NLdigital

Versie: Augustus 2024

Verwerkers-overeenkomst Ivengi

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

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):**
   Ivengi.com, een handelsnaam van Ivengi Benelux BV, gevestigd te Maastricht aan het Withuisveld 24, 6226NV (KVK 14073759). Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met: privacy@ivengi.com of 088 20 23 900.

2. **Dit Data Pro Statement geldt vanaf 25 mei 2018**
   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. Laatste revisie augustus 2024.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor**
   Het leveren van een volledige web-/softwareapplicatie ontwikkeling, beheer en hosting.

4. **Omschrijving product/dienst**
   Ivengi.com biedt volledige ontwikkeling en beheer van webapplicaties, inclusief softwareontwikkeling, onderhoud, consultancy, applicatiebeheer en hosting, om uw digitale behoeften optimaal te ondersteunen met gebruik van het door Ivengi geïmplementeerde content management systeem.

5. **Beoogd gebruik**
   Product/dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:
   Het design en de beveiligingsmaatregelen van de door Ivengi ontwikkelde web-/software applicatie zijn geschikt voor algemeen gebruik en beheer. Deze zijn **niet** ontworpen voor gebruik van bijzondere persoonsgegevens, gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever. Voor diensten en producten die bijzondere persoonsgegevens verwerken dienen expliciet afspraken te worden gemaakt.

   De opdrachtgever laat de data processor de volgende gegevens verwerken in het kader van de opdracht:

   - NAW-gegevens
     - Telefoonnummer
     - E-mailadres
     - IP-adres (locatiegegevens)
     - Toegangs- of identificatiegegevens
     - Geslacht, geboortedatum en/of leeftijd.
     - Beeldmateriaal.

6. **Data processor heeft bij het ontwerpen van het product/de dienst privacy by design/privacy by default op de volgende wijze toegepast:**
Ivengi bouwt veilige web-/softwareapplicaties en zorgt voor beheer, en kan dat laten zien met een ISO27001 certificaat. Ivengi adviseert haar opdrachtgevers bij ontwerp gebruik te maken van privacy by design/ privacy by default. Ook stelt Ivengi by default bewaartermijnen in voor verzamelde data. De opdrachtgever kan echter van adviezen afwijken en de verantwoordelijkheid voor privacy by design/ privacy by default ligt uiteindelijk bij de opdrachtgever.

7. **Ivengi.com gebruikt de Data Pro Standaardclausules voor verwerkingen, zoals opgenomen in de NLdigital Voorwaarden 2020, "Hoofdstuk 2: Standaardclausules voor verwerkingen". De NLdigital Voorwaarden 2020 zijn als bijlage bij de Overeenkomst te vinden.**

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

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

Sub verwerker	Dienst	Certificaat	Verwerking binnen EU
Southern Hill	Connectiviteit & netwerk bescherming	Gecertificeerd ISO27001	Ja
Lemontree	Hosting/housing	Gecertificeerd ISO27001	Ja

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
Ivengi verwijst betrokkenen met een verzoek voor inzage, correctie, verwijdering, beperking van verwerking of transfer naar een ander systeem, altijd terug naar de opdrachtgever om daarover te beslissen. Ivengi heeft via haar helpdesk ondersteuning geregeld voor haar opdrachtgevers die hulp nodig hebben bij het uitvoeren van dit soort verzoeken.

11. **Data processor zal op de volgende wijze medewerking verlenen aan Data Privacy Impact Assessments:**
Medewerking aan een DPIA kan via een serviceverzoek worden aangevraagd.

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).**
Ivengi verstrekt standaard een eindbrief bij beëindiging van de overeenkomst en bevestigt hiermee de vernietiging van alle data en persoonsgegevens binnen deze termijn.

13. **Na beëindiging van de Overeenkomst met opdrachtgever kan data processor alle persoonsgegevens die hij voor opdrachtgever verwerkt binnen 3 maanden retourneren.**

Ivengi zal na opzegging van overeenkomst in overleg treden over de afwikkeling van de dienst en de overdracht van gegevens. Dit is een standaard procedure.

Beveiligingsbeleid

14. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
De vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de dienstverlening wordt met meerdere technische en organisatorische maatregelen geborgd. De doeltreffendheid van deze maatregelen wordt door een externe partij vastgesteld, hetgeen blijkt uit de ISO27001 certificering. De belangrijkste maatregelen worden hier opgesomd:

- Via logging en monitoring op systeem, netwerk en applicatie niveau wordt het systeem 24/7 in de gaten gehouden;
- Bescherming tegen malware en snel verhelpen kwetsbaarheden.
- Testen van security en functionaliteit is onderdeel van ontwikkelproces;
- Versiebeheer van ontwikkelde componenten;
- Housing omgeving met beveiliging zones middels firewalls;
- Voor alle applicaties wordt SSL encryptie gebruikt die voldoet aan de NCSC richtlijn;
- Gepersonaliseerde persoonlijke toegang en wachtwoord; 2 factor authenticatie is mogelijk.
- Een autorisatiemodel maakt inzichtelijk wie toegang heeft tot gegevens.
- Indien mogelijk ontwikkeling op OTAP omgeving;
- Verzorgen van een actuele back-up.
- Servers draaien in gecertificeerd rekencentrum; fysieke beveiliging, brand beveiliging, beveiliging tegen stroomuitval
- Ivengi personeel werkt onder geheimhoudingsverplichting. Er is blijvende aandacht voor veilige omgang met informatie.

Bij een incident wordt de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig hersteld op de volgende manieren:

- Helpdesk en support organisatie pakt alle externe signalen op en zorgt voor snelle oplossing.
- Systemen en netwerk worden 24/7 gemonitord, bij problemen worden de juiste technici geïnformeerd die storingen verhelpen.
- Bij ernstige problemen wordt er via afgesproken procedure opgeschaald naar management en senior technici.
- Back-up en redundant uitgevoerde systemen (voor opdrachtgevers die hier specifiek voor kiezen) bieden de mogelijkheid om na een storing snel weer in de lucht te zijn.
- Deze maatregelen worden getoetst door een externe controleur in het kader van de ISO 27001 certificering.

Persoonsgegevens worden in de websites en webapplicaties niet gepseudonimiseerd of versleuteld. Enkel passwords worden versleuteld opgeslagen.

Voor applicaties wordt default een korte bewaartermijn ingesteld die echter door de opdrachtgever aangepast kan worden naar eigen inzicht.

15. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**

    - ISO 27001
    - Privacy richtsnoeren van Autoriteit Persoonsgegevens (AP)
    - Richtlijnen van het Nederlands Cyber Security Center (NCSC)

16. **Data processor heeft de volgende certificeringen:**
    - Data Pro Verified
    - ISO 27001

Datalekprotocol

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

    In geval van datalek zal Ivengi contact opnemen met de bij ons bekende contactpersonen van opdrachtgever zonder onredelijke vertraging. .

In geval U een vermoeden van datalek wilt melden bij Ivengi zijn dit de mogelijkheden:

1. Servicedesk via de supportsite, 24/7: https://servicedesk.ivengi.com/
2. Servicedesk via support telefoon, tijdens kantooruren: 088 202 39 00

Het Ivengi respons-team wordt via email en sms op de hoogte gebracht van een melding in de supportsite. Afhankelijk van de urgentie van de melding nemen zij direct contact op of de eerstvolgende werkdag.

Ivengi heeft een datalekprotocol dat hier puntsgewijs is samengevat:

1. Een (vermoeden van) datalek wordt geregistreerd in het service portaal en gelabeld met ’datalek’ en krijgt daarmee meteen hoge prioriteit in de afhandeling.
2. De melding wordt direct doorgezet naar het crisisteam, de coördinator bepaalt, eventueel met hulp van de Functionaris Gegevensbescherming, of er sprake is van datalek binnen de verantwoordelijkheid van Ivengi.
3. Crisisteam bepaalt de aanpak die kan bestaan uit technische en/of organisatorische maatregelen, communicatie met opdrachtgevers of inroepen van externe hulp, bijvoorbeeld via de verzekering.
4. De operationele technici van het crisisteam voeren geplande maatregelen uit en koppelen voortgang terug aan het crisisteam. Zij stellen technisch bewijsmateriaal veilig, eventueel met externe hulp.
5. Crisis coördinator bereidt een eventuele melding aan opdrachtgevers voor aan de hand van het datalekprotocol.
6. Via afgesproken klantcontact kanalen worden opdrachtgevers zonder onredelijke vertraging op de hoogte gebracht van het datalek.

7. De gehele afhandeling wordt in het datalek dossier gedocumenteerd in het serviceportaal dat ook als datalek register dient.
8. Een datalek wordt altijd geëvalueerd, eventuele verbeteracties worden opgenomen in het verbeterplan Informatiebeveiliging & Privacy.