Blue 10 B.V.
Oude Middenweg 17
2491 AC Den Haag | NL

T +31 (0) 88 258 31 00
blue10@blue10.com
www.blue10.com

KVK 27195343
BTW NL809410199B01
ING Bank NL06INGB0683496832

DATA PRO STATEMENT
&
VERWERKERSOVEREENKOMST

Versie: 2.0
Datum: 8 januari 2021

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 Blue 10 B.V., verder te noemen: Blue10 of Data Processor.

Algemene informatie

1. **Dit Data Pro Statement is opgesteld door:**
   Blue10 B.V., gevestigd en kantoorhoudend aan de Oude Middenweg 17, 2491 AC, te Den Haag.
   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   - *Privacy contactpersoon:* Marije van Schie / Marcel Duijvestijn
   - *E-mail:* privacy@blue10.com
   - *Tel:* +31882583100

2. **Dit Data Pro Statement geldt vanaf 08-05-2018.**
   De omschreven beveiligingsmaatregelen in dit Data Pro Statement worden aangepast op het moment dat de stand van de techniek en/of de genomen beveiligingsmaatregelen wijzigen. Blue10 houdt haar opdrachtgevers / klanten op de hoogte van nieuwe versies van dit document via e-mail en/of nieuwsbrief. Naast de Data Pro Statement en de Standaardclausules voor verwerkingen beschikt Blue10 ook over een Privacy Policy.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van Blue10:**
   Het Data Pro Statement is van toepassing op de Blue10 software, welke gebruikt wordt door opdrachtgever. De Blue10 software noemen we hier verder: de Blue10 dienst.

4. **Omschrijving product/dienst**
   Blue10 helpt organisaties met cloud software voor het automatiseren van administratieve processen, zoals de digitale verwerking van inkoop- en verkoopfacturen, pakbonnen en bonnetjes. Daarmee is Blue10 de assistent op de financiële administratie, waarbij gebruikers de controle en het overzicht houden over de verschillende administratieve processen binnen de organisatie.

   Met Blue10 komen boekingsdocumenten (facturen, pakbonnen en bonnetjes) in één systeem samen en worden naadloos verwerkt in de financiële administratie. Facturen kunnen bovendien eenvoudig rondgestuurd worden in de organisatie voor de gewenste goedkeuring en zijn in het digitale archief snel en eenvoudig terug te vinden. Met Blue10 heb je altijd en overal inzicht in jouw administratie.

5. **Beoogd gebruik**
   De Blue10 dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:
   - Voor de verwerking van boekingsdocumenten worden zowel kop- als detailgegevens verwerkt. Kopgegevens zijn: Administratienaam, leveranciersnaam (incl. Btw-, IBAN- en KVK-nummer), factuurnummer, factuurdatum, betaalcondities, boekingsperiodes, btw-codes en (totaal) bedragen. Detail-/boekingsgegevens zijn: grootboekrekeningen, kostenplaatsen en andere kosten(verbijzonderingen) van boekingen.
   - Een document wordt in zijn geheel uitgelezen/herkend met behulp van OCR-herkenning. De Blue10 dienst gebruikt deze data geautomatiseerd, zonder menselijke tussenkomst, voor het verwerken van documenten naar een financieel systeem en voor het terugvinden van documenten in de Blue10 Dienst. Op deze boekingsdocumenten kunnen zich persoonsgegevens bevinden, zoals contactpersonen of contactgegevens. Opdrachtgever bepaalt zelf welke documenten verwerkt worden in de Blue10 dienst. Blue10 controleert de gegevens niet en zal gegevens alleen inzien op verzoek van opdrachtgever, bijvoorbeeld als dat nodig is om een vraag, welke gesteld is aan de servicedesk van Blue10, te beantwoorden. Indien opdrachtgever meer gevoelige of bijzondere persoonsgegevens gaat verwerken met de Blue10 dienst, kan opdrachtgever ten behoeve van de toegangsbeveiliging van de Blue10 dienst een abonnement afnemen waarin SSO via Azure AD wordt aangeboden door Blue10.

Met behulp van SSO via Azure AD heeft opdrachtgever de mogelijkheid om zelfstandig de hoogte van het beveiligingsniveau in de authenticatie te bepalen.

- De genomen beveiligingsmaatregelen in de Blue10 dienst zijn geaudit op de richtlijn 3000, waarbij Blue10 beschikt over een SOC2 verklaring. Het is de verantwoordelijkheid van opdrachtgever om te bepalen of de genomen beveiligingsmaatregelen in de Blue10 dienst voldoende zijn voor de verwerking van de gegevens die opdrachtgever met de Blue10 dienst gaat verwerken.
- Opdrachtgevers van Blue10 zijn zelf verantwoordelijk voor de inrichting en het gebruik van de Blue10 dienst. Dat wil zeggen:
    - Opdrachtgever maakt zelf de diverse administraties/bedrijven aan in de Blue10 dienst en koppelt deze aan de administraties in het door hen gebruikte financieel systeem.
    - Opdrachtgever is zelf verantwoordelijk voor het aanmaken, beheren en het verstrekken van toegang aan gebruikers binnen de eigen organisatie in relatie tot het gebruik van de Blue10 dienst.
    - Ten behoeve van het gebruik van de Blue10 dienst door opdrachtgever, verkrijgt opdrachtgever de beschikking over inloggegevens voor de Blue10 dienst. Opdrachtgever is verantwoordelijk voor de sterkte van het wachtwoord en deugdelijk beheer en vertrouwelijkheid van deze inloggegevens.
    - Tijdens het gebruik van de Blue10 dienst verzorgt opdrachtgever zelf de upload van gegevens, inclusief door hen gekozen bijlagen. Opdrachtgever kan gegevens en documenten zowel wijzigen als verwijderen.

6. **Blue10 heeft bij het ontwerpen van de Blue10 dienst *privacy by design* op de volgende wijze toegepast:**
   Blue10 tracht voor het gebruik van de Blue10 dienst zo min mogelijk persoonsgegevens te verwerken en houdt in de Blue10 dienst alleen de gegevens bij die benodigd zijn voor de authenticatie van gebruikers in de Blue10 dienst, te weten: naam, e-mail adres en wachtwoord. Andere (persoons)gegevens van gebruikers zijn voor het gebruik van de Blue10 dienst niet relevant en worden daarom niet bijgehouden.

7. **Verwerkersovereenkomst**
   Blue10 gebruikt de Data Pro Standaardclausules voor verwerkingen, welke terug te vinden zijn in ‘DEEL 2: STANDAARDCLAUSULES VOOR VERWERKINGEN’ van Blue10 B.V.

8. **Verwerking binnen/buiten de EU**
   Blue10 en haar sub-processors verwerken de persoonsgegevens van haar opdrachtgevers binnen de EU/EER.

9. **Blue10 maakt gebruik van de volgende sub-processors:**
   Microsoft Ireland Operations Ltd.
   - De Blue10 dienst wordt gehost op het platform van Microsoft Azure, meer specifiek in de Azure regio’s West-Europa en Noord-Europa.
   - Meer informatie over de beveiliging van Microsoft: https://www.microsoft.com/nl-nl/security/default.aspx
   - Meer informatie over het privacy beleid van Microsoft: https://privacy.microsoft.com/nl-nl https://privacy.microsoft.com/nl-NL/privacystatement

   Google Ireland Ltd.
   - Meer informatie over de beveiliging van het Google Cloud Platform: https://cloud.google.com/security/compliance?hl=nl
   - Meer informatie over het privacy beleid van Google: https://policies.google.com/privacy?hl=nl

10. **Blue10 ondersteunt opdrachtgevers op de volgende manier bij verzoeken van betrokkenen:**
    - Inzage-, correctie- Dataportabiliteit- en verwijderverzoeken kan opdrachtgever zelf doorvoeren in de Blue10 dienst.
    - Bewaartermijnen
        - Opdrachtgever blijft ten alle tijden rechthebbende op zijn boekingsdocumenten en kan op ieder gewenst moment de verwerkte boekingsdocumenten in Pdf-formaat exporteren uit de Blue10 dienst, met een bestandsnaam waarin de verschillende kenmerken staan die bekend zijn in de Blue10 dienst, namelijk: Blue10-nummer, leveranciersnaam en factuurnummer.
        - Blue10 heeft als uitgangspunt voor de wettelijke, fiscale bewaartermijn, van boekingsdocumenten een periode van twaalf (12) jaar gekozen, zodat geen onderscheid gemaakt hoeft te worden tussen verschillende boekings-documenten met verschillende wettelijke, fiscale bewaartermijnen.
        - Op het moment dat de wettelijke bewaartermijn van boekingsdocumenten gepasseerd is, wordt de volgende procedure gevolgd:
            - Opdrachtgever krijgt een keuze of de betreffende boekings-documenten en bijbehorende data bewaard moeten blijven (tegen betaling) in de Blue10 dienst of dat deze documenten en bijbehorende data verwijderd mogen worden door Blue10.
            - Indien gekozen wordt voor het verwijderen van de betreffende boekingsdocumenten en bijbehorende data, wordt opdrachtgever in de gelegenheid gesteld om in een periode van dertig (30) dagen deze documenten te exporteren in Pdf-formaat, zoals hierboven beschreven.
            - Na deze 30 dagen ontvangt opdrachtgever een bericht, waarbij opdrachtgever gevraagd wordt om Blue10 uitdrukkelijk toestemming te geven voor het verwijderen van de betreffende boekingsdocumenten en bijbehorende data.
                - Indien opdrachtgever de toestemming voor het verwijderen van haar data uit de Blue10 dienst uitdrukkelijk heeft verleend aan Blue10, worden de boekingsdocumenten en bijbehorende data van opdrachtgever, welke de wettelijke, fiscale bewaartermijn van twaalf (12) jaar hebben gepasseerd, ten minste na dertig (30) dagen en uiterlijk na negentig (90), na de uitdrukkelijke toestemming van opdrachtgever tot verwijdering, definitief verwijderd uit de Blue10 dienst.
                - Indien deze toestemming door opdrachtgever niet wordt verleend, is Blue10 genoodzaakt om alsnog de bewaartermijn van de betreffende boekingsdocumenten en bijbehorende data van opdrachtgever te verlengen en worden de kosten, die op dat moment hiervoor van toepassing zijn, automatisch aan opdrachtgever berekend, tot het moment dat Blue10 de uitdrukkelijke toestemming tot verwijderen van de betreffende boekingsdocumenten en bijbehorende data van opdrachtgever heeft ontvangen en daadwerkelijk tot verwijdering kan overgaan.
        - Naast de documenten kan opdrachtgever diverse export-bestanden opmaken in Excel format, zoals gebruikersoverzichten met daarin gebruikersnamen en e-mail adressen van de gebruikers binnen de Blue10 dienst.

11. **Beëindiging van de overeenkomst**
    Na beëindiging van de overeenkomst met opdrachtgever verwijdert Blue10 alle gegevens van opdrachtgever binnen de Blue10 dienst, die hij voor opdrachtgever verwerkt heeft, in principe binnen drie (3) maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).

12. **Na beëindiging van de overeenkomst kan opdrachtgever zijn gegevens zelf exporteren uit de Blue10 dienst**
    Bij beëindiging van de overeenkomst voor gebruik van de Blue10 dienst, wordt de volgende procedure gevolgd.
    - Opdrachtgever heeft bij beëindiging van de overeenkomst voor gebruik van de Blue10 dienst twee mogelijkheden:
        - Een export maken van de verwerkte boekingsdocumenten (in Pdf-formaat) in de Blue10 dienst.
        - Een zogenaamd 'inkijk-abonnement' (tegen betaling) afsluiten bij Blue10, waarmee de data van opdrachtgever in de Blue10 dienst beschikbaar blijft zolang als dat het inkijk-abonnement actief is.
    - Nadat de beëindiging van het abonnement van opdrachtgever geregistreerd is bij Blue10, heeft opdrachtgever dertig (30) dagen de tijd om een export te maken van de boekingsdocumenten (in Pdf-formaat) die opdrachtgever verwerkt heeft in de Blue10 dienst. Opdrachtgever wordt hiervoor actief benaderd via geautomatiseerde e-mail berichten aan de bij Blue10 bekende primaire contactpersoon. Opdrachtgever wordt in deze e-mails tevens gevraagd om Blue10 uitdrukkelijk toestemming te geven voor het verwijderen van de betreffende boekingsdocumenten en bijbehorende data uit de Blue10-omgeving van opdrachtgever.
        - Indien opdrachtgever de toestemming voor het verwijderen van haar data uit de Blue10 dienst uitdrukkelijk heeft verleend aan Blue10, worden de boekingsdocumenten en bijbehorende data van opdrachtgever, ten minste na dertig (30) dagen en uiterlijk na negentig (90), na beëindiging van de overeenkomst, definitief verwijderd uit de Blue10 dienst.
        - Indien deze toestemming door opdrachtgever niet uitdrukkelijk wordt gegeven, is Blue10 genoodzaakt om de Blue10 dienst weer te activeren voor opdrachtgever, waarbij het inkijk-abonnement van de Blue10 dienst voor opdrachtgever wordt geactiveerd. Voor het inkijk-abonnement worden de dan geldende prijzen voor het inkijk-abonnement, aan opdrachtgever doorbelast, tot het moment dat Blue10 de uitdrukkelijke toestemming tot verwijderen van de betreffende boekingsdocumenten en bijbehorende data van opdrachtgever heeft ontvangen en daadwerkelijk tot verwijdering kan overgaan.

BEVEILIGINGSBELEID

13. **Blue10 heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
    Voor meer informatie over de beveiligingsmaatregelen rondom de Blue10 dienst wordt verwezen naar de Security & Availability Policy van Blue10.

14. **Blue10 heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**
    - SOC 2 / Richtlijn 3000
    - Data Pro Code van NL Digital

    Alle medewerkers bij Blue10, al dan niet werkend met (persoons)gegevens van opdrachtgevers van Blue10, hebben getekend voor strikte geheimhouding van alles wat hem omtrent de onderneming (Blue10) bekend is geworden en waaromtrent hem geheimhouding is opgelegd of waarvan hij het vertrouwelijke karakter redelijkerwijs kan vermoeden.

15. **Blue10 heeft de volgende certificeringen**
    - Blue10 beschikt over een SOC2 verklaring
    - Blue10 beschikt over een Data Pro certificaat van NL Digital

DATALEKPROTOCOL

16. **In geval er toch iets mis gaat, hanteert Blue10 het volgende datalekprotocol om ervoor te zorgen dat opdrachtgevers op de hoogte zijn van incidenten:**
    - Blue10 zal zich inspannen de hieronder nader uitgewerkte beveiligingsincidenten te melden aan opdrachtgever:
        - Het onrechtmatig verkrijgen van toegang tot de Blue10-omgeving van opdrachtgever door een niet geautoriseerde gebruiker / hacker;
        - Het onrechtmatig verkrijgen van (gebruikers)namen, e-mail adressen, wachtwoorden en/of andere contactgegevens van opdrachtgever door een derde.
    - Blue10 zal op het moment dat zij een beveiligingsincident ontdekt als volgt te werk gaan:
        - Indien Blue10 een beveiligingsincident ontdekt, wordt opdrachtgever zo snel als mogelijk op de hoogte gebracht van het incident;
        - Opdrachtgever wordt per e-mail geïnformeerd door Blue10;
        - Blue10 informeert bij een beveiligingsincident alleen de beheerder(s) die bekend is/zijn in de Blue10-omgeving van Opdrachtgever;
        - Een melding van een beveiligingsincident omvat de volgende kenmerken:
            - Samenvatting van het beveiligingsincident;
            - Datum melding en de datum waarop Blue10 op de hoogte is geraakt van het beveiligingsincident;
            - De manier waarop het beveiligingsincident zich heeft voorgedaan. Concreet: wat is de aard is van het beveiligingsincident en gaat het hierbij om lezen, kopiëren, veranderen, verwijderen/ vernietigen en/of diefstal van persoonsgegevens?
            - De (vermeende) oorzaak van het beveiligingsincident.
            - Indien bekend:
                - Omschrijving van de groep mensen van wie persoonsgegevens zijn betrokken bij het beveiligings-incident
                - Aantal personen getroffen door het beveiligingsincident
                - Type persoonsgegevens (Bijvoorbeeld: Namen, toegangs- of identificatiegegevens, financiële gegevens, bijzondere gegevens etc.)
            - Vervolgacties ter voorkoming en reparatie van het beveiligingsincident
        - Bij een beveiligingsincident kan opdrachtgever extra informatie vragen in het kader van zijn melding bij de servicedesk (support@blue10.com) van Blue10. In de melding van het incident door Blue10 wordt een specifieke contactpersoon benoemd voor opdrachtgever.

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.