelijk bij de verwerkingsverantwoordelijke, dus bij u. Alleen u weet wat het incident voor uw mensen en uw klanten betekent.
>
> Wij zouden die inschatting in uw plaats kunnen maken, maar dan zouden wij zelf het doel van de verwerking bepalen. Precies daardoor zouden wij juridisch van verwerker naar verwerkingsverantwoordelijke opschuiven, en dat is voor geen van beide partijen een goede zaak.

Bij een storing zonder gegevensrisico

Dan geldt de service level agreement: u meldt, wij delen de melding in op prioriteit, en wij reageren binnen de termijn die bij die prioriteit hoort. Bij een kritieke storing krijgt u minstens om de vier bedrijfsuren een stand van zaken, ook wanneer er niets veranderd is.

Wanneer iemand ons rechtstreeks om zijn gegevens vraagt

Vraagt een van uw klanten of medewerkers rechtstreeks bij ons om inzage, verbetering of verwijdering, dan behandelen wij dat verzoek niet zelf. Wij sturen het binnen twee werkdagen naar uw contactpunt en bevestigen aan die persoon enkel dat wij het hebben doorgestuurd. U heeft daarna één maand om te antwoorden. Wij helpen u met het technische werk: een uittreksel maken, een gegeven aanpassen, een account verwijderen of een export aanleveren.

Onze leveranciers en de keten erachter

- Elke leverancier die gegevens van uw mensen verwerkt, staat met naam in bijlage 3 van de betrokken module, met vermelding van waar hij verwerkt en of er gegevens buiten Europa gaan.
- Komt er een leverancier bij of wordt er een vervangen, dan melden wij dat dertig kalenderdagen vooraf per e-mail. U kan binnen die termijn gemotiveerd bezwaar maken. Vinden wij samen geen oplossing, dan kan u de betrokken module beëindigen zonder schadevergoeding.
- Valt een leverancier weg, dan melden wij dat ook, maar dan is er geen bezwaartermijn: er komt immers niets bij.
- Wij publiceren die lijst ook op onze website, maar dat vervangt de e-mail niet. Verwachten dat u een webpagina in de gaten houdt, is geen informeren.
- Van elke leverancier houden wij naam, adres van de zetel en een contactpunt bij, en wij bezorgen die binnen vijf werkdagen op eenvoudig verzoek.
- Wij vermelden ook uitdrukkelijk welke hulpmiddelen géén subverwerker zijn en waarom. Dat voorkomt dat u bij elke licentiewijziging een melding krijgt over iets dat uw gegevens nooit ziet.

Gegevens buiten Europa

De hosting van uw website, uw databank en uw mailboxen blijft binnen de Europese Economische Ruimte. De ondersteunende diensten die in bijlage 3 met naam staan, zoals het systeem waarin uw vragen geregistreerd worden of de dienst waarmee wij op afstand meekijken, verwerken wel gegevens buiten die ruimte.

Waar dat gebeurt, staat het in bijlage 3, samen met het mechanisme waarop wij ons beroepen. Dat is telkens een van deze drie: een adequaatheidsbesluit van de Europese Commissie, de standaardcontractbepalingen die de Commissie heeft vastgesteld, of bindende bedrijfsvoorschriften.

Wordt zo'n mechanisme ongeldig verklaard, en dat is sinds 2015 twee keer gebeurd voor de Verenigde Staten, dan melden wij dat binnen tien werkdagen en stellen wij een alternatief voor. Komen wij er niet uit, dan kan de betrokken module beëindigd worden.

Wat wij niet doen, en waarom

Wij beloven niet	Reden
Een beschikbaarheidspercentage	Wij meten dat vandaag niet zelf. Een percentage beloven zonder eigen meting is een belofte die bij betwisting niet standhoudt. Wij verbinden ons daarom aan reactietermijnen.
Een hersteltermijn	Bij de meeste storingen ligt de uitvoering bij een leverancier. Wij volgen op en escaleren, maar wij herstellen niet in hun plaats.
Dat uw e-mail versleuteld aankomt	Onze servers zijn ingesteld op versleutelde verbindingen, maar de server van de tegenpartij bepaalt mee. E-mail is daarom nooit het juiste kanaal voor gevoelige gegevens.
Dat de datacenters fysiek beveiligd zijn	Dat is een uitspraak over iemand anders. Wij verwijzen naar de certificeringen en verklaringen van die partij en houden die documentatie ter beschikking.
Dat alles bij Microsoft in Europa blijft	Microsoft verklaart dat klantgegevens binnen de Europese datagrens blijven en documenteert tegelijk uitzonderingen. Wij nemen die nuance over in plaats van ze weg te laten.
Juridisch advies	Documenten die een hulpmiddel voor u genereert, zoals een privacyverklaring, zijn geen advies en zijn niet door een jurist nagekeken.

Waar u ons aan kan houden

- U mag één keer per jaar een audit laten uitvoeren, en telkens na een vastgesteld incident. U kondigt die dertig dagen vooraf aan. Wij mogen in de plaats daarvan een certificaat of een auditrapport voorleggen wanneer dat dezelfde vraag beantwoordt.
- U mag op elk ogenblik onze actuele lijst van leveranciers opvragen, met hun identiteitsgegevens. Wij bezorgen die binnen vijf werkdagen.
- U mag ons verwerkingsregister en onze procedures opvragen.
- De Gegevensbeschermingsautoriteit kan onderzoek voeren en sancties opleggen, ook rechtstreeks aan ons. Een betrokkene kan ons rechtstreeks voor de rechter dagen op grond van artikel 82 van de AVG. Onze aansprakelijkheidsbeperking tegenover u verandert daar niets aan.

Vragen

Alles wat hier staat, kan u navragen. Neem contact op met Luka Stoop via admin@zorion.be. Vragen die tot een aanpassing van dit document leiden, worden in de volgende versie verwerkt.