

Privacyreglement Vertas B.V.¹

Bescherming en verwerking van persoonsgegevens – versie 2.0, augustus 2026

Artikel 1. Introductie

Dit privacyreglement beschrijft hoe Vertas B.V. (hierna: 'Vertas') omgaat met de verwerking van persoonsgegevens in het kader van haar werkzaamheden en dienstverlening. Vertas hecht groot belang aan de bescherming van de privacy van betrokkenen en verwerkt persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG/GDPR) en de Uitvoeringswet AVG (UAVG).

Artikel 2. Verantwoordelijke en contactgegevens

Vertas B.V. is de verwerkingsverantwoordelijke in de zin van de AVG voor de persoonsgegevens die zij verwerkt in het kader van haar eigen bedrijfsvoering en dienstverlening.

Vertas B.V.

E-mail: info@vertas.nl

Website: www.vertas.nl

Artikel 3. Functionaris gegevensbescherming

Als functionaris gegevensbescherming is aangewezen de directeur van Vertas B.V. De functionaris is bereikbaar via info@vertas.nl.

Artikel 4. Doeleinden van verwerking

Vertas verwerkt persoonsgegevens voor de volgende doeleinden:

- Het uitvoeren van opdrachten en overeenkomsten met opdrachtgevers.
- Het verlenen van toegang tot en het beheren van de geautomatiseerde systemen ORT (Objective Ranking Tool) en SPT (Security Planning Tool) via www.veilig.in.
- Het toekennen en beheren van gebruiksrechten binnen deze systemen.
- Het (de)activeren van gebruikersaccounts.
- Het informeren van betrokkenen over relevante ontwikkelingen.
- Het voldoen aan wettelijke verplichtingen.
- Het onderhouden van zakelijke relaties en communicatie.
- Het voeren van de financiële administratie.
- Het doorlopend leren en ontwikkelen van het Vertas-framework op basis van geanonimiseerde projectresultaten (zie artikel 9).

Artikel 5. Categorieën persoonsgegevens

Vertas kan de volgende categorieën persoonsgegevens verwerken:

- Identificatiegegevens: volledige naam (voornaam, tussenvoegsel, achternaam).
- Contactgegevens: e-mailadres, telefoonnummer, adresgegevens.
- Werkgegevens: naam van het bedrijf of de organisatie waarvoor betrokkene werkzaam is, functie.
- Accountgegevens: (in)actief-status van het account, datum laatste mutatie, toegekende lees- en schrijfrechten, activering tweestapsverificatie, het account dat de laatste mutatie heeft doorgevoerd.
- Financiële gegevens: factuurgegevens, betalingsgegevens (uitsluitend voor de financiële administratie).

Artikel 6. Grondslagen voor verwerking

Vertas verwerkt persoonsgegevens op basis van een of meer van de volgende grondslagen uit artikel 6 AVG:

- Noodzakelijk voor de uitvoering van een overeenkomst.
- Noodzakelijk voor het voldoen aan een wettelijke verplichting.
- Gerechtvaardigd belang van Vertas (zoals het onderhouden van zakelijke relaties en het doorlopend verbeteren van het Vertas-framework).
- Toestemming van de betrokkene.

Artikel 7. Verstrekking aan derden

Vertas verstrekt persoonsgegevens niet aan derden, tenzij:

- Verstrekking noodzakelijk is voor de uitvoering van de overeenkomst.
- Verstrekking voortvloeit uit een wettelijke verplichting.
- Verstrekking noodzakelijk is bij storingen van de geautomatiseerde systemen om de toegang van betrokkene te borgen.
- Betrokkene uitdrukkelijke toestemming heeft gegeven.

Met partijen aan wie persoonsgegevens worden verstrekt, sluit Vertas een verwerkersovereenkomst volgens de AVG. De website www.veilig.in wordt beheerd vanuit een Nederlandse server. Alle medewerkers van Vertas, inclusief ingehuurd personeel, zijn gebonden aan geheimhoudings- en integriteitsverklaringen.

Artikel 8. Doorgifte buiten de EER

Vertas geeft in beginsel geen persoonsgegevens door aan landen buiten de Europese Economische Ruimte (EER). Indien doorgifte noodzakelijk is, zorgt Vertas voor passende waarborgen volgens hoofdstuk V van de AVG,

¹ Dit document is opgesteld met ondersteuning van generatieve AI, onder menselijke controle en inhoudelijke eindverantwoordelijkheid

zoals het hanteren van door de Europese Commissie goedgekeurde standaardcontractbepalingen.

Artikel 9. Bewaartermijnen en projectresultaten

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel waarvoor zij zijn verzameld, of zo lang als wettelijk vereist is. Specifiek gelden de volgende termijnen:

- Accountgegevens: zolang betrokkene geautoriseerde toegang heeft tot de systemen. Na intrekking van de autorisatie worden gegevens verwijderd, tenzij wettelijke bepalingen zich daartegen verzetten.
- Financiële gegevens: gedurende de wettelijke bewaartermijn van zeven (7) jaar.
- Projectresultaten: worden drie (3) jaar na afronding van de opdracht geanonimiseerd, zodanig dat zij niet meer herleidbaar zijn naar de opdrachtgever of betrokkenen. De geanonimiseerde resultaten worden opgeslagen ten behoeve van doorlopend leren en ontwikkelen van het Vertas-framework.

Projectresultaten worden altijd beoordeeld op toegevoegde waarde voor het framework dat binnen Vertas in gebruik is. Alleen resultaten met daadwerkelijke meerwaarde voor de kennisbasis van Vertas worden in geanonimiseerde vorm bewaard.

Artikel 10. Controle wenselijkheid toegang

Periodiek wordt gecontroleerd of de toegang tot de geautomatiseerde systemen nog wenselijk is, onder meer door het toezenden van een bevestigingslink aan het vastgelegde e-mailadres. Als niet op deze link wordt gereageerd, wordt de toegang automatisch gedeactiveerd. Op deze wijze wordt mede invulling gegeven aan het beperken van mogelijke risico's met betrekking tot de BIV-classificatie van de systemen.

Artikel 11. Rechten van betrokkenen

Op grond van de AVG heeft de betrokkene de volgende rechten:

- Recht op inzage: het recht om te weten welke persoonsgegevens Vertas verwerkt.
- Recht op rectificatie: het recht om onjuiste of onvolledige gegevens te laten corrigeren.
- Recht op gegevenswissing ('recht op vergetelheid'): het recht om verwijdering van persoonsgegevens te verzoeken.
- Recht op beperking van de verwerking: het recht om de verwerking tijdelijk te laten beperken.
- Recht op overdraagbaarheid: het recht om persoonsgegevens in een gestructureerd, gangbaar en machineleesbaar formaat te ontvangen.
- Recht van bezwaar: het recht om bezwaar te maken tegen de verwerking op basis van gerechtvaardigd belang.
- Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, waaronder profilering.

Een verzoek kan worden ingediend via info@vertas.nl. Vertas reageert binnen één (1) maand op het verzoek. Ter verificatie van de identiteit kan Vertas om een geldig legitimatiebewijs vragen.

Artikel 12. Beveiliging

Vertas treft passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking, verlies, vernietiging of beschadiging. Deze maatregelen omvatten onder meer:

- Toegang tot systemen uitsluitend via geautoriseerde accounts met sterke wachtwoorden.
- Gebruik van SSL/TLS-versleuteling voor alle onlineverbindingen.
- Tweestapsverificatie voor gevoelige systemen.
- Regelmatische back-ups van gegevens.
- Fysieke beveiligingsmaatregelen voor kantoor en apparatuur.
- Periodieke evaluatie en actualisering van beveiligingsmaatregelen.
- Geheimhoudings- en integriteitsverklaringen voor alle medewerkers, inclusief ingehuurd personeel.

Bij de inzet van kunstmatige intelligentie (AI) als ondersteunend instrument geldt aanvullend het AI-reglement van Vertas, beschikbaar op www.vertas.nl. Persoonsgegevens worden daarbij uitsluitend verwerkt in overeenstemming met dit privacyreglement en, waar Vertas als verwerker optreedt, de verwerkersovereenkomst.

Artikel 13. Cookies

De website www.veilig.in plaatst uitsluitend functionele cookies om de website goed te laten functioneren en analytische cookies om websitebezoek te monitoren. Deze informatie is niet herleidbaar tot individuele IP-adressen. Betrokkene kan via de browserinstellingen bepalen op welke wijze met cookies wordt omgegaan.

Artikel 14. Datalekken

Vertas heeft een procedure voor het melden en afhandelen van datalekken volgens artikel 33 en 34 AVG. De volledige procedure datalekken is opgenomen als bijlage bij dit privacyreglement. In hoofdlijnen geldt het volgende:

- Iedere medewerker van Vertas, inclusief ingehuurd personeel, is verplicht een (vermoedelijk) datalek onmiddellijk te melden bij de functionaris gegevensbescherming via info@vertas.nl.
- De functionaris gegevensbescherming beoordeelt het incident, neemt directe maatregelen en registreert het incident in het datalekkenregister.
- Melding aan de Autoriteit Persoonsgegevens geschiedt binnen 72 uur na ontdekking als het lek een risico inhoudt voor de rechten en vrijheden van betrokkenen.
- Betrokkenen worden geïnformeerd als het lek een hoog risico oplevert voor hun rechten en vrijheden.

Artikel 15. Klachten

Klachten over de verwerking van persoonsgegevens kunnen worden ingediend bij Vertas via info@vertas.nl. Daarnaast heeft de betrokkene het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens via www.autoriteitpersoonsgegevens.nl.

Artikel 16. Wijzigingen

Vertas behoudt zich het recht voor dit privacyreglement te wijzigen. De meest actuele versie is beschikbaar op www.vertas.nl. Bij ingrijpende wijzigingen worden betrokkenen hierover actief geïnformeerd.

IJsselstein, augustus 2026

P.L. Prak

Directeur

Bijlage: Procedure Datalekken

Deze procedure beschrijft de stappen die Vertas B.V. neemt bij het ontdekken, melden en afhandelen van een inbreuk in verband met persoonsgegevens (datalek) conform de artikelen 33 en 34 van de AVG.

1. Ontdekking en interne melding

Iedere medewerker van Vertas, inclusief ingehuurd personeel dat onder de vlag van Vertas werkt, is verplicht een (vermoedelijk) datalek onmiddellijk te melden bij de functionaris gegevensbescherming via info@vertas.nl. De melding bevat ten minste:

- Naam van de melder en contactgegevens.
- Datum en tijdstip van ontdekking.
- Beschrijving van het incident.
- Welke (categorieën) persoonsgegevens mogelijk zijn getroffen.

2. Eerste beoordeling

De functionaris gegevensbescherming beoordeelt binnen twee (2) uur na melding:

- Of sprake is van een daadwerkelijk datalek in de zin van de AVG.
- Welke persoonsgegevens zijn getroffen (type, hoeveelheid, categorieën betrokkenen).
- Wat de waarschijnlijke gevolgen zijn voor betrokkenen.
- Welke directe maatregelen nodig zijn om het lek te dichten en verdere schade te beperken.

3. Directe maatregelen

De functionaris gegevensbescherming neemt onmiddellijk maatregelen om:

- Het datalek te dichten (zoals het intrekken van toegangsrechten, het wijzigen van wachtwoorden, het isoleren van getroffen systemen).
- Verder gegevensverlies te voorkomen.
- Bewijsmateriaal veilig te stellen voor nader onderzoek.

4. Registratie in het datalekkenregister

Elk datalek wordt vastgelegd in het datalekkenregister van Vertas. Het register bevat per incident:

- Datum en tijdstip van ontdekking en melding.
- Aard van de inbreuk.
- Type en hoeveelheid getroffen persoonsgegevens.
- Categorieën en geschat aantal betrokkenen.
- Waarschijnlijke gevolgen.
- Genomen en voorgestelde maatregelen.
- Contactpersoon voor verdere afwikkeling.
- Beslissing over melding aan de Autoriteit Persoonsgegevens en/of betrokkenen.

5. Melding aan de Autoriteit Persoonsgegevens

Indien het datalek een risico inhoudt voor de rechten en vrijheden van betrokkenen, meldt de functionaris gegevensbescherming het incident binnen 72 uur na ontdekking bij de Autoriteit Persoonsgegevens via het meldformulier op www.autoriteitpersoonsgegevens.nl. De melding omvat:

- De aard van de inbreuk.
- De categorieën en het geschatte aantal betrokkenen en persoonsgegevens.
- De naam en contactgegevens van de functionaris gegevensbescherming.
- De waarschijnlijke gevolgen van de inbreuk.
- De maatregelen die zijn genomen of worden voorgesteld.

Indien niet alle informatie tegelijkertijd beschikbaar is, wordt deze zonder onredelijke vertraging in fasen verstrekt.

6. Melding aan betrokkenen

Indien het datalek een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, worden zij hierover onverwijld geïnformeerd in duidelijke en eenvoudige taal. De melding aan betrokkenen bevat:

- De aard van de inbreuk.
- De naam en contactgegevens van de functionaris gegevensbescherming.
- De waarschijnlijke gevolgen.
- De genomen en voorgestelde maatregelen, inclusief maatregelen die betrokkenen zelf kunnen nemen.

7. Melding aan opdrachtgever(s)

Indien Vertas als verwerker optreedt, wordt de betreffende opdrachtgever (verwerkingsverantwoordelijke) onverwijld en uiterlijk binnen 24 uur na ontdekking geïnformeerd, conform de verwerkersovereenkomst.

8. Onderzoek en evaluatie

Na afhandeling van het acute incident voert de functionaris gegevensbescherming een evaluatie uit:

- Wat was de oorzaak van het datalek?
- Waren de bestaande beveiligingsmaatregelen toereikend?
- Welke structurele verbeteringen zijn nodig om herhaling te voorkomen?
- Dient het beveiligingsbeleid of de procedure te worden bijgesteld?

De bevindingen worden vastgelegd in het datalekkenregister en leiden, waar nodig, tot aanpassing van beleid en maatregelen.

9. Jaarlijkse evaluatie

Het datalekkenregister wordt minimaal jaarlijks geëvalueerd door de functionaris gegevensbescherming om trends te signaleren, de effectiviteit van maatregelen te beoordelen en verbeteringen door te voeren.

Vertas B.V.

Johann Knoopstraat 8

3404 AV IJsselstein

info@vertas.nl | www.vertas.nl

IJsselstein, augustus 2026

P.L. Prak, directeur