2JOURS STANDAARD VERWERKERS-OVEREENKOMST

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Versie 1.0.0

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:

   2Jours B.V., gevestigd te 8107 AD Broekland aan de Van Dongenstraat 1.
   Geregistreerd bij de Kamer van Koophandel onder nummer 60949880.
   Verder te noemen: data processor

   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
   G.W. Gerritsen, telefoonnummer 0570-538135, email: gerben@2jours.nl.

2. Dit Data Pro Statement geldt vanaf 25 mei 2018

   De in dit Data Pro Statement 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.

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

4. Omschrijving producten/diensten
   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
   Producten en diensten zijn ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

   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 te vullen 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).

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

Het product/dienst 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 dit product/deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.

5. 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.

6. Data Processor gebruikt de Data Pro Standaardclausules voor verwerkingen, welke te vinden zijn op onze website: https://www.2jours.nl onder `Over 2Jours` en vervolgens AVG.

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

8. Backups worden maximaal 3 maanden bewaard. Het is mogelijk om andere afspraken te maken echter zijn hier wel kosten aan verbonden.

9. Data Processor gebruikt de Data Pro Standaardclausules voor verwerkingen, welke in het tweede gedeelte van dit document is opgenomen.

10. Data Processor maakt gebruik van de volgende Sub-verwerkers als het gaat om de Persoonsgegevens en overige data van Betrokkenen

    - Voor “Calculatiesoftware 2Jours” heeft Data Processor gekozen voor het datacentrum van Previder. De servers van Data Processor worden onderhouden door Netzozeker B.V..
    - Automatische incasso’s worden uitbesteed en uitgevoerd door Buckaroo.
    - Als boekhoudprogramma maakt 2Jours B.V. gebruik van Exact Online.
    - Indien een klant met een betaling in gebreke blijft, zal deze worden uitbesteed aan Gerechtsdeurwaarder Smit en Legebeke te Ommen.

11. 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).

    Na 1 jaar na beëindigen van de overeenkomst wordt er door Data Processor contact opgenomen met de opdrachtgever om haar product of diensten opnieuw te mogen aanbieden en voor 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.

12. Na beëindiging van de Overeenkomst met opdrachtgever kan de Data Processor alle persoonsgegevens voor opdrachtgever retourneren.

    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

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

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 subbewerker 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 heef 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 producten/diensten 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 producten/diensten 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

Netzozeker monitort ongewone server- of netwerkactiviteit via real-time monitoring tools. Data Processor neemt in overleg met Netzozeker, 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 wordt inlogt en met welk IP nummer. Deze gegevens worden voor rapportage doeleinden gebruikt en gebruikt om verdacht gebruik te kunnen opsporen.

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 zet 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

14. Data Processor is Data Pro Code compliant. Zodra de Data Pro Code certificering beschikbaar is zullen wij ons laten certificeren. Ieder jaar zal dit opnieuw worden getoetst door een onafhankelijke partij.

DATALEKPROTOCOL

15. 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: Netzozeker BV

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):
    - Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met Persoonsgegevens kwijtgeraakt of gestolen;
    - Brief of postpakket met Persoonsgegevens kwijtgeraakt of geopend retour ontvangen;
    - Hacking, malware (bijv. ransomware) en/of phishing;
    - Persoonsgegevens bij oud papier gezet;
    - Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USB-stick);
    - Persoonsgegevens per ongeluk gepubliceerd;
    - Persoonsgegevens van verkeerde klant getoond in klantportaal; -
    - Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger.
    - 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)

- Op (datum)
- Tussen (begindatum) en (einddatum)
  - Nog niet bekend

6. Wat is de aard van de inbreuk? (meerdere opties mogelijk)
- Lezen (vertrouwelijkheid)
- Kopiëren
- Veranderen (integriteit)
- Verwijderen of vernietigen (beschikbaarheid)
- Diefstal
- Nog niet bekend
- Anders:

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

Persoonsgegevens met informatie over
- Ras of etnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuigingen
- Lidmaatschap van een vakbond
- Genetische gegevens

- Biometrische gegevens met het oog op unieke identificatie van een persoon
- Gezondheid
- Iemands seksueel gedrag of seksuele gerichtheid
- Strafrechtelijke veroordelingen of strafrechtelijke feiten
- Onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
- iemands godsdienst of levensovertuiging
- overige, <toelichting>
- 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 Gerben Gerritsen, bereikbaar per e-mail: gerben@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.