Versie: 1.3/ 2024-07-17

Verwerkers-overeenkomst MindYourPass B.V.

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):**
   MindYourPass B.V.
   High Tech Campus 27
   5656 AE Eindhoven

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

   Fabian Doodkorte
   fabian.doodkorte@mindyourpass.com
   06-10983764

2. **Dit Data Pro Statement geldt vanaf** 2024-07-17
   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 eventuele nieuwe versies via onze website. Tevens sturen wij deze nieuwe versies naar onze opdrachtgever(s) op.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor**

   MindYourPass Password Firewall
   MindYourPass Cyber Dashboard
   MindYourPass Password Generator B2B

4. **Omschrijving product/dienst**
   Deze verwerkersovereenkomst betreft de volgende drie producten van MindYourPass. Gezamenlijk worden deze hierna ook aangeduid als **'onze/deze producten'**. Wanneer bepaalde specificaties in deze verwerkersovereenkomst slechts van toepassing zijn op één van de producten van MindYourPass zal dit worden aangegeven.

   MindYourPass Password Firewall. Deze applicatie, bedoeld voor B2B-relaties, monitort waar ingelogd wordt en wat de kwaliteit van de gebruikte wachtwoorden is. Afhankelijk van het door de opdrachtgever gekozen abonnement, kan het de toegang tot accounts met zwakke wachtwoorden blokkeren.
   MindYourPass Cyber Dashboard. Deze applicatie, bedoeld voor B2B-relaties, geeft inzicht in de accounts die door de medewerkers van een organisatie gebruikt worden en de kwaliteit van de gebruikte wachtwoorden. Tevens geeft deze applicatie inzicht in de ontwikkeling na verloop van tijd van de cyberveiligheid op het gebied van onlineaccounts.
   MindYourPass Password Generator B2B. Deze applicatie, bedoeld voor B2B-relaties, genereert unieke en zeer sterke wachtwoorden uit o.a. een voor de gebruiker eenvoudig te onthouden wachtwoord.

Wachtwoorden worden steeds opnieuw gegenereerd op het moment dat de gebruiker wil inloggen. Hierdoor hoeven de gegenereerde wachtwoorden niet opgeslagen te worden.

5. **Beoogd gebruik**

Onze producten zijn ontworpen vanuit de concepten “Privacy by design” en “Security by design”. Om die reden worden gebruikers geanonimiseerd en worden e-mailadressen slechts tijdelijk opgeslagen en daarna verwijderd, en worden er geen andere persoonsgegevens opgeslagen. Deze overige gegevens die worden opgeslagen zijn license keys (in de vorm van global unique identifiers), URLs, kwaliteitsscores van wachtwoorden, client ID’s (in de vorm van global unique identifiers) en time stamps. Wij zien dit niet als persoonsgegevens. Indien en voor zover dit toch gezien wordt als het verwerken van persoonsgegevens is deze verwerkersovereenkomst van toepassing.

Mocht MindYourPass op enig moment het e-mailadres tijdens registratie en inloggen nodig hebben, dan zal het op dat moment de gebruiker vragen deze gegevens te verstrekken. MindYourPass gebruikt deze gegevens dan alleen voor het uitvoeren van de aangegeven handeling (zoals een inlog-procedure) en verwijdert deze gegevens daarna direct.

MindYourPass houdt bij deze producten geen rekening met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.

6. **Data processor heeft bij het ontwerpen van deze producten privacy by design/privacy by default op de volgende wijze toegepast:**

Onze producten zijn van de grond af aan zo ontworpen dat er geen persoonsgegevens opgeslagen hoeven te worden. Als persoonsgegevens nodig zijn worden deze op dat moment aan de gebruiker gevraagd, en nadat deze niet meer nodig zijn worden deze gegevens direct verwijderd. Zo wordt bijvoorbeeld tijdens registratie en inloggen om een e-mailadres gevraagd, maar wordt deze slechts tijdelijk opgeslagen en verwijderd zodra het account is aangemaakt of er is ingelogd.
Anders dan een traditionele wachtwoordmanager, slaat MindYourPass via het product Password Generator B2B geen wachtwoorden op maar genereert het deze opnieuw op het moment dat ze nodig zijn. Er is dus geen sprake van een (digitale) kluis met bijbehorende risico’s.
Omdat MindYourPass geen persoonsgegevens opslaat, kan in de producten gebruik worden gemaakt van one-way versleuteling (hashing). Dit is significant veiliger omdat er (per definitie) geen sleutel bestaat om de versleutelde informatie te ontsleutelen. Bij onze producten worden gebruikersnamen gepseudonimiseerd door daar license keys voor te genereren. De opdrachtgever bewaart de koppelingen tussen de license keys en de gebruikersnamen. MindYourPass heeft alleen toegang tot de license keys, niet tot deze koppelingen. De opdrachtgever is zelf verantwoordelijk voor een veilige en adequate beveiliging van de koppelingen.

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

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

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

Sub-processor	**Doelbinding**	**Data binnen EU/EER**	**Maatregelen gegevensbescherming**
MailJet (https://mailjet.com/).	Verwerking van e-mailadressen via MindYourPass Password Generator B2B	Ja	https://www.mailjet.com/security-privacy/
Google Cloud (https://cloud.google.com/)	Hosting MindYourPass producten en data-opslag	Ja	https://privacy.google.com/intl/nl/businesses/

10. **MindYourPass ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
Opdrachtgever kan door middel van het sturen van een e-mail naar info@mindyourpass.com een verzoek tot inzage, correctie, verwijdering of dataportabiliteit indienen bij MindYourPass. Bij een dergelijke verzoek neemt MindYourPass binnen 3 werkdagen contact op met opdrachtgever ter afstemming van het verzoek.

11. **MindYourPass zal op de volgende wijze medewerking verlenen aan Data Privacy Impact Assessments:**
MindYourPass verleent, zo volledig mogelijk en voor zover redelijkerwijs van data processor verwacht kan worden, medewerking aan het uitvoeren van een Data Privacy Impact Assessment (DPIA). Hierin ondersteunt MindYourPass de uitvoer van het DPIA door het verstrekken van alle benodigde informatie over door data processor genomen beveiligingsmaatregelen ter waarborging van de privacy bij gegevensverwerking.

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), of zullen deze persoonsgegevens op verzoek binnen 3 maanden worden geretourneerd.**
Behalve bij het registreren en het inloggen verwerkt MindYourPass geen persoonsgegevens. Het e-mailadres dat tijdens registratie en inloggen gebruikt wordt, wordt tijdelijk opgeslagen en daarna verwijderd. Indien en voor zover opdrachtgever van mening is dat MindYourPass overige persoonsgegevens verwerkt, worden deze na beëindiging van de Overeenkomst met een opdrachtgever in principe binnen 3 maanden op zodanige wijze verwijderd dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible). Tevens kunnen op verzoek de gegevens na beëindiging van de Overeenkomst met opdrachtgever geretourneerd worden. Data processor zal dan per e-mail een zipfile sturen met de betreffende gegevens.

13. **Met de opdrachtgever zijn geen specifieke afspraken gemaakt omtrent het retourneren van door data processor verwerkte persoonsgegevens.**

Beveiligingsbeleid

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

- *Hoe wordt vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van het product of de dienst geborgd;*
  Vertrouwelijkheid en integriteit worden geborgd doordat MindYourPass niet over persoonsgegevens beschikt. Vertrouwelijkheid en integriteit komen hiermee nimmer in het geding. Beschikbaarheid en veerkracht worden geborgd doordat MindYourPass een volledig schaalbare oplossing is die op basis van state-of-the-art technologieën in de Cloud draait. Hierbij vormt MindYourPass zelf een SaaS-oplossing, maar maakt deze intern gebruik van PaaS oplossingen (Kubernetes). Hierdoor kan MindYourPass beschikken over alle in gebruik zijnde mechanismen om de beschikbaarheid en de veerkracht van MindYourPass te kunnen waarborgen. Zie ook onder punt 6 hoe MindYourPass privacy by design/privacy by default waarborgt.

- *Hoe wordt geborgd dat bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig hersteld wordt.*
  MindYourPass draait als een verzameling microservices in een Kubernetes cluster. Het Kubernetes cluster wordt gehost bij Google in een Nederlands datacentrum. Deze opzet zorgt ervoor dat de beschikbaarheid van MindYourPass op alle mogelijke fronten gewaarborgd wordt. Mocht er toch een incident plaatsvinden dan biedt deze opzet tevens uitgebreide mogelijkheden om een incident te identificeren en om alle services operationeel te houden en/of weer in de lucht te brengen. MindYourPass is ontworpen om zoveel mogelijk gebruik te maken van standaard oplossingen die zich in de praktijk bewezen hebben. MindYourPass heeft hiervoor ook externe deskundigheid ingeschakeld om ontwerpen te maken en/of de bestaande ontwerpen en implementaties te valideren.

15. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**
MindYourPass is sinds 18 december 2023 ISO27001:2022 gecertificeerd welke dienst doet als ISMS. Daarnaast heeft MindYourPass de ambitie om in de toekomst aan meerdere normeringen te voldoen. Momenteel volgt MindYourPass de volgende normeringen:
    - ISO27001:2022;
    - OWASP;
    - NCSC Webrichtlijnen.

16. **Data processor heeft de volgende certificeringen:**
MindYourPass heeft de ambitie om aan meerdere certificeringen te voldoen. Momenteel beschikt MindYourPass reeds over de volgende certificering(en):
    - Data Pro Certificaat
    - ISO27001:2022
    - ISAE 3000

Datalekprotocol

17. **In geval er toch iets misgaat, hanteert data processor een datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten.**
MindYourPass heeft een intern datalekkenprotocol vastgesteld om datalekken te ontdekken, te voorkomen en te dichten. In het geval van een datalek zal MindYourPass haar opdrachtgevers per e-mail en/of telefoon op de hoogte stellen van het incident. MindYourPass zal zelf geen meldingen doen van een datalek aan de AP of aan betrokkenen. Het wel of niet melden aan hen blijft de verantwoordelijkheid van de opdrachtgever.

MindYourPass zal de opdrachtgever desgewenst en voor zover mogelijk ondersteunen bij het meldproces, door de volgende informatie (wanneer van toepassing) te delen met opdrachtgevers:
- specificatie van het incident
- samenvatting van het incident
- eventueel betrokken sub-processors
- hoeveel personen er zijn betrokken bij het datalek
- omschrijving van de groep betrokkenen bij het datalek
- tijdstip van het datalek
- aard van het datalek
- om welke type persoonsgegevens het gaat
- welke gevolgen de inbreuk kan hebben voor de persoonlijke levenssfeer van betrokkenen
- de vervolgacties naar aanleiding van het datalek
- de gehanteerde technische beschermingsmaatregelen ten tijde van het ontdekken van het datalek
- eventuele internationale aspecten

Deel 2: Standaardclausules voor verwerkingen

Versie: september 2019

Vormt samen met het Data Pro Statement de verwerkersovereenkomst en is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden.

Artikel 1. Definities

Onderstaande begrippen hebben in deze Standaardclausules voor verwerkingen, in het Data Pro Statement en in de overeenkomst de volgende betekenis:

1.1 **Autoriteit Persoonsgegevens (AP):** toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 Avg.
1.2 **Avg:** de Algemene verordening gegevensbescherming.
1.3 **Data Processor**: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.
1.4 **Data Pro Statement**: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, sub-processors, datalekken, certificeringen en omgang met rechten van Data subjects.
1.5 **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon.
1.6 **Opdrachtgever:** partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.
1.7 **Overeenkomst**: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.
1.8 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.
1.9 **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 Avg.

Artikel 2. Algemeen

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.
2.2 Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.
2.3 Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.

2.4 Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de Avg, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de Avg en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de Avg zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de Avg voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de Avg handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor.

Artikel 3. Beveiliging

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico's en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten of door de overheid uitgegeven persoonsnummers.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

Artikel 4. Inbreuken in verband met Persoonsgegevens

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 Avg) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

4.2 Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 Avg moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 Avg.

4.4 Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

Artikel 5. Geheimhouding

5.1 Data Processor waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

Artikel 6. Looptijd en beëindiging

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

6.2 Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen aan Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de Avg is ten aanzien van de Persoonsgegevens.

Artikel 7. Rechten Data subjects, Data Protection Impact Assessment (DPIA) en Auditrechten

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 Avg.

7.3 Data Processor zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

7.4 Data Processor kan desgewenst de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of een daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige, indien hij over een dergelijk certificaat of auditrapport beschikt.

7.5 Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de Avg of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.6 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.7 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

Artikel 8. Sub-Processors

8.1 Data Processor heeft in het Data Pro Statement vermeld of, en zo ja welke derde partijen (sub-processors of subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere sub-processors in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

8.3 Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

Artikel 9. Overig

Deze Standaardclausules voor verwerkingen vormen tezamen met het Data Pro Statement een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst.

NLdigital
De Corridor 5
3621 ZA Breukelen

info@nldigital.nl
+31 (0) 348 - 49 36 36

KVK 3017 4840

NLdigital