AllesOnline

Versie: 1.0

Verwerkersovereenkomst

AllesOnline B.V.

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):**
   AllesOnline B.V., Jan van der Heydenstraat 18, 2665 JA Bleiswijk. KvK 55765939, btw NL851852105B01.
   Voor vragen over dit Data Pro Statement of over gegevensbescherming is de contactpersoon privacy & security: Stefan Grevelink, stefan@allesonline.nl, telefoon 085 003 0302.

2. Dit Data Pro Statement geldt vanaf 8 juni 2026 (versie 1.0).
   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: Cluster 1 – Maatwerk webapplicatie- en softwareontwikkeling en applicatiebeheer (CMS-websites, webapplicaties, portals en webshops, inclusief onderhoud, consultancy en support); en Cluster 2 – Managed webapplicatie-hosting en infrastructuurbeheer. In de Overeenkomst tussen Data Processor en opdrachtgever is bepaald welke producten/diensten zijn afgenomen.

4. Omschrijving product(en)/dienst(en): AllesOnline ontwikkelt en beheert op maat gemaakte websites en webapplicaties, grotendeels op basis van het eigen content-managementsysteem (Cluster 1: softwareontwikkeling, onderhoud, applicatiebeheer en support), en verzorgt het hosten en beheren van deze webapplicaties op een managed Kubernetes-omgeving inclusief opslag, databases, e-mailafhandeling en back-ups (Cluster 2).

5. Uitsluitend bij specifieke maatwerktoepassingen is rekening gehouden met de verwerking van bijzondere persoonsgegevens (art. 9 AVG), gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (art. 10 AVG) of door de overheid uitgegeven persoonsnummers. Waar een opdrachtgever in zo'n maatwerktoepassing dergelijke gegevens verwerkt, richt AllesOnline die toepassing daarop in met passende aanvullende beveiligingsmaatregelen, worden daarover separate afspraken gemaakt en wordt de opdrachtgever ondersteund bij een eventuele DPIA.

6. **Privacy by design/privacy by default**
   AllesOnline faciliteert privacy by design/by default onder meer door dataminimalisatie (formulieren bevatten alleen de benodigde velden), versleutelde opslag van wachtwoorden, mogelijkheid tot twee-factor-authenticatie, een autorisatiemodel met rollen en rechten (standaard 'geen toegang'), verwijderfuncties en instelbare bewaartermijnen, en gescheiden ontwikkel-, acceptatie- en productieomgevingen. De eindverantwoordelijkheid voor privacy by design/by default ligt bij de opdrachtgever; AllesOnline adviseert hierin.

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 in beginsel binnen de EU/EER. Voor een beperkt aantal ondersteunende diensten — zoals error monitoring en bot-/spambescherming — vindt doorgifte naar de Verenigde Staten plaats; data processor heeft op de volgende manier geborgd dat een passend beschermingsniveau van toepassing is: Data processor heeft met de betreffende sub-verwerkers in de Verenigde Staten standaardbepalingen (Standard Contractual Clauses, SCC's) afgesloten en/of deze sub-verwerkers zijn aangesloten bij het EU-VS Data Privacy Framework, met dataminimalisatie. Het betreft: Sentry (error monitoring; standaard ingezet) en de Google-diensten reCAPTCHA (botbescherming van formulieren) en Maps (kaartweergave), die afhankelijk van de opdracht via een sleutel van data processor worden ingezet. Daarnaast staan enkele transactionele e-maildomeinen (Mailgun) nog op de US-regio en worden naar de EU-regio gemigreerd; in de tussentijd geldt voor deze doorgifte dezelfde waarborg (SCC's/DPF).

9. **Data processor maakt gebruik van de volgende sub-processors:**
   DigitalOcean (hosting, opslag, databases – regio Amsterdam, EU); Mach3Builders BV (SaaS CMS en hosting voor klantwebsites – Nederland, EU); TransIP (domeinregistratie/DNS en webhosting – NL, EU); Mailgun (transactionele e-mail – primair EU-regio; enkele resterende domeinen nog op US-regio, in migratie naar EU); SimpleBackups/SimpleStorage (database-back-ups – EU, Stockholm (Zweden)); Microsoft 365 (Exchange/Teams – ondersteunende e-mail- en supportcommunicatie waarbij incidenteel persoonsgegevens van betrokkenen kunnen worden verwerkt; EU Data Boundary); Sentry (error monitoring – VS, DPF/SCC's; standaard ingezet); Google reCAPTCHA en Google Maps (botbescherming respectievelijk kaartweergave – VS, DPF/SCC's; afhankelijk van de opdracht, via een sleutel van data processor). Door de opdrachtgever zelf gekozen of aangeleverde diensten (zoals een betaalprovider of een eigen OpenAI-sleutel) zijn directe verwerkers van de opdrachtgever.

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
    Data processor neemt geen zelfstandige beslissingen over verzoeken van betrokkenen, maar ondersteunt de opdrachtgever hierbij. Afhankelijk van de applicatie kan de opdrachtgever zelf gegevens inzien, exporteren, wijzigen of verwijderen; daarnaast kan via de helpdesk een verzoek tot export, aanpassing of verwijdering worden ingediend. Eventuele bijkomende kosten worden vooraf — dat wil zeggen vóór uitvoering van de werkzaamheden — kenbaar gemaakt.

11. **Data processor zal op de volgende wijze medewerking verlenen aan Data Protection Impact Assessments (DPIA):**
    Indien Opdrachtgever daartoe verplicht is, zal Data processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een Data Protection Impact Assessment (DPIA). Eventuele bijkomende kosten worden vooraf — dat wil zeggen vóór uitvoering van de werkzaamheden — kenbaar gemaakt.

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). Verwijdering omvat tevens de back-ups volgens de reguliere back-upcyclus.

13. Retourneren van persoonsgegevens na beëindiging van de Overeenkomst. Op verzoek van de opdrachtgever retourneert data processor de persoonsgegevens vóór verwijdering, in een gangbaar, machineleesbaar formaat (bijvoorbeeld een database-export). Hierover worden bij beëindiging nadere afspraken gemaakt; eventuele kosten worden vooraf — vóór uitvoering — kenbaar gemaakt.

Beveiligingsbeleid

14. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
    De getroffen beveiligingsmaatregelen zijn samengevat hieronder; de volledige uitwerking is vastgelegd in het interne informatiebeveiligingsbeleid van AllesOnline en is op verzoek beschikbaar voor de opdrachtgever:
    - Persoonsgegevens worden in de regel niet gepseudonimiseerd.
    - Wachtwoorden worden versleuteld (gehasht) opgeslagen; gegevensoverdracht verloopt versleuteld via TLS/SSL conform de NCSC-richtlijnen.
    - Vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht worden geborgd door toegangsbeheer met rollen/rechten (least privilege) en twee-factor-authenticatie, strikte scheiding van omgevingen (OTAP) en logische scheiding van klantdata, 24/7 logging en monitoring, bescherming tegen malware, patch- en vulnerabilitymanagement, waaronder periodieke kwetsbaarheidsscans (Greenbone) en — voor omgevingen met gevoelige gegevens — geautomatiseerde CVE-scanning, secure development met versiebeheer en tests, en een geheimhoudingsplicht voor medewerkers.
    - Bij een incident wordt de beschikbaarheid en toegang tijdig hersteld door back-ups met restore-mogelijkheid en waar technisch van toepassing redundant uitgevoerde infrastructuurcomponenten, ondersteund door 24/7 monitoring en een opschalingsprocedure.

15. Data processor hanteert een intern informatiebeveiligingsbeleid gebaseerd op de principes van een Information Security Management System (ISMS), conform de richtsnoeren van de Autoriteit Persoonsgegevens en de richtlijnen van het NCSC.

16. Data processor beschikt op dit moment niet over een formele privacy-verificatie of beveiligingscertificering. AllesOnline heeft een aanvraag ingediend voor het Data Pro Verified-keurmerk (toetsing en toezicht door SCOPE Europe). De aanvraag is op het moment van publicatie van dit Data Pro Statement nog in behandeling.

Datalekkenprotocol

17. **In geval er toch iets mis gaat, hanteert data processor het volgende datalekkenprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**
    Potentiële beveiligingsincidenten worden gesignaleerd via 24/7 logging en monitoring en via meldingen bij de helpdesk. Incidenten worden intern gemeld en geregistreerd in het datalekregister. Indien data processor een inbreuk in verband met persoonsgegevens ontdekt, stelt hij de opdrachtgever zonder onredelijke vertraging op de hoogte via de bekende contactpersoon, en levert hij zoveel mogelijk relevante informatie aan: omschrijving en aard van het incident, categorieën persoonsgegevens en betrokkenen, geschat aantal betrokkenen, tijdstip, mogelijke gevolgen en de getroffen en te nemen maatregelen. Data processor doet zelf geen melding aan de Autoriteit Persoonsgegevens of aan betrokkenen – dat is de verantwoordelijkheid van de verwerkingsverantwoordelijke; data processor ondersteunt daarbij desgewenst.