



NLdigital

Versie: 2.0 / 05-10-2026

Verwerkers- overeenkomst Agyle

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 samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

Algemene informatie

1. Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):

Agyle B.V.

Lagelandseweg 84, 6545 CG NIJMEGEN

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:

Quirijn Prevoo

quirijn.prevoo@agyle.nl

[+31637317586](tel:+31637317586)

2. Dit Data Pro Statement geldt vanaf 20-07-2026

Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze normale kanalen.

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor
Afhankelijk van de aard van de opdracht kunnen hieronder softwareontwikkeling, applicatiebeheer, integratieoplossingen, data-uitwisseling, consultancy en managed services vallen. Welke diensten onder deze verwerkersovereenkomst vallen wordt per opdracht schriftelijk vastgelegd in de overeenkomst, offerte of opdrachtbevestiging tussen partijen.

Zie het complete portfolio op <https://www.agyle.nl/>

4. Omschrijving product(en)/dienst(en)

Agyle levert softwareontwikkeling, applicatiebeheer, integratieoplossingen, data-uitwisseling, consultancy en managed services aan zakelijke opdrachtgevers. De diensten ondersteunen de ontwikkeling, het beheer en de koppeling van digitale systemen en bedrijfsprocessen. De concrete dienstverlening wordt nader omschreven in de betreffende overeenkomst, offerte of opdrachtbevestiging.

5. Beoogd gebruik

Product/dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

De diensten zijn ontworpen voor de verwerking van persoonsgegevens die noodzakelijk zijn voor de uitvoering van softwareontwikkeling, applicatiebeheer, integratieoplossingen, data-uitwisseling, consultancy en managed services. Afhankelijk van de aard van de opdracht kunnen onder meer de volgende categorieën persoonsgegevens worden verwerkt:

- Contactgegevens (e-mail, telefoon)
- Identifiers (klant-ID, personeelsnummer)
- Gebruikersgegevens (accounts, loggegevens)

De exacte categorieën persoonsgegevens verschillen per opdracht en worden in samenspraak met de opdrachtgever vastgesteld en vastgelegd in de betreffende overeenkomst, offerte of opdrachtbevestiging

- Bij alle diensten is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. Bijzondere persoonsgegevens alleen indien expliciet toegestaan door opdrachtgever.

6. Privacy by design/privacy by default

Agyle past privacy by design en privacy by default toe binnen haar dienstverlening. Hierbij worden privacy- en beveiligingsvereisten vanaf de ontwerpfase meegenomen in de ontwikkeling, implementatie en het beheer van systemen en applicaties. Dit wordt onder meer gerealiseerd door:

- Dataminimalisatie en verwerking van uitsluitend noodzakelijke persoonsgegevens;
- Autorisatie op basis van rollen en het least-privilege-principe;
- Logische scheiding van klantomgevingen en klantgegevens (tenant-isolatie);
- Beveiligde standaardconfiguraties (secure by default);
- Logging en monitoring van toegang en wijzigingen;
- Toepassing van beveiligingsmaatregelen tijdens softwareontwikkeling volgens gangbare security best practices, waaronder secure coding principes en relevante OWASP-richtlijnen;
- Periodieke evaluatie van beveiligings- en privacymaatregelen op basis van risico's en wijzigingen in de dienstverlening.

Voor zover de opdrachtgever specifieke inrichting, doeleinden van verwerking of categorieën persoonsgegevens bepaalt, blijft de opdrachtgever verantwoordelijk voor de juiste toepassing van privacy by design en privacy by default binnen die verwerking.

7. Data processor gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn.

8. Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.

9. Data processor maakt gebruik van de volgende sub-processors:

Agyle maakt gebruik van Kropman als subverwerker.

Klantgegevens en medewerkergegevens worden verwerkt in ERP/HRM bij Kropman.

Kenmerken:

- Verwerking binnen EU/EER of met passende waarborgen
- Contractueel geborgd gelijkwaardig beveiligingsniveau
- Wijzigingen worden gecommuniceerd via Data Pro Statement

10. Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:

Agyle ondersteunt opdrachtgever bij verzoeken van betrokkenen met betrekking tot:

- Inzage in persoonsgegevens;
- Correctie of aanvulling van persoonsgegevens;
- Verwijdering van persoonsgegevens;
- Beperking van de verwerking;
- Dataportabiliteit, voor zover dit technisch mogelijk is binnen de betreffende dienstverlening.

Agyle verleent op verzoek van opdrachtgever redelijke medewerking door relevante persoonsgegevens beschikbaar te stellen, gegevens te corrigeren of te verwijderen, dan wel technische ondersteuning te bieden bij het exporteren van persoonsgegevens in een gangbaar en machineleesbaar formaat. Verzoeken van betrokkenen worden door Agyle niet zelfstandig afgehandeld. Indien een betrokkene zich rechtstreeks tot Agyle wendt, wordt deze verwezen naar de verwerkingsverantwoordelijke (opdrachtgever), die verantwoordelijk blijft voor de beoordeling en afhandeling van het verzoek.

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

Agyle:

- Verleent medewerking aan DPIA's indien vereist
- Stelt informatie beschikbaar over verwerking, systemen en beveiliging

Opdrachtgever kan audits laten uitvoeren (conform overeenkomst), met inachtneming van vertrouwelijkheid en proportionaliteit. Inzageverzoeken en audits (alle inspanningen) moeten tegen commercieel tarief worden vergoed.

12. Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).

13. Retourneren van persoonsgegevens na beëindiging van de Overeenkomst

Afspraken over het retourneren van persoonsgegevens na beëindiging van de overeenkomst worden per opdracht in samenspraak met de opdrachtgever gemaakt. De wijze van retourneren is afhankelijk van de aard van de dienstverlening en wordt vastgelegd in de betreffende overeenkomst, offerte of opdrachtbevestiging. Daarna worden de persoonsgegevens verwijderd conform de gemaakte afspraken.

Beveiligingsbeleid

14. Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:

Agyle hanteert een risico-gebaseerde beveiligingsaanpak, passend bij de aard van de dienstverlening en de verwerkte persoonsgegevens.

Pseudonimisering en versleuteling

- Persoonsgegevens worden waar mogelijk gepseudonimiseerd, afhankelijk van de aard van de opdracht, de technische mogelijkheden en de doeleinden van de verwerking.
- Persoonsgegevens worden waar mogelijk versleuteld opgeslagen en versleuteld verzonden via actuele beveiligingsstandaarden.

Vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht

- Toegangsbeheer op basis van rollen en autorisaties.
- Multi-factor authenticatie waar technisch mogelijk.
- Logging en monitoring van systemen en activiteiten.
- Netwerksegmentatie en beveiligingsmaatregelen ter voorkoming van ongeautoriseerde toegang.
- Vulnerability management, patchbeheer en periodieke beveiligingsevaluaties.
- Security awareness en geheimhoudingsverplichtingen voor medewerkers.

Herstel bij incidenten

- Back-up- en herstelprocedures zijn ingericht om de beschikbaarheid van en toegang tot persoonsgegevens tijdig te kunnen herstellen na een technisch incident of beveiligingsincident.
- De effectiviteit van deze maatregelen wordt periodiek geëvalueerd en waar nodig aangepast op basis van risico's, dreigingen en wijzigingen in de dienstverlening.

Agyle past de beveiligingsmaatregelen aan op basis van risicoanalyses, actuele dreigingen en de stand van de techniek.

15. **Data processor heeft zich geconformeerd aan een Information Security Management System (ISMS), geborgd in/via:**
NIST Cybersecurity Framework 2.0
NIST SP 800 series
16. **Data processor heeft de volgende verificaties en certificeringen:**
N.V.T.

Datalekkenprotocol

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

Bij een beveiligingsincident:

- Wordt opdrachtgever **zonder onredelijke vertraging** geïnformeerd
- Worden minimaal de volgende gegevens gedeeld:
 - aard van het incident
 - getroffen systemen en data
 - mogelijke impact
 - genomen maatregelen

Bij constatering van een mogelijk datalek:

- melding **direct** aan:
 - Security verantwoordelijke
- registratie in incidentmanagementsysteem

Voorbeelden van incidenten:

- ongeautoriseerde toegang tot systemen
- verlies van data of backups
- ransomware waarbij data is geëxfiltreerd
- verkeerd verstuurde persoonsgegevens

De verwerkingsverantwoordelijke blijft verantwoordelijk voor melding aan de Autoriteit Persoonsgegevens. Het volledige datalekkenprotocol staat beschreven in het Datalekprotocol van Agyle Versie 1.0 (05-2026).