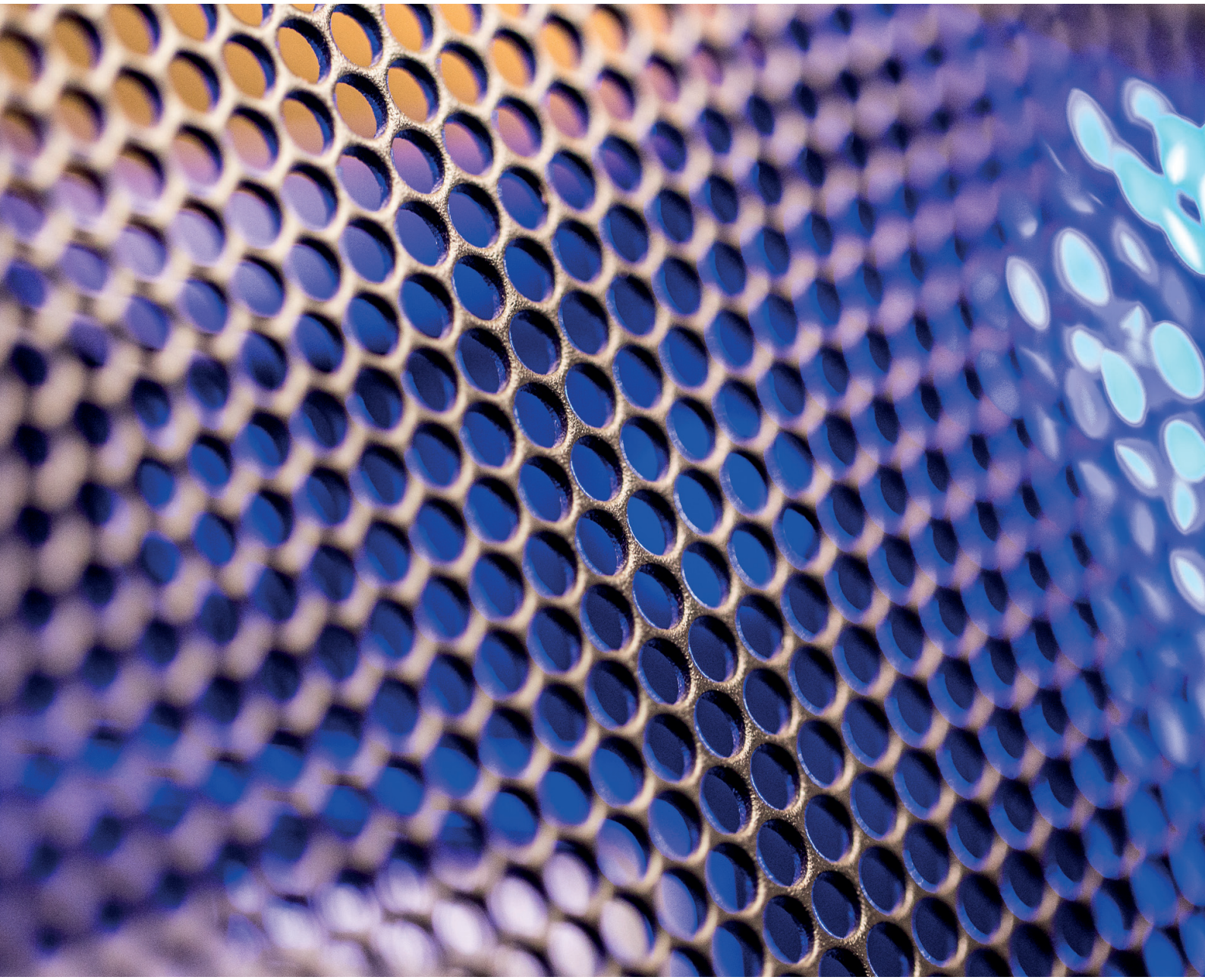
r@to
internetburo



Verwerkersovereenkomst

DATA PRO CREATED BY NEDERLAND ICT

Bestaande uit:
Deel 1. Data Pro Statement
Deel 2. Standaardclausules voor verwerkingen

Versie: 06-08-2018

meer @ffect!

Deel 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de Verwerkersovereenkomst voor de producten en de diensten van Reto.

Op het document 'Specificatie persoonsgegevens en betrokkenen' (Reto - Specificatie persoonsgegevens en betrokkenen.pdf) kunnen aanvullend soorten persoonsgegevens en de daar bijhorende categorieën worden opgegeven. Tevens geeft u middels dit document een functionaris op en ondertekend u hiermee de Verwerkersovereenkomst en Algemene Voorwaarden.

ALGEMENE INFORMATIE

1. Dit Data Pro Statement is opgesteld door:

Reto
Nieuwegracht 13
3763 LP Soest

KvK-nummer: 68968396

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

Reto
T.a.v. Functionaris Gegevensbescherming (FG)
Nieuwegracht 13
3763 LP Soest

+31 (0)35-603 23 05
persoonsgegevens@reto.nl

2. Dit Data Pro Statement geldt vanaf 1 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. Een actuele versie is te lezen en als PDF te downloaden op onze website:
https://www.reto.nl/verwerkersovereenkomst

3. Dit data Pro Statement is van toepassing op de volgende producten en diensten van Reto

- **Producten**
    - Buildix Enterprise SaaS (hierna te noemen Buildix)
    - Web & overige applicaties
    - Managed (Cloud) Services
    - Hardware & Supplies
- **Diensten**
    - Consultancy
    - Support
    - Maatwerkontwikkeling

4. Omschrijving producten/diensten A

1. **Buildix**
   Buildix is een modulair opgezet webbased management systeem, waarmee u de inhoud van uw online-omgeving zeer gebruiksvriendelijk op internet of uw intranet kunt onderhouden, beheren en publiceren zonder te beschikken over enige technische kennis. Buildix wordt gelicentieerd in verschillende pakketten en modules en vormen samen een flexibel bouwsysteem. Daarmee kunt u zelf uw totaalpakket samenstellen. Reto is 100% ontwikkelaar en eigenaar van Buildix. Lees meer over Buildix op: https://www.reto.nl/buildix-enterprise

2. **Web & overige applicaties**
   Naast genoemde softwarepakketten levert Reto aanverwante applicaties en web modules. Deze aanvullende applicaties en modules dienen altijd een specifiek doel en wisselt daarvoor doorgaans data uit met Buildix.

3. **Managed (Cloud) Services**
   Onder onze managed (cloud) services valt het geheel aan activiteiten met betrekking tot het faciliteren van de opslag van data en/of het uitvoeren van applicaties vanaf externe locaties (zoals een datacenter) inclusief de daarbij behorende ondersteunende diensten en maatregelen op het gebied van snelheid en beveiliging. Onze managed services worden vrijwel uitsluitend geleverd aan de afnemers van onze (maatwerk)softwareproducten.

Voorbeelden van services zijn:

- Reto Mail (inclusief webmail);
- Reto Matomo Statistieken;
- Reto AWStats Statistieken;
- Reto DNS-beheer;
- Reto CDN (static.reto.media);
- Reto MailCenter;
- Reto Back-up;
- Reto OwnCloud.

3. Hardware & Supplies
Reto business-unit IT levert hardware o.a. servers, PC's, routers, netwerkapparatuur, IP telefonie, handhelds, etc, alsmede ook supplies zoals printertoners, etiketten en andere randzaken. De producten worden geproduceerd en geleverd door derden. In bepaalde gevallen worden enkel onderdelen geleverd door derden en verzorgt Reto IT de assemblage van deze onderdelen en eventuele installatie van bijbehorende software. Onze hardware & supplies producten worden vrijwel uitsluitend geleverd aan de afnemers van onze (maatwerk)softwareproducten.

4. Consultancy
Consultancy is in ons geval te beschouwen als het geheel aan diensten uitgevoerd door het personeel van Reto ter training en/of bevordering van de kennis en kunde met betrekking tot het gebruik van onze (bovenvermelde) software bij de gebruikers van deze software, alsmede het analyseren van en adviseren over bedrijfsprocessen, inrichtingen en methodieken met betrekking tot diverse facetten van de bedrijfsvoering bij onze klanten.

5. Support
Support is te beschouwen als het geheel aan diensten uitgevoerd door het personeel van Reto ter (functionele) ondersteuning van de gebruiker. Geboden ondersteuning kan bestaan uit o.a. het beantwoorden van gebruikersvragen.

6. Maatwerkontwikkeling
Bij maatwerk denkt u aan iets dat precies past, alsof het gegoten is. Dat is nu juist waar het om gaat als u specifieke wensen heeft voor uw website: of u nu kiest voor een corporate, marketingwebsite, een webshop of alleen een app; Elke opdracht binnen Reto bevat maatwerk, hier ligt onze kracht.

5. Beoogd gebruik

Producten/diensten A is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

1. Buildix (vanaf versie Caren)

Buildix is ontworpen en ingericht om een grote verscheidenheid aan gegevens te verwerken ter administratie van de bedrijfsvoering en bijbehorende processen. Denkt u hierbij aan o.a.: persoonsgegevens, artikelgegevens, bedrijfsgegevens, transactiegegevens, voorraadadministratie, etc. Er worden in Buildix zowel geïdentificeerde als (direct en indirect) identificeerbare persoonsgegevens verwerkt.

Een voorbeeld van gegevens die, afhankelijk van gebruik/wensen door maatwerk, verwerkt kunnen worden, vindt u onderstaand:

- NAW-gegevens waarbij meerdere adressen mogelijk zijn;
- titulatuur;
- geslacht;
- relatienummer;
- demografische gegevens;
- contactgegevens, o.a. telefoonnummers en e-mailadressen;
- bankrekeningen en betaalinformatie;
- transacties; bestellingen en services en bijhorende documenten;
- IP-adres;
- aantal medewerkers (fte);
- Social Media verwijzingen;
- Kamer van Koophandel;
- btw-nummer;
- logingegevens waarbij alle wachtwoorden gehasht zijn, zie artikel 11 BEVEILIGINGSBELEID;
- overheidsidentificatienummer (OIN);
- informatie over bestelde objecten;
- relaties met andere personen/bedrijven en instanties;
- gekoppelde records zoals: CPV-codes, afbeeldingen, fotoalbums en nieuwsberichten;
- documenten en persoonsgegevens of andere privacygevoelige informatie kunnen worden gekoppeld.

Buildix is als maatwerk ingericht per opdrachtgever. Bij modules met persoonsgegevens zoals de Contact Manager kunt u via de modules 'Bronnen (AVG/GDPR) en 'Doelen (AVG/GDPR)' vastleggen hoe u de persoonsgegevens van uw relatie heeft verkregen en wat het doel is.
Voor informatie over de door Buildix verwerkte gegevens verwijzen wij u graag naar de volgende webpagina: https://www.reto.nl/buildix-privacy-en-cookiebeleid

Aanvullende documenten:

- **Notice & Takedown**
  https://www.reto.nl/buildix-notice-and-takedown

- **Gebruikersvoorwaarden**
  https://www.reto.nl/buildix-gebruikersvoorwaarden

Bij dit product is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

2. **Web & overige applicaties**
   Tijdens de ontwikkeling/uitvoering van web & overige applicaties kunnen onze medewerkers in aanraking komen met gegevens die direct (als databestanden) of indirect (benaderbaar via applicaties) ter beschikking worden gesteld door derden of opdrachtgever.
   Al onze medewerkers zijn door werkgever geïnformeerd en zijn zich terdege bewust van de verantwoordelijkheid die zij dragen wanneer zij in aanraking komen met vertrouwelijke en/of privacygevoelige informatie en zullen hier te allen tijde zorgvuldig en discreet mee omgaan, zoals ook contractueel overeengekomen met werkgever.
   Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

3. **Managed (Cloud) Services**
   Tijdens de uitvoering van managed services kunnen onze medewerkers in aanraking komen met gegevens die direct (als databestanden) of indirect (benaderbaar via applicaties) ter beschikking worden gesteld door derden of opdrachtgever.
   Al onze medewerkers zijn door werkgever geïnformeerd en zijn zich terdege bewust van de verantwoordelijkheid die zij dragen wanneer zij in aanraking komen met vertrouwelijke en/of privacygevoelige informatie en zullen hier te allen tijde zorgvuldig en discreet mee omgaan, zoals ook contractueel overeengekomen met werkgever.
   Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

4. **Hardware & Supplies**
   De hardware, de hardwarecomponenten en supplies die door ons worden geleverd bevatten en verwerken op zichzelf geen gegevens. Indien er aanvullende werkzaamheden (installaties, configuraties, e.d.) worden verricht, kunnen onze medewerkers in aanraking komen met gegevens die direct (als databestanden) of indirect (benaderbaar via applicaties) ter beschikking worden gesteld door derden of opdrachtgever.
   Al onze medewerkers zijn door werkgever geïnformeerd en zijn zich terdege bewust van de verantwoordelijkheid die zij dragen wanneer zij in aanraking komen met vertrouwelijke en/of privacygevoelige informatie en zullen hier te allen tijde zorgvuldig en discreet mee omgaan, zoals ook contractueel overeengekomen met werkgever.
   Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

5. **Consultancy**
   Tijdens de uitvoering van consultancy diensten zullen onze medewerkers in aanraking komen met gegevens die direct (als databestanden) of indirect (benaderbaar via applicaties) ter beschikking worden verwerkt door derden of opdrachtgever.
   Al onze medewerkers zijn door werkgever geïnformeerd en zijn zich terdege bewust van de verantwoordelijkheid die zij dragen wanneer zij in aanraking komen met vertrouwelijke en/of privacygevoelige informatie en zullen hier te allen tijde zorgvuldig en discreet mee omgaan.
   Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. **Support**
   Tijdens de uitvoering van supportdiensten zullen onze medewerkers in aanraking komen met gegevens die direct (als databestanden) of indirect (benaderbaar via applicaties) ter beschikking worden verwerkt door derden of opdrachtgever.
   Al onze medewerkers zijn door werkgever geïnformeerd en zijn zich terdege bewust van de verantwoordelijkheid die zij dragen wanneer zij in aanraking komen met vertrouwelijke en/of privacygevoelige informatie en zullen hier te allen tijde zorgvuldig en discreet mee omgaan, zoals ook contractueel overeengekomen met werkgever.
   Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

7. **Maatwerkontwikkeling**
   Tijdens de ontwikkeling/uitvoering van maatwerkontwikkeling kunnen onze medewerkers in aanraking komen met gegevens die direct (als databestanden) of indirect (benaderbaar via applicaties) ter beschikking worden gesteld door derden of opdrachtgever.
   Al onze medewerkers zijn door werkgever geïnformeerd en zijn zich terdege bewust van de verantwoordelijkheid die zij dragen wanneer zij in aanraking komen met vertrouwelijke en/of privacygevoelige informatie en zullen hier te allen tijde zorgvuldig en discreet mee omgaan, zoals ook contractueel overeengekomen met werkgever.
   Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. Reto heeft bij het ontwerpen van het product/de dienst *privacy by design* op de volgende wijze toegepast:

- de schermen bevatten standaard alleen die gegevens die nodig zijn voor de dienstverlening van de opdrachtgever. De opdrachtgever bepaalt welke velden beschikbaar zijn of niet. Reto heeft hierin een adviseerde rol;
- opdrachtgever kan zelf bestanden uploaden in verschillende formaten (PDF, MS Word, MS Excel enz.) en kunnen gegevens in voorkomende gevallen zelf wijzigen en verwijderen;
- Reto controleert de gegevens niet en zal gegevens alleen inzien op verzoek van de opdrachtgever, bijvoorbeeld als dat nodig is om een vraag te beantwoorden;
- voor Buildix is er een aanvullende privacyverklaring: https://www.reto.nl/buildix-privacy-en-cookiebeleid

Reto gebruikt de Data Pro Standaardclausules voor verwerkingen, zie Deel 2 vanaf pagina 15.

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

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

Sub-processors - infrastructuur en dataopslag

BEDRIJF	OMSCHRIJVING	VESTEGINGSLAND
BIT B.V.	Cloud Service Provider	Nederland
TUXIS INTERNET ENGINEERING V.O.F.	Cloud Service Provider	Nederland
MICROSOFT CORPORATION	Cloud Service Provider	United States
GOOGLE, INC.	Cloud Service Provider	United States
AMAZON, INC.	Cloud Service Provider	United States

Sub-processors - dienst specifiek

BEDRIJF	OMSCHRIJVING	VESTEGINGSLAND
MOLLIE B.V.	Verwerking van betalingen	Nederland
BENK GROEP B.V.	Verwerking van VoIP	Nederland
TRENGO V.O.F.	Unified messaging	Nederland
EXACT NETHERLANDS B.V.	Verwerking van facturen	Nederland
MANDRILL	Verwerking van e-mail	United States
SPAMEXPERTS B.V.	Mail-filtering	Nederland
MESSAGEBIRD B.V.	SMS-diensten	Nederland
MAILCAMP B.V.	E-mailmarketing software	Nederland

Het is aan opdrachtgever ter eigen beoordeling of deze sub-processors en -contractors voldoen aan hun eisen. Zo NIET, adviseren wij de opdrachtgever GEEN gebruik te maken van de Reto diensten. Wij adviseren in die situatie opdrachtgever om contact met ons op te nemen voor meer informatie.

Reto ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:

- Reto heeft de beschikking over een supportdesk ingericht ter ondersteuning van alle klanten met een actieve supportovereenkomst. In het geval van vragen betreffende AVG gerelateerde functionaliteiten in het systeem kan contact opgenomen worden met de supportdesk op telefoonnummer +31 (0)35-603 23 05. Bovenstaande is ook van toepassing op specifieke vragen betreffende:
    - dataportabiliteit;
    - anonimisering;
    - pseudonimisering.
- In de beheersoftware Buildix kunnen opdrachtgevers zelf exports maken van gegevens uit het dossier in een combinatie van MS Excel (module: Export sjablonen) voor de gegevens die gestructureerd zijn vastgelegd.

9. **Na beëindiging van de overeenkomst met een opdrachtgever verwijdert Reto de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen drie maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**

10. **Na beëindiging van de overeenkomst met opdrachtgever retourneert Reto op verzoek alle persoonsgegevens die hij voor opdrachtgever verwerkt binnen drie maanden op de volgende manier:**
    - back-up van de database (vaak PostgreSQL) plus alle bestanden die buiten de database zijn opgeslagen via SFTP, versleuteld en beveiligd met een wachtwoord dat separaat wordt overgedragen.

BEVEILIGINGSBELEID

11. Reto heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn producten en diensten:

- Reto maakt voor de opslag van data gebruik van ISO27001 gecertificeerde datacentra;
- deze datacentra staan fysiek in de EER (Europese Economische Ruimte);
- beveiligingssoftware, zoals virusscanners en firewalls;
- producten worden in een continu proces van updates beschikbaar gesteld;
- updates worden ontworpen en onderhouden met de laatst beschikbare technieken;
- interne wachtwoorden zijn opgeslagen in een wachtwoordkluis met verschillende bevoegdheidsrollen en logging;
- dagelijkse back-up die beveiligd op twee fysieke locaties in Nederland wordt opgeslagen en minimaal 30 dagen wordt bewaard;
- optie om toegang tot dossiers te loggen;
- optie om toegang te beperken via IP-restricties;
- optie om de databases te hosten in eigen datawarehouse van opdrachtgever;
- anonimiseren van dossiers na een door de opdrachtgever vastgelegde periode;
- verwijderen van dossiers na een door de opdrachtgever vastgelegde periode;
- iedere medewerker zal alleen gebruik kunnen maken van datacommunicatie lijnen en toegang tot klantsystemen met gebruik van een persoonsgebonden gebruikersnaam en wachtwoord;
- geheimhoudingsplicht voor alle medewerkers vastgelegd in een arbeidsovereenkomst;
- geen toegang tot source voor derden, enkel en alleen via API;
- 4-ogen principe voor kritische bedrijfsonderdelen;
- gedetailleerde logging & monitoring (intern en extern);
- two-factor authentication voor gevoelige onderdelen;
- DKIM, SPF en DMARC zijn drie internetstandaarden die wij gebruiken om te voorkomen dat u uit onze naam e-mails ontvangt die virussen bevatten, spam zijn of bedoelt zijn om persoonlijke (inlog)gegevens te bemachtigen;
- DNSSEC is een extra beveiliging (aanvullend op DNS) voor het omzetten van onze domeinnamen (bijvoorbeeld onze corporate naam reto.nl) naar de hieraan gekoppelde IP-adressen (servernamen); deze worden voorzien van een digitale handtekening. U kunt die handtekening automatisch laten controleren. Op die manier voorkomen wij dat u omgeleid wordt naar een vals IP-adres;
- medewerkerstoegang tot data op basis van need-to-know-principe;
- Reto zal ‘friendly hackers’ aanmoedigen om eventuele kwetsbaarheden in haar producten en diensten te melden;

- **Buildix (vanaf versie Caren)**
    - privacy gevoelige gegevens die met Buildix verstuurd worden, slaan wij versleuteld op. We coderen gegevens met behulp van bewezen technologie. Buildix zorgt ervoor dat alleen de verzender en de ontvanger bij deze data kunnen komen (geen Man-in-the-middle);
    - inloggen kan met behulp van two-factor authenticatie (gebruikersnaam, wachtwoord en bijvoorbeeld een SMS-code);
        - two-factor authenticatie (TFA) is een extra stap tijdens het inlogproces. Door het gebruik van TFA is de communicatie beter beveiligd tegen kwaadwillende, zoals hackers. Als TFA is ingeschakeld via het gebruikersaccount dan heeft de hacker ook een mobiele telefoon nodig en dat is vanaf zijn bureaustoel wat lastiger te verkrijgen. Bij versturen van persoonsgegevens is gebruik van TFA bijzonder aanbevolen;
    - Buildix communiceert met zowel zender als ontvanger via een TLS-verbinding (ook wel bekend als SSL);
        - een TLS-verbinding is een gecodeerde verbinding tussen de server (Buildix) en bezoeker (verzender en ontvanger). Een TLS-verbinding kan eenvoudig worden herkend aan de URL (http**s**://domain.com). Een goede browser geeft aan dat de lijn beveiligd is door middel van een klein slotje achter de URL of een groene balk (zie de adresbalk van Buildix);
        - TLS is min of meer verplicht gesteld in de Algemene verordening gegevensbescherming (Avg). Men moet immers de informatie via een beveiligde verbinding versturen en TLS is de enige die breed wordt gebruikt;
        - certificaten worden door verschillende bedrijven uitgegeven;
    - per Buildix-gebruiker instelbare toegangsrechten tot vormen van dienstverlening en (delen van) dossiers;
    - Buildix-gebruikers adviseren en stimuleren wij hun wachtwoord regelmatig te wijzigen, tenminste eenmaal per zes maanden;
    - Buildix slaat wachtwoorden nooit plain-tekst op en heeft geen toegang tot de decryptiesleutels van ‘data at rest’. Wachtwoorden worden gehashed met het bcrypt algoritme voor controle bij inloggen;
- strikte scheiding van gegevens per opdrachtgever;
- de datacommunicatielijnen gebruikt voor services (consultancy en support) zijn beveiligd.

12. Reto heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):

- ISO 27001
  (we hebben geen certificering maar werken zoveel mogelijk volgens de normen).

13. Reto heeft de volgende certificeringen

- momenteel hebben wij geen certificaten. We zijn voornemens om ons te certificeren met het Data pro certificaat indien deze beschikbaar is;
- periodiek laten we onze servers en applicaties middels een Security assessment testen en rapporteren.

DATALEKPROTOCOL

1. **In geval er toch iets mis gaat, hanteert Reto het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**

- Er is een procedure voor het intern melden van incidenten.
  Zie bijgevoegd document 'Reto – Datalekprotocol binnen Reto.pdf'. Tevens is op onze website altijd de meeste recente versie te vinden.
  https://www.reto.nl/datalekprotocol

  Indien Reto in haar organisatie een datalek ontdekt, zal Reto haar opdrachtgever daarvan zo snel mogelijk op de hoogte stellen, door contact op te nemen met de daarvoor door de opdrachtgever aangewezen functionaris. Reto levert zo veel mogelijk relevante gegevens aan, waaronder omschrijving van het incident, aard van de inbreuk, aard persoonsgegevens c.q. categorieën van betrokken data subjects, schatting van aantal betrokken data subjects en mogelijk betrokken databases, indicatie wanneer incident heeft plaatsgevonden en wat er gebeurd is.

- Meldingen worden indien mogelijk binnen vier uur gedaan aan opdrachtgevers. Reto zal zelf geen meldingen doen aan AP of Data subjects. Wel of niet melden blijft de verantwoordelijkheid van de door de opdrachtgever aangewezen functionaris zoals opgegeven in de 'Specificatie persoonsgegevens en betrokkenen' (Reto - Specificatie persoonsgegevens en betrokkenen.pdf).
  https://www.reto.nl/verwerkersovereenkomst

  De Reto zal de opdrachtgever of de controller desgewenst ondersteunen bij het meldproces.

Deel 2: Standaardclausules voor verwerkingen

Versie: januari 2018
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, subverwerkers, 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, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van 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.

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

7.4 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.

7.5 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport.

7.6 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. SUBVERWERKERS

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

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere subverwerkers 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.