impactID
Tielweg 16
2803 PK Gouda

Tel. +31 (0)85 2021202
www.impactid.nl
info@impactid.nl

Verwerkersovereenkomst

Dit document vormt, samen met de Standaardclausules voor verwerkingen, zoals opgenomen in hoofdstuk 2 van de NLdigital voorwaarden, de verwerkersovereenkomst voor producten en diensten van impactID.

ALGEMENE INFORMATIE

1. **Deze Verwerkersovereenkomst geldt vanaf 1 april 2025**

   De in deze Verwerkersovereenkomst 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.

2. **Deze Verwerkersovereenkomst is van toepassing op de volgende producten en diensten van ImpactID:**

   Levering van impactID producten als SaaS dienst

   Hosting van impactID

   Service en Support op producten van impactID

3. **Omschrijving product/dienst**

   ImpactID biedt verschillende tools voor specifieke doeleinden binnen de goede doelen sector zoals een projectmanagementsysteem en fondsenwervende tools. Deze worden ingezet voor opdrachtgevers, zijnde Goede Doelen of organisaties die met haar activiteiten actief zijn met of voor Goede Doelen. Data Processor levert hiervoor service- en supportdiensten, zoals nader omschreven in de afgesloten overeenkomst. Data Processor levert producten van impactID als SaaS dienst, zoals nader omschreven in de SaaS overeenkomst, indien deze dienst wordt afgenomen.

4. **Beoogd gebruik**

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

   impactID biedt Software as a Service (SaaS) diensten en hieraan gerelateerde hosting diensten, service en support, aan Goede Doelen en aanverwante organisaties, waarin van diverse groepen betrokkenen persoonlijke gegevens worden vastgelegd.

   Bij deze producten/deze diensten is specifiek rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerking van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is ter eigen beoordeling door Opdrachtgever.

5. **Data processor heeft bij het ontwerpen van het product/de dienst *privacy by design* op de volgende wijze toegepast:**

De autorisatie tot het systeem is gebaseerd op aan gebruikers toe te wijzen gebruikersprofielen of betrokkenheden, die via rollen toegang verlenen tot specifieke (persoons)gegevens.
Tevens zijn in voorkomende gevallen (bijv. toegang tot persoonlijke gegevens van medewerkers) extra toegangscontroles ingericht.
Verder ondersteunt impactID, door middel van specifieke aanpassingen in het kader van de AVG, extra functionaliteit voor het borgen van de rechten van betrokkenen. Bij gebruik van producten van impactID als SaaS dienst is deze AVG functionaliteit beschikbaar.

6. **Data processor gebruikt de Standaardclausules voor verwerkingen, welke in hoofdstuk 2 van de NLdigital Voorwaarden zijn opgenomen.**

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

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

   1 – Matthat Software, gevestigd te Gouda

   2 – Ekco, gevestigd te Alkmaar

   3 – BRICC, gevestigd te Nijkerk

   4 – Microsoft, gevestigd te Ierland

   Met sub-processors is een subverwerkersovereenkomst aangegaan waarmee afspraken tussen Opdrachtgever en Data Processor ook voor sub-processors van toepassing zijn.

9. **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).**

   Data Processor zorgt voor het intrekken van eventuele toegangen tot de SaaS dienst.

10. **Gegevensoverdracht bij beëindiging van de overeenkomst:**

    Wanneer producten van impactID on-premise of anderszins door Opdrachtgever zijn geïnstalleerd, is Opdrachtgever zelf verantwoordelijk voor het zo nodig bewaren en installeren van een back-up om hieruit data beschikbaar te krijgen.
    Wanneer producten van impactID als SaaS service worden aangeboden, is Opdrachtgever zelf verantwoordelijk voor een download van de gegevens die zijn opgeslagen in de SaaS diensten vóór beëindiging van de overeenkomst. Hiervoor kunnen de beschikbare rapportage- en download functies worden gebruikt.
    Andere vormen van data overdracht kunnen aanvullend worden besproken.

BEVEILIGINGSBELEID

11. De in deze verwerkersovereenkomst 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.

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

a. Beveiliging van gegevens in de producten van impactID

Voor beveiliging van gegevens in de producten van impactID maakt data processor gebruik van de volgende beveiligingsmaatregelen:

a.1 Autorisatie

Iedere gebruiker krijgt in de producten van impactID een eigen account. Accounts worden ingedeeld in gebruikersgroepen. Met het product wordt een set standaard gebruikersgroepen uitgeleverd, waarmee de gebruikersgroep een set voor gedefinieerde rechten in het product heeft.

a.2. Logging

Producten van impactID bieden, in achterliggende databases, de mogelijkheid om mutaties te registreren. Dit betreft creatie en mutatie van objecten, waarbij wordt vastgelegd door welke gebruiker (account) en op welk tijdstip de mutatie is uitgevoerd. Voor SaaS klanten is rapportage met geregistreerde logs beschikbaar op aanvraag en tegen gangbare tarieven.

a.3. Beveiliging van gegevens

Alle informatie in de databases achter producten van impactID wordt automatisch versleuteld opgeslagen. Alle informatie in back-up bestanden van deze producten wordt eveneens automatisch versleuteld opgeslagen.

Communicatie tussen de database en alle web portalen en web services wordt versleuteld uitgewisseld. Alle web portalen en webservices die vanaf het internet bereikbaar zijn, kunnen uitsluitend via versleutelde gegevensuitwisseling worden gebruikt.

b. Beveiliging bij gebruik van service- en supportdiensten

Voor service- en supportdiensten kan impactID gebruikmaken van toegang tot systemen waarin opdrachtgever werkt, hierbij worden de volgende beveiligingsmaatregelen toegepast:

b.1. Meekijken en bediening overnemen

Voor het behandelen en kunnen oplossen van incidenten en wijzigingsverzoeken kan Opdrachtgever een verzoek aan Data Processor doen om mee te kijken met of de bediening over te nemen van de computer van een medewerker. Opdrachtgever is verantwoordelijk hierbij geen persoonsgegevens op het scherm te tonen. Wanneer dit in de aard van het werk

wel noodzakelijk is dan vermeldt opdrachtgever dit expliciet. Gegevens worden in deze situatie door Data Processor niet opgeslagen of anderszins verwerkt.

Opdrachtgever is zich bewust dat, wanneer Data Processor via deze techniek handelingen uitvoert, het systeem registreert dat deze handelingen zijn uitgevoerd door de medewerker van Opdrachtgever onder wiens naam op dat moment is aangemeld.

b.2.a Toegang tot de applicatie (alleen on-premise en hosting)

Voor het behandelen en kunnen oplossen van incidenten en wijzigingsverzoeken in producten van impactID die on-premise zijn geïnstalleerd, kan Data Processor genoodzaakt zijn onder een support account in de applicatie van Opdrachtgever aan te melden. Voor dit doel stelt Opdrachtgever toegangen beschikbaar op serverniveau waarmee de applicatie gestart kan worden (en niet meer dan dit), en in de applicatie waarmee voldoende rechten beschikbaar worden gesteld om de benodigde werkzaamheden te kunnen uitvoeren.

Afgegeven toegangen worden door Data Processor beheerd door de Support coördinator en dienst vervanger. Support medewerkers gebruiken deze voor het eigen werk, zonder zelf de toegangsgegevens te kennen.

Opdrachtgever hanteert een autorisatie procedure voor zowel de toegang op serverniveau als binnen de applicatie; Data Processor conformeert zich aan deze procedure. Data Processor hanteert voor de eigen medewerkers en externen die werken in haar opdracht, Two-Factor Authentication. Ook de mogelijkheid tot verbinding met systemen van Opdrachtgever zijn met deze toegang beveiligd.

b.2.b Toegang tot de applicatie (alleen SaaS)

Voor het behandelen en kunnen oplossen van incidenten en wijzigingsverzoeken in producten van impactID die als SaaS dienst worden aangeboden, kan Data Processor genoodzaakt zijn onder een support account in de applicatie van Opdrachtgever aan te melden. Data Processor hanteert voor de eigen medewerkers en externen die werken in haar opdracht, Two-Factor Authentication voor de aanmelding op het SaaS Cloud platform.

b.3.a Beheer toegang op de server (alleen on-premise)

Voor installatie, upgrade en onderhoud van componenten van de applicatie op de server kan Data Processor genoodzaakt zijn onder een beheer toegang op de server van Opdrachtgever aan te melden. Voor dit doel stelt Opdrachtgever één beheer toegang beschikbaar op server niveau, waarmee deze specifieke werkzaamheden kunnen worden uitgevoerd (en voor zover mogelijk niet meer dan dit).

Afgegeven toegangen worden door Data Processor beheerd door de Support coördinator en diens vervanger. Support medewerkers gebruiken deze voor het eigen werk, zonder zelf de toegangsgegevens te kennen.

Opdrachtgever hanteert een autorisatie procedure voor zowel de toegang op serverniveau als binnen de applicatie; Data Processor conformeert zich aan deze procedure. Data Processor hanteert voor de eigen medewerkers en externen die werken in haar opdracht, Two-Factor Authentication. Ook de mogelijkheid tot verbinding met systemen van Opdrachtgever zijn met deze toegang beveiligd.

b.3.b Beheer toegang op de server (alleen hosting en SaaS)

Voor installatie, upgrade en onderhoud van componenten van de applicatie op de server gebruikt Data Processor een beheer toegang op het Cloud platform.

Afgegeven toegangen worden door Data Processor beheerd door de Support coördinator en diens vervanger. Support medewerkers gebruiken deze voor het eigen werk, zonder zelf de toegangsgegevens te kennen.

c. Beveiliging bij gebruik van hosting en SaaS diensten

Voor hosting- en SaaS diensten maakt data processor gebruik van diensten van een gespecialiseerde IT partner, hierbij worden de volgende beveiligingsmaatregelen toegepast:

c.1.a Authenticatie (alleen hosting)

Voor toegang door medewerkers en partners van Opdrachtgever tot de hosted omgeving stelt Data Processor tenminste authenticatie met gebruikersnaam en wachtwoord verplicht. Het gebruik van Two Factor Authentication (verder afgekort tot 2FA) is beschikbaar in de hosting omgeving, Opdrachtgever kan dit laten toepassen. In dat geval is 2FA van toepassing op zowel de RDS toegang tot Pluriform client als op de toegang tot de webportalen die gekoppeld zijn aan Pluriform. 2FA wordt uitsluitend geactiveerd voor alle accounts van Opdrachtgever. De aanvullende kosten voor 2FA zijn voor rekening van Opdrachtgever.

c.1.b Authenticatie (alleen SaaS)

Voor toegang door medewerkers en partners van Opdrachtgever tot de web portal stelt Data Processor tenminste authenticatie met gebruikersnaam en wachtwoord verplicht. Het gebruik van Two Factor Authentication (verder afgekort tot 2FA) is beschikbaar en aanbevolen, Opdrachtgever kan dit laten toepassen. 2FA wordt uitsluitend geactiveerd voor alle accounts van Opdrachtgever. De aanvullende kosten voor 2FA zijn voor rekening van Opdrachtgever.

c.2. Beschikbaarheid (hosting en SaaS)

De hosting en SaaS diensten zijn standaard continu beschikbaar. Als borging van deze beschikbaarheid is op de gehele omgeving, zowel op infrastructuur als op productie Pluriform servers en services, automatische monitoring actief.

Tenminste dagelijks wordt zowel een volledige back-up van de productie serversystemen als een data-back-up van de productie Pluriform databases gemaakt, deze back-ups worden naar een tweede locatie gerepliceerd.

Binnen het Cloud platform zijn voorzieningen opgenomen om bij uitval van een component door te kunnen werken. Automatische fail-over zorgt dat bij uitval van een component binnen de infrastructuur automatisch het werk door een vervangende component wordt overgenomen.

DATALEKPROTOCOL

13. 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:

Data processor informeert Opdrachtgever op passende wijze, zonder onredelijke vertraging doch uiterlijk binnen twee werkdagen, nadat hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens. Hiertoe wordt zo mogelijk telefonisch contact gezocht met de functionaris voor gegevensbescherming of de privacy verantwoordelijke van Opdrachtgever, of als deze niet aanwezig is bij een nader door Opdrachtgever aan te wijzen contactpersoon. Na eventueel telefonisch contact wordt het contact per e-mail bevestigd.
In de melding voorziet Data processor aan Opdrachtgever tenminste de volgende informatie:

- aard van de inbreuk in verband met persoonsgegevens;
- de persoonsgegevens en betrokkenen die het betreft;
- waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- maatregelen die Data processor voorstelt of heeft genomen in verband met de inbreuk, als van toepassing ter beperking van eventueel nadelige gevolgen hiervan, en ter voorkoming van nieuwe inbreuken.

14. In geval opdrachtgever constateert dat iets mis gaat in relatie tot verwerking door data processor, hanteert opdrachtgever het volgende protocol om ervoor te zorgen dat data processor op de hoogte is van incidenten:

Opdrachtgever informeert Data processor op passende wijze, zonder onredelijke vertraging, nadat Opdrachtgever kennis heeft genomen van een inbreuk in verband met persoonsgegevens waarbij Data processor betrokken is. Hiertoe wordt zo mogelijk telefonisch contact gezocht met privacy contactpersoon van Data processor, in deze rol is Gert van Ramshorst uw aanspreekpunt. Na eventueel telefonisch contact wordt het contact per e-mail bevestigd aan het mailadres privacy@impactID.nl.