STANDAARD VERWERKERSOVEREENKOMST

Data Pro Statement
Versie juli 2024

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen volgens hoofdstuk 2 van de NL Digital voorwaarden 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:
   ICT Teamwork B.V.
   Boris Pasternaklaan 20
   2719 DA ZOETERMEER

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   Directie: Raymond Kroes
   [raymond@ictteamwork.nl]
   of
   Security Officer: Kwinten de Kleijn
   [kwinten@ictteamwork.nl]
   Algemeen telefoonnummer 079-3633100

2. Dit Data Pro Statement geldt vanaf versiedatum zoals aangegeven op het eerste vel. De in dit Data Pro Statement omschreven beveiligings-maatregelen 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.
   - Connectivity
   - VOIP
   - Teamcloud
   - VDS Hosting
   - Full Service
   - Mobile Device management
   - Projecten (consultancy en werkzaamheden)

4. Onderstaand een korte functionele omschrijving op hoofdlijnen van genoemde producten. Nadere detaillering in de SLA.

Connectivity
Verbindingstechnologie zoals internetlijnen via diverse carriers (Glas, Kabel, Koper, Radio) en VPN connecties daaroverheen.

VOIP (*)
Telefoniediensten naar vast en mobiel vanaf vast en mobiel inclusief gehoste telefooncentrale en telefonie diensten daarbinnen.

Teamcloud (*)
Standaard werkplekken op afstand, aangeboden als dienst en bereikbaar op diverse devices zoals Windows PC of notebook, Apple PC of notebook, Tablet, etc.

VDS Hosting (*)
Maatwerk (netwerk-)infrastructuren waarbinnen onder andere werkplekken op afstand of generieke hostingdienstenkunnen worden aangeboden. De aangeboden diensten zijn bereikbaar op diverse devices en protocollen afhankelijk van de gewenste inrichting.

Full Service
Beheer en (gebruikers-)ondersteuning voor clients, servers en overige devices

Mobile Device Management
Beheer en (gebruikers-)ondersteuning voor mobile devices zoals tablets en smartphones

Projecten (consultancy en werkzaamheden)
Levering van consultancy en (installatie-) werkzaamheden binnen de ICT dienstverlening

Beoogd gebruik

5. Alle bovenstaande diensten zijn bedoeld voor algemeen zakelijk gebruik. Deze zijn generiek (bijvoorbeeld een bureaublad of een goed beheerd systeemplatform) en dus niet specifiek ingericht op het verwerken van persoonsgegevens. Diensten aangegeven met een (*) zijn echter geschikt voor de daarbinnen redelijkerwijs te verwachten verwerking van persoonsgegevens.
   Alle bovenstaande diensten zijn niet specifiek ingericht voor de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. Privacy by design is door de fabrikanten van bij artikel 3 en 4 gebruikte producten toegepast volgens de bij haar geldende principes die volgens artikel 1.4 van de NL Digital voorwaarden aan klant worden doorgegeven. ICT Teamwork heeft deze principes toegapast volgens de normen van het door haar gevoerde ISO27001 ISMS.

7. ICT Teamwork gebruikt niet de Data Pro Standaardclausules voor verwerkingen maar de Standaardclausules voor verwerkingen zoals opgenomen in hoofdstuk 2 van de NL Digital voorwaarden welke als bijlage bij de overeenkomst te vinden zijn

8. ICT Teamwork verwerkt de persoonsgegevens van haar opdrachtgevers binnen de EU/EER.

9. ICT Teamwork maakt gebruik van de volgende subverwerkers:
   - Atom86
   - Datafiber
   - ICT Teamwork Continuity Services
   - Microsoft
   - NorthC Datacenters Delft
   - NorthC Datacenters Amsterdam
   - N-able
   - Routit

   Deze zijn binnen de ISO27001 certificering van ICT Teamwork geborgd met aanvullende verwerkersovereenkomsten waarbinnen onder andere is aangegeven dat gegevens alleen binnen de EU/EER worden verwerkt. Deze zijn op eerste verzoek verkrijgbaar.

10. De wijze waarop ICT Teamwork opdrachtgevers ondersteunt bij verzoeken van betrokkenen (Data subjects) is vastgelegd in ons Privacy Statement / Privacy Verklaring (zie https://ictteamwork.nl/privacy-statement)

11. Artikel 11 van het standaard Data Pro Statement aangaande Data Privacy Impact Assessments zoals opgesteld door de brancheverenigingen NL Digital is niet van toepassing.

12. Na beëindiging van de overeenkomst met een opdrachtgever verwijdert ICT Teamwork de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible). Opdrachtgever vrijwaart verwerker van alle directe en indirecte gevolgen hiervan.

13. Indien gewenst kan opdrachtgever na beëindiging van de overeenkomst de persoonsgegevens die bij ICT Teamwork aanwezig naar haar eigen systemen verplaatsen binnen een periode van 3 maanden. Hierna zullen deze alsnog niet langer toegankelijk zijn (render inaccessible).

Beveiligingsbeleid

14. ICT Teamwork heeft zich geconformeerd aan het ISO27001 Information Security Management System dat gericht is op borging van vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van haar dienstverlening. Binnen dit ISMS is beleid vastgesteld, uitgewerkt en periodiek getoetst qua opzet, bestaan en werking voor diverse beveiligingsmaatregelen waaronder:
   - Informatiebeveiligingsbeleid
   - Logische en fysieke toegangsbeveiliging, incl. priviliged rights management
   - Wachtwoorden en access tokens
   - Encryptie, specifiek van customer data
   - Sleutelbeheer, informatietransport (VPN, TLS)
   - Gedocumenteerde en periodiek geteste Back-up-, restore- en uitwijkprocedures
   - Beveiliging van Systemen, IPS, IDS, EDR, Segmentering, Firewalling
   - Personeelsscreening, NDA's en VOG's
   - Risicobeoordeling en -behandeling van informatiebeveiliging
   - Monitoring, Pentesting en Vulnerability testing
   - Gedocumenteerde procedures voor systeembeheer
   - Projectbeheer, Change management
   - Incident management en security incidenten
   - Datalekkenprocotcol

   ICT Teamwork heeft geen inzicht in klantdata (al dan niet met persoonsgegevens) en zal gegevens alleen inzien op uitdrukkelijk verzoek.

15. ICT Teamwork heeft zich geconformeerd aan NEN-ISO27001 en aan de eisen die de Nederlandse Staat stelt aan het verwerken van vertrouwelijke informatie.

16. ICT Teamwork is gecertificeerd volgens de volgende normen
   - NL Digital DataProCode certificering (809-199-2020)
   - ISO 27001 (ISO/IEC27001 BSI-ISC-221)

Datalekprotocol

17. In geval er toch iets mis gaat, hanteert ICT Teamwork een datalekkenprotocol dat is opgenomen binnen haar ISO27001 omgeving. Hieronder een korte functionele omschrijving.

Wat is een datalek?

Een datalek is iedere inbreuk op de beveiliging waarbij persoonsgegevens verloren zijn gegaan, of ongeoorloofd zijn gewijzigd, verstrekt of ingezien.

Wat doen we bij een inbreuk?

Een inbreuk wordt gezien als een security incident. Alle gegevens aangaande dit incident worden vastgelegd in onze systemen en met hoge prioriteit behandeld. Er worden acties ondernomen om de aard en omvang van het incident vast te stellen en zo mogelijk worden de eerste maatregelen genomen om het incident en/of de gevolgen daarvan in te dammen.

Wat noteren we van een inbreuk?

- een korte omschrijving van de inbreuk;
- wanneer het plaatsvond;

- Welke eerste maatregelen zijn of worden genomen om de gevolgen te beperken
- wat er met de gegevens is gebeurd (verloren, ingezien, gekopieerd, gewijzigd etc);
- wat voor soort gegevens er gelekt zijn, en om hoeveel personen het gaat;
- inschatting van de (mogelijke) gevolgen van de inbreuk

Aan wie melden wij een inbreuk?

Als de inbreuk het domein van een klant raakt, zal de contactpersoon of het management door ons persoonlijk hierover zo spoedig mogelijk geïnformeerd worden. Het is daarna aan de klant, als eindverantwoordelijke voor de persoonsgegevens om te bepalen hoe ernstig zij de inbreuk acht en of zij de melding moet doorzetten aan de Autoriteit Persoonsgegevens en/of de Betrokkene. Wij zullen ons vooral op de technische kant van de inbreuk concentreren en op het herstellen en voorkomen ervan.