Versie: 2.0 – maart 2024

Verwerkers-overeenkomst 2Jours 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

0. **Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):**
   2Jours B.V., gevestigd te Vrieswijk 3, 8103 PB Raalte. Geregistreerd bij de Kamer van Koophandel onder nummer 60949880.

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   M.A. Ruiter, telefoonnummer 0570-538135, e-mail: marcel@2jours.nl, of
   N.J. Koopman, telefoonnummer 0570-538135, email: niekjan@2jours.nl

1. **Dit Data Pro Statement geldt vanaf** 18 maart 2024, versie 2.0.
   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.

2. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor**
   Calculatiesoftware 2Jours.

3. **Omschrijving Calculatiesoftware 2Jours**
   Data Processor levert en ontwikkelt calculatiesoftware (SaaS) voor het doen van offerte-aanvragen bij onderaannemers en leveranciers, het maken van calculaties, het opstellen van offertes en planningen en het voeren van een projectadministratie. De software wordt geleverd aan bedrijven die actief zijn in de bouwnijverheid.

   Beoogd gebruik
   Data Processor verwerkt persoonsgegevens van gebruikers van de calculatiesoftware. Deze persoonsgegevens worden als volgt verworven;

   A. *Aanmelding voor een gratis demoversie van de calculatiesoftware*.
      De gebruiker vult een aanvraagformulier in, waarin de volgende persoonsgegevens worden vastgelegd:

      a) Geslacht
      b) Voornaam
      c) Achternaam
      d) Bedrijfsnaam
      e) Kamer van Koophandel nummer
      f) Adres
      g) Postcode
      h) Plaats

i) E-mailadres

j) Telefoonnummer of mobielnummer

k) Inloggegevens (gebruikersnaam en wachtwoord)

B. *(Potentiële) klant;*
Van (potentiële) klanten worden naast bij punt A genoemde persoonsgegevens, de volgende aanvullende persoonsgegevens bijgehouden:

a) Postadres

b) Btw- nummer (in verband met facturen versturen binnen de EU)

c) E-mail administratie (in verband met versturen van facturen)

d) Opleidingsplaats en jaar (alleen bij studenten)

e) IP- nummer

f) Het datum en tijdstip van het inloggen

g) Contactgeschiedenis

- Er worden gegevens verwerkt over het contact dat er is geweest met klanten
- Waarover het contact ging; aankoop in website of vraag
- Wanneer er contact was en met wie
- Hoe er contact is geweest (telefonisch, e-mail, via de website).

De calculatiesoftware is ontworpen en ingericht om er het volgende soort gegevens mee te verwerken:

C. *Gebruik calculatiesoftware*
In de calculatiesoftware kunnen gebruikers zelf de volgende persoonsgegevens vastleggen:

a) Bedrijfsnaam
b) Kamer van Koophandel nummer
c) Voorletters
d) Voornaam
e) Achternaam
f) Geslacht
g) Geboortedatum
h) Adres
i) Postcode
j) Plaats
k) Mobiel
l) Email
m) Datum in- uit dienst
n) Inloggegevens voor uren app
o) Nationaliteit
p) Burgerlijke staat
q) Burgerservicenummer (BSN)
r) IBAN

s) Nummer identiteitsbewijs

De calculatiesoftware is doorgaans essentieel voor de opdrachtgever om hun dagelijkse taken te kunnen verrichten. Een beperkt aantal medewerkers van de data processor kunnen in principe bij alle gegevens van de opdrachtgevers ten behoeve van onderhoud en support. Zij zullen, tenzij anders afgesproken geen persoonsgegevens toevoegen of wijzigen, maar slechts inzien om een (technisch) probleem te kunnen oplossen.

Bij de calculatiesoftware is rekening gehouden met de verwerking van bijzondere persoonsgegevens. Verwerken van deze gegevens met de calculatiesoftware door opdrachtgever is ter eigen beoordeling door opdrachtgever.

4. **Data Processor levert ook licenties aan opleidingscentra.**
De Klant is verantwoordelijk voor het aanleveren van een lijst met gebruikers. Klant is zelf verantwoordelijk voor schriftelijke toestemming van ouders of verzorgers van minderjarige studenten

5. **Data processor gebruikt de Standaardclausules voor verwerkingen**, welke in het tweede gedeelte van dit document zijn opgenomen en ook te vinden zijn op onze website: https://2jours.nl/avg

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

7. **Backups worden maximaal 3 maanden bewaard, daarna 1x per week tot maximaal een jaar**.

8. **Data processor maakt gebruik van de volgende sub-processors:**
   - Voor “Calculatiesoftware 2Jours” heeft Data Processor gekozen voor het datacentrum van Previder. De servers van Data Processor worden onderhouden door Let’s Develop:
     - https://previder.nl/verwerkersovereenkomst
     - https://www.letsdevelop.tech/over-lets-develop/algemene-voorwaarden/
   - Automatische incasso’s worden uitbesteed en uitgevoerd door Buckaroo en Mollie:
     - https://www.buckaroo.nl/algemene-voorwaarden
     - https://www.mollie.com/nl/privacy
   - Als boekhoudprogramma maakt 2Jours B.V. gebruik van Exact Online:
     - https://support.exactonline.com/community/s/knowledge-base#All-All-HNO-Landing-general-security-gdpr-gen-sec-gdprl
   - Indien een klant met een betaling in gebreke blijft, zal deze worden uitbesteed aan Gerechtsdeurwaarder Smit en Legebeke te Ommen.
   - Freshdesk wordt gebruikt als ticketsysteem.
     - https://www.freshworks.com/nl/freshdesk/gdpr/
   - Microsoft Office 365/Microsoft Dynamics
     - https://privacy.microsoft.com/nl-nl/privacystatement

9. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
Opdrachtgever kan een dataportabiliteitsverzoek mailen naar helpdesk@2jours.nl onder vermelding van ‘dataportabiliteitsverzoek’. Binnen 1 maand ontvangt opdrachtgever een schriftelijke reactie. Opdrachtgever heeft zelf de mogelijkheid om in de calculatiesoftware persoonsgegevens aan te passen of te verwijderen.

10. **Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 1 jaar op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**
Eén jaar na beëindigen van de overeenkomst wordt er door Data Processor contact opgenomen met de opdrachtgever om haar product of diensten opnieuw aan te bieden en ten behoeve van rapportage-doeleinden. Indien de opdrachtgever hier niet mee akkoord is, kan dit worden aangegeven bij het beëindigen van de overeenkomst. Data Processor zal dan binnen 3 maanden de persoonsgegevens verwijderen.

11. **Na beëindiging van de Overeenkomst met opdrachtgever kan data processor alle persoonsgegevens binnen 3 maanden retourneren, die hij voor opdrachtgever verwerkt op de volgende manier:**
Opdrachtgever dient hiervoor een schriftelijk verzoek in te dienen bij Data Processor. Data Processor zal alle persoonsgegevens binnen 4 weken retourneren aan opdrachtgever in een standaard Excel document. Het is mogelijk om de persoonsgegevens op een ander formaat te retourneren, hier zijn kosten aan verbonden.

Beveiligingsbeleid

12. **Datacentrum en hosting**
Producten en diensten van Data Processor worden gehost vanuit het datacentrum van Previder op Virtual Private Servers (VPS). Data Processor heeft gekozen voor de datacentra van Previder en deze is hiermee subverwerker van de klantdata. De fysieke locatie is Expolaan 50, 7556 BE Hengelo. Het datacentrum is ISO 9001, ISO 27001, ISO 14001 en NEN 7510 gecertificeerd.

De datacentra vallen onder Nederlandse wet- en regelgeving. Gebruikers kunnen namens de Verwerkingsverantwoordelijke alleen toegang krijgen tot de software via een beveiligde SSL-verbinding. Hierdoor wordt de mogelijkheid van ‘afluisteren’ door derden geëlimineerd.

Fysieke toegangscontrole kantoorgebouw
Het pand van 2Jours is voorzien van een alarmsysteem en camera toegangsbewaking.

Tweeweg- authenticatie
Gebruikers hebben de mogelijkheid om in te loggen middens een tweeweg authenticatie. Nadat authenticatie heeft plaatsgevonden middels een gebruikersnaam en wachtwoord, ontvangt de gebruiker een SMS code op haar/zijn mobiel welke ingevoerd moet worden op een aparte pagina. Na verificatie van de SMS code heeft de gebruiker toegang tot de producten/diensten van Data Processor. Indien de inloggegevens in handen komen van een derde, heeft deze ook het mobiele nummer nodig van de gebruiker om te kunnen inloggen. Gebruikers dienen contact op te nemen om tweeweg authenticatie te activeren.

Virussen en Malware
Data Processor beveiligt eigen apparatuur (zoals servers, switches en routers) en eigen randapparatuur (zoals werkstations en laptops) onder beheer van de data processor waarmee de data processor toegang

heeft tot de persoonsgegevens, door middel van firewalls, authenticatiemiddelen, het hanteren van `up-to-date` virussen, trojans en andere malware detectie software.

De Verwerkingsverantwoordelijke dient zelf zorg te dragen voor een toereikende virusscanner op haar eigen systeem. Data Processor kan niet voorkomen dat door het gebruik van een geïnfecteerd systeem, gegevens worden blootgesteld aan derden, of dat bestanden welke in de calculatiesoftware worden opgeslagen, het virus bij zich dragen. Data Processor draagt er zorg voor dat eventuele virussen afkomstig uit het netwerk van de gebruiker, niet kunnen propageren binnen de instantie van de producten/diensten van de Data Processor, of tussen verschillende instanties van Data Processor.

Isolatie van gegevens
De gegevens van de Verwerkingsverantwoordelijke zijn binnen de infrastructuur van Data Processor geïsoleerd. De database waar de gegevens in worden opgeslagen is niet direct via internet toegankelijk en kan alleen via de calculatiesoftware van Data Processor worden benaderd. De documenten en dossiers in de software zijn niet direct toegankelijk, waardoor eventuele virussen op het netwerk van een gebruiker niet zelfstandig kunnen propageren naar de desbetreffende documenten in de software. Daarnaast heeft iedere Verwerkingsverantwoordelijke een eigen database in plaats van één grote database. Hiermee probeert Data Processor te voorkomen dat wanneer een database of tabel crasht deze geïsoleerd is en geen impact heeft op overige Verwerkingsverantwoordelijken.

Monitoring
Let's develop monitort ongewone server- of netwerkactiviteit via real-time monitoring tools. Data Processor neemt in overleg met Let's develop, na het vaststellen hiervan indien noodzakelijk actie. In het geval dat de server onbereikbaar is, zullen medewerkers van Data Processor hier binnen enkele minuten automatisch van op de hoogte zijn. Hierdoor kan er indien noodzakelijk direct actie worden ondernomen.

Data Processor monitort wie op welk tijdstip inlogt en met welk IP nummer. Deze gegevens worden voor rapportagedoeleinden gebruikt en het opsporen van verdacht gebruik.

Medewerkers van Data Processor
Alle medewerkers van Data Processor die toegang hebben tot vertrouwelijke gegevens zijn contractueel verplicht om correct en vertrouwelijk met alle gegevens van de Verwerkingsverantwoordelijke om te gaan. Alle medewerkers als ook eventueel ingehuurde krachten hebben een geheimhoudingsverklaring getekend. Dit betreft alle communicatie met de Verwerkingsverantwoordelijke en indien van toepassing, de Persoonsgegevens van de klanten in de database. Een beperkt aantal medewerkers van Data Processor heeft toegang tot de software en de Persoonsgegevens van klanten. Deze toegang wordt uitsluitend gebruikt voor het leveren van support en onderhoud aan de software en servers en uitdrukkelijk niet voor het wijzigen van gegevens.

Het kan voorkomen dat medewerkers een back-up van de klant terug zetten op zijn of haar eigen systeem. Nadat deze back-up is teruggezet, worden persoonsgegevens geanonimiseerd. Indien persoonsgegevens nodig zijn om de klant te helpen, zal hier toestemming voor worden gevraagd. Nadat de klant geholpen is zal de back-up worden verwijderd door de medewerker.

Behoud persoonsgegevens
De Verwerkingsverantwoordelijke is zelf verantwoordelijk voor het verwijderen van Persoonsgegevens van oud-klanten na de voor hen geldende maximale bewaarperiode.

Melding beveiligingsincidenten
Data Processor zal zich inspannen de hieronder nader uitgewerkte beveiligingsincidenten te melden aan klant:

- Bij een DDOS (Distributed Denial of Service) aanval
- Daadwerkelijke datalekken
- Onbevoegde on site fysieke toegang tot het systeem.

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:**

Stap 1: Constateren van een datalek
Er is sprake van een 'inbreuk in verband met Persoonsgegevens' (hierna: datalek) als er een inbreuk is op de beveiliging die als gevolg of mogelijk gevolg heeft:

- vernietiging van Persoonsgegevens (bijvoorbeeld door brand of wissen); of
- verlies van Persoonsgegevens (bijvoorbeeld USB of laptop die kwijtraakt);
- of wijziging van Persoonsgegevens (zonder dat dit de bedoeling was);
- of ongeoorloofde verstrekking van Persoonsgegevens (bijvoorbeeld e-mail/bestanden verzonden aan verkeerde geadresseerde of onbedoelde CC's);
- of ongeoorloofde toegang tot doorgezonden/opgeslagen/anderszins verwerkte Persoonsgegevens (bijvoorbeeld door een hacker of een niet-bevoegd personeelslid).

Het maakt daarbij niet uit of sprake is van een opzettelijk datalek (zoals een hacker die zich ongeoorloofd toegang verschaft tot Persoonsgegevens) of dat er per ongeluk iets mis gaat (bijvoorbeeld door per ongeluk wissen van gegevens die niet gewist moesten worden). Het maakt wel uit of sprake is van Persoonsgegevens. Als er geen gevolgen zijn voor Persoonsgegevens, is er geen datalek.

Indien een datalek geconstateerd wordt, volgt Data Processor de volgende stappen in dit plan.

Stap 2: Crisisteam
Indien een datalek geconstateerd of vermoed wordt vormen de volgende personen het crisisteam. Het team bevat – zo mogelijk – de volgende expertise:

- Directie Serverbeheerder
- Let's develop

Eventueel en indien noodzakelijk zal deze team worden aangevuld met:

- ICT / netwerk-specialist
- Jurist
- Verzekeraar

Stap 3: Maatregelen om het (actieve) lek te stoppen of de gevolgen te beperken
In het geval er een datalek wordt geconstateerd, draagt Data Processor zorg om de schade te beperken. Indien Data Processor een datalek constateert zullen zal Data Processor hier actie op ondernemen door het gedeeltelijk of geheel blokkeren van toegang tot de software. In overleg kan op een later tijdstip de toegang weer gedeeltelijk hersteld worden. Ook zal de betrokken Verwerkingsverantwoordelijke binnen 24 uur na het ontdekken van de datalek worden ingelicht over het datalek en de status van het onderzoek hiernaar. Andere mogelijke acties ter beperking van de schade en stoppen van het datalek zijn na het constateren van het datalek zijn:

- Blokkeren van alle netwerkverkeer naar de servers
- Beperkt openstellen van netwerkverkeer naar de server voor analyse
- Het wijzigen van beheer- en onderhoudswachtwoorden
- Verplaatsen van data naar een veilige locatie
- Formatteren/herinstalleren systeem
- Zoeken (bijvoorbeeld bij kwijtgeraakte USB-stick of harde schijf)
- Remote wipe (bijvoorbeeld bij gestolen laptop)

Van alle belangrijke constateringen en genomen stappen zal Data Processor een log bijhouden.

Stap 4: Verzameling van informatie

1. Wat is het voor incident (kies er 1):
    a. Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met Persoonsgegevens kwijtgeraakt of gestolen;
    b. Brief of postpakket met Persoonsgegevens kwijtgeraakt of geopend retour ontvangen;
    c. Hacking, malware (bijv. ransomware) en/of phishing;
    d. Persoonsgegevens bij oud papier gezet;
    e. Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USB-stick);
    f. Persoonsgegevens per ongeluk gepubliceerd;
    g. Persoonsgegevens van verkeerde klant getoond in klantportaal;
    h. Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger.
    i. Overig;

2. Geef een samenvatting van het incident:
    <samenvatting>

3. Indien het incident plaatsvond bij een Sub-verwerker:
    <naam subverwerker>

4. Van hoeveel personen zijn Persoonsgegevens betrokken bij de inbreuk?
    - Minimaal: <vul aantal in>
    - Maximaal: <vul aantal in>

5. Wanneer vond de inbreuk plaats? (kies 1 optie en vul zo nodig aan)

a. Op (datum)

b. Tussen (begindatum) en (einddatum)
   - Nog niet bekend

6. Wat is de aard van de inbreuk? (meerdere opties mogelijk)

   a. Lezen (vertrouwelijkheid)

   b. Kopiëren

   c. Veranderen (integriteit)

   d. Verwijderen of vernietigen (beschikbaarheid)

   e. Diefstal

   f. Nog niet bekend

   g. Anders:

7. Om welk type Persoonsgegevens gaat het? (meerdere opties mogelijk)
   a. Naam-, adres en woonplaatsgegevens
   b. Telefoonnummers
   c. E-mailadressen of andere adressen voor elektronische communicatie
   d. Toegangs- of identificatiegegevens
   e. Financiële gegevens
   f. Burgerservicenummer (BSN)
   g. Paspoortkopieën of kopieën van andere legitimatiebewijzen
   h. Geslacht, geboortedatum en/of leeftijd
   i. Zorggegevens
   j. Diploma's
   k. Anders nl:

   Persoonsgegevens met informatie over

   a. Ras of etnische afkomst
   b. Politieke opvattingen
   c. Religieuze of levensbeschouwelijke overtuigingen
   d. Lidmaatschap van een vakbond
   e. Genetische gegevens
   f. Biometrische gegevens met het oog op unieke identificatie van een persoon
   g. Gezondheid
   h. Iemands seksueel gedrag of seksuele gerichtheid
   i. Strafrechtelijke veroordelingen of strafrechtelijke feiten
   j. Onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
   k. Iemands godsdienst of levensovertuiging
   l. Overige, <toelichting>
   m. Onbekend

Toelichting:

<toelichting in geval van toepassing>

Stap 5: Informeren Verwerkingsverantwoordelijke

Indien Verwerkingsverantwoordelijke over een Data Protection Officer / Functionaris van de Gegevensbescherming beschikt zal de melding tenzij anders is afgesproken bij deze gemeld worden als contactpersoon. In overleg kan door de Verwerkingsverantwoordelijke (ook) een contactpersoon worden

aangewezen welke ook buiten kantoortijden beschikbaar is. Als er geen contactpersoon is aangewezen of de contactpersoon niet bereikbaar is, zal Data Processor zich inspannen om een Verantwoordelijke binnen de organisatie van de Verwerkingsverantwoordelijke te bereiken via telefoon of e-mail. De Verwerkingsverantwoordelijke is zelf verantwoordelijk voor het melden bij het Autoriteit Persoonsgegevens (AP) van het datalek.

Een datalek zal per email met het onderwerp: “datalek melding” worden gemeld bij de contactpersoon van de Klant:

Contactgegevens van contactpersoon 1 van Verwerkingsverantwoordelijke:

Naam: ……..……..

Emailadres: ……..……..

Telefoonnummer: ……..……..

Contactgegevens van contactpersoon 2 van Verwerkingsverantwoordelijke:

Naam: ……..……..

Emailadres: ……..……..

Telefoonnummer: ……..……..

Inhoud van de melding: In de melding zullen de gegevens worden vermeld die in Stap 5 zijn verzameld:

Contactpersonen Data Processor

De contactpersoon vanuit Data Processor is Marcel Ruiter, bereikbaar per mail: marcel@2jours.nl en telefonisch op 0570 – 53 81 35.

Data Protection Officer is Niek-Jan Koopman, bereikbaar per e-mail: niekjan@2jours.nl en telefonisch: 0570-53 81 35.

Stap 6: Voorkomen van herhaling in de toekomst

Om herhaling te voorkomen zal er naar aanleiding van het onderzoek naar de datalek eventueel stappen genomen worden om te voorkomen dat het datalek zich nogmaals voordoet.

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.

Bijlage 2: Uitgangspunten privacybeleid en Data Pro Statement

De Data Pro Code vraagt om het invullen van een Data Pro Statement. Om tot een evenwichtige en toetsbare invulling van het Data Pro Statement te komen, zal een data processor een onderliggend privacybeleid moeten hebben. Dat privacybeleid kan hij nader invullen aan de hand van onderstaande algemene uitgangspunten. De uitgangspunten dwingen tot bewuste keuzes in de omgang met persoonsgegevens en stimuleren een veilige en verantwoorde omgang met gegevens.

Uitgangspunten

Uitgangspunt 1 - Omschrijving en beoordeling dienstverlening

De door de data processor aangeboden diensten of producten zijn door de data processor omschreven en beoordeeld, rekening houdend met de markt waarin hij opereert, het door de data processor beoogd gebruik van zijn dienst of product en daarmee de binnen of met zijn dienst of product verwachte aard van de te verwerken data en het aantal te verwerken data subjects.

Uitgangspunt 2 - Beleid en governance

De data processor heeft een gedocumenteerd beleid voor dataprotectie, waaronder een datalekprocedure.

Uitgangspunt 3 - Organisatie en middelen

De data processor heeft zijn dataverwerking in kaart gebracht.

Uitgangspunt 4 - Limitering gebruik

De data processor heeft geborgd dat de verkregen persoonsgegevens van zijn opdrachtgever uitsluitend worden verwerkt voor de verlening van zijn diensten aan die opdrachtgever.

Uitgangspunt 5 - Beveiliging van persoonsgegevens

5.1 De data processor heeft passende technische en organisatorische maatregelen getroffen om een beveiligingsniveau voor persoonsgegevens te waarborgen dat is afgestemd op het risico dat is verbonden aan het door de data processor beoogde gebruik van zijn dienst of product.

5.2 Bij de beoordeling van het passende beveiligingsniveau houdt de data processor rekening met de verwerkingsrisico's verbonden aan zijn dienst of product, met name ten aanzien van mogelijke gevolgen van vernietiging, verlies, wijziging of ongeoorloofde toegang tot persoonsgegevens binnen of via zijn dienst of product, hetzij per ongeluk hetzij onrechtmatig.

5.3 De data processor hanteert een information security management systeem, beveiligingsnorm of -standaard, waarbij is voorzien in een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de getroffen beveiligingsmaatregelen voor persoonsgegevens door de data processor (plan, do, check, act).

Toelichting op uitgangspunten

Hieronder wordt voor ieder uitgangspunt uitgewerkt wat eronder wordt verstaan en welke uitgangspunten of best practices daarbij nagestreefd worden.

Bij uitgangspunt 1 - Omschrijving en beoordeling dienstverlening

Een goede omschrijving van de diensten is de basis voor goede informatievoorziening en geeft de basis om tot een juiste risicoafweging te komen, waarop de gekozen beveiligingsmaatregelen gebaseerd moeten zijn. Het is daarom van belang om de volgende onderdelen intern uit te werken en daarin heldere keuzes te maken:

0. De data processor heeft het beoogd gebruik van zijn dienst of product helder omschreven.
1. De data processor heeft de verwachte aard van de te verwerken persoonsgegevens in of met zijn dienst of product omschreven (*ten minste aangeven: wel/niet bijzondere persoonsgegevens*).
2. De data processor heeft de markt waarin hij opereert beoordeeld en heeft zijn dienst of producten op die beoordeling afgestemd (privacy by design), daarbij rekening houdend met:
    - het aantal data-elementen per data subject (*dataminimalisatie*);
    - het verwachte aantal te verwerken data subjects (*minder of meer dan 100.000 betrokkenen*);
      het beoogde gebruik van zijn dienst of product (ten minste aangeven: is dienst of product wel/niet cruciaal in de bedrijfsvoering van een opdrachtgever; Deze beoordeling vormt een Data Protectie Impact Assessment (DPIA) op de dienstverlening).

Bij Uitgangspunt 2 - Beleid en governance

Compliance met de Avg vergt een intern privacybeleid. Onderstaande onderwerpen moeten daarbij aandacht krijgen:

0. De data processor heeft zijn keuze voor het niveau van door hem te treffen beveiligingsmaatregelen gedocumenteerd (*visie op dataprotectie*).
1. Bij de inrichting van zijn eigen dienst of product heeft de data processor maatregelen genomen om verwerking van niet-noodzakelijke persoonsgegevens bij het gebruik van zijn dienst of product te voorkomen (*privacy by design*).
2. De data processor weet in geval van een datalek hoe te handelen (*datalekprotocol*).
3. De data processor heeft een contactpersoon aangewezen voor dataprotectie die kennis heeft (of verkrijgt door opleiding) van dataprotectie.

Bij Uitgangspunt 3 - Organisatie en middelen

Voor de invulling van de informatieplichten en om een goede risicobeoordeling te kunnen geven, is inventarisatie van zowel toeleveranciers als klanten van groot belang. Denk daarbij aan de volgende onderdelen:

0. De data processor heeft de door hem gebruikte middelen en door hem ingezette leveranciers in kaart gebracht (*er is een overzicht van middelen en leveranciers ((sub)data processors) die nodig zijn voor zijn dienstverlening*).
1. De data processor heeft beoordeeld of de door hem gebruikte middelen en door hem ingezette leveranciers ((sub)data processors) voldoende waarborgen bieden ten aanzien van dataprotectie.
2. De data processor heeft een accurate contractadministratie (*kan daarmee voldoen aan de verwerkingsregisterplicht*).

Bij Uitgangspunt 4 - Limitering gebruik

Dataminimalisatie en limitering van gebruik van gegevens is verankerd in de Avg. Klanten zullen van data processors inzicht willen hoe dit geregeld is. Best practices hierbij zijn:

0. Persoonsgegevens van een opdrachtgever worden alleen gebruikt voor het uitvoeren van de overeenkomst met die opdrachtgever.
1. Persoonsgegevens van een opdrachtgever worden door de data processor gescheiden van persoonsgegevens van andere opdrachtgevers.
2. Medewerkers van de data processor is geheimhouding opgelegd van persoonsgegevens van een opdrachtgever.
3. De data processor zal persoonsgegevens na het einde van de overeenkomst met de opdrachtgever in een machineleesbaar formaat aan de opdrachtgever ter beschikking stellen indien dit is overeengekomen.
4. De data processor borgt dat persoonsgegevens van een opdrachtgever na het einde van de overeenkomst met die opdrachtgever of na voltooiing van een opdracht voor die opdrachtgever binnen drie maanden na het einde ervan worden verwijderd op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*).

Bij Uitgangspunt 5 - Beveiliging van persoonsgegevens

Misschien wel de belangrijkste verplichting van een data processor is het zorgen voor een passende beveiliging van de persoonsgegevens die hij verwerkt. In een snel veranderende wereld vergt een goed beveiligingsbeleid ook doorgaand onderhoud. Om een afweging te kunnen maken welke maatregelen passend zijn en hoe de beveiliging doorgaand kan worden bijgehouden, helpt het om de volgenden uitgangspunten te hanteren:

0. Data processor maakt gebruik van een in de branche erkend Information Security Management Systeem (ISMS), technische beveiligingsstandaard of checklist.
1. Data processor kiest aan de hand daarvan de beveiligingsmaatregelen die specifiek voor zijn product of dienst geschikt zijn.
2. De data processor heeft de volgende beveiligingsmaatregelen meegewogen in zijn keuzes :
    - pseudonimisering en versleuteling van persoonsgegevens;
    - het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
    - het vermogen om bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen (*back ups, redundantie*).
3. Bij de beoordeling van een passend beveiligingsniveau voor zijn dienst of product houdt de data processor rekening met:
    - de stand van de techniek;
    - de uitvoeringskosten;
    - de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van individuele data subjects;
    - de markt waarin hij opereert;
    - het aantal data-elementen per data subject en de verwachte aard van de te verwerken data (ten minsten aangeven: wel/niet bijzondere persoonsgegevens);
    - het verwachte aantal van te verwerken data subjects (ten minste aangeven: minder of meer dan 100.000 betrokkenen);

- het beoogde gebruik van zijn dienstverlening door een opdrachtgever (ten minste aangeven: is de dienstverlening wel/niet cruciaal in de bedrijfsvoering van een opdrachtgever).

4. Data processor legt de keuzes en genomen maatregelen vast in zijn dataprotectiebeleid.
5. Data processor legt de relevante delen van de beveiligingsmaatregelen vast in zijn Data Pro Statement, of ander document waarvan opdrachtgever kennis kan nemen.
6. Data processor doorloopt de opgestelde procedures van zijn dataprotectiebeleid zo vaak als nodig doch ten minste eens in de 12 maanden en in lijn met het gehanteerde ISMS.
7. Data processor zal de aanbevolen verbetermaatregelen na een controle doorvoeren voor zover redelijkerwijze van hem mag worden verwacht. Data processor documenteert de aanpassingen die volgen uit de doorlopen procedure in het dataprotectiebeleid.