



NLdigital

Versie: oktober 2026

Verwerkers- overeenkomst Teqa Informatica B.V.

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

NLdigital versie maart 2025

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 de volgende data processor (verwerker):

Teqa Informatica B.V.
Reykjavikstraat 1
3543 KH
Utrecht
Nederland
Hierna te noemen 'data processor'.

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

J.W. Snijders
Postbus 4
3540 AA
Vleuten
privacy@teqa.eu
+31 030 237 3030

2. Dit Data Pro Statement geldt vanaf 01-oktober-2026

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

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor i-Reserve

4. Omschrijving product(en)/dienst(en)

Teqa opereert in de informatietechnologiesector en is de leverancier van een aanpasbare applicatie voor reserveringsbeheer, i-Reserve genaamd. Teqa levert i-Reserve volgens een Software as a Service (SaaS) model. De i-Reserve-dienst vergemakkelijkt de boeking / organisatie van objecten of activiteiten in een breed scala van sectoren. Momenteel zijn de belangrijkste klanten van Teqa bedrijven die boekbare opties aanbieden op het gebied van sport en fitness, rondleidingen, trainingen, cursussen, vergaderruimtes en entertainmentactiviteiten. Teqa ontwikkelt, levert en implementeert i-Reserve zelf. De infrastructuur waarop i-Reserve draait, wordt beheerd door Teqa of door een door Teqa geselecteerde hostingpartij (zie bepaling 9). Teqa adviseert en ondersteunt haar klanten ook bij het gebruik van de geleverde software.

5. Beoogd gebruik

Product/dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

i-Reserve software biedt een verscheidenheid aan standaard en aangepaste velden die kunnen worden gebruikt om informatie te verzamelen, zoals NAW gegevens, e-mailadressen, telefoonnummers, interesses, opleidingsniveau, voorkeuren, afspraken, facturatiegegevens, inhoud e-mailverkeer en andere communicatie met de klant. Teqa heeft niet de controle over welke informatie u wilt verzamelen.

Sla geen bijzondere persoonsgegevens op. Teqa raadt je ten zeerste af om bijzondere persoonsgegevens in onze software vast te leggen. Denk aan: gegevens over gezondheid, gegevens waaruit de etnische en/of religieuze afkomst afleidbaar is, BSN-nummers, genetische gegevens etc. Technisch kunnen wij niet afdwingen dat je geen bijzondere persoonsgegevens opslaat of verstuurt, aangezien je daar zelf de controle over hebt. Maar we raden het opslaan van dit type persoonsgegevens ten strengste af.

Bij dit product/deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. Indien u toch bijzondere persoonsgegevens verwerkt, dan kunt u het beste uw privacy officer contact met ons op laten nemen om eventuele aanvullende mogelijkheden te bespreken. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is altijd ter eigen beoordeling door opdrachtgever.

6. Privacy by design/privacy by default

Bij de ontwikkeling en het onderhoud van i-Reserve past data processor de beginselen van privacy by design en privacy by default toe.

Dit betekent onder meer dat:

- standaard alleen de velden verplicht zijn die nodig zijn om een reservering te maken;
- aanvullende velden, waaronder vrij in te richten velden, optioneel zijn en door opdrachtgever zelf worden ingericht en ingeschakeld;
- toegangsrechten binnen i-Reserve rolgebaseerd kunnen worden ingericht, zodat uitsluitend geautoriseerde gebruikers toegang hebben tot persoonsgegevens;
- gegevensoverdracht plaatsvindt via beveiligde verbindingen (HTTPS/SSL);
- functionaliteiten beschikbaar zijn voor het verwijderen van persoonsgegevens en voor het automatisch anonimiseren daarvan. Opdrachtgever stelt zelf in welke gegevens worden geanonimiseerd. Of gegevens daarna niet meer tot een persoon te herleiden zijn, hangt af van die instelling: blijven bijvoorbeeld geboortedatum en postcode bewaard, dan kan een persoon mogelijk nog worden herleid;
- logging- en monitoringmechanismen worden toegepast ter detectie van ongeautoriseerde toegang;
- nieuwe functionaliteiten vooraf worden beoordeeld op privacy- en beveiligingsrisico's.

Opdrachtgever is onder andere verantwoordelijk voor:

- het beperken van de invoer van persoonsgegevens tot hetgeen noodzakelijk is;
- het correct configureren van autorisaties en bewaartermijnen;
- het inrichten van aanvullende velden en van de instellingen voor automatisch anonimiseren.

Data processor faciliteert privacyvriendelijke instellingen, maar heeft geen zeggenschap over de concrete inrichting en het gebruik van het systeem door Opdrachtgever.

7. Data processor gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn.

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

9. Data processor maakt gebruik van de volgende sub-processors:

De meest actuele stand is terug te vinden op <https://teqa.nl/data-pro-statement>

- Leaseweb Netherlands B.V. – hosting van databases, webserver en bestandsopslag
Locatie verwerking: Nederland (EU)
Certificeringen: ISO 9001, ISO 27001
- Mailgun (Sinch) – verzending van e-mail vanuit i-Reserve (o.a. bevestigingen en notificaties), via de EU-regio van Mailgun
Locatie verwerking: EU
- Acronis – opslag van back-ups
Locatie verwerking: datacenter Frankfurt, Duitsland (EU)

i-Reserve kan worden gekoppeld met producten van externe partijen, zoals Exact, King, Accountview, Cardgate, Mollie, Buckaroo, Google kalenders en anderen. Indien i-Reserve wordt gekoppeld met producten van dergelijke externe partijen, is Opdrachtgever zelf verantwoordelijk voor het maken van afspraken met deze externe partijen omtrent de verwerkingen van persoonsgegevens.

10. Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:

In i-Reserve is het mogelijk dat uw klant zelf zijn/haar gegevens kan inzien, corrigeren, verwijderen of downloaden. De beheerder kan ook zelf klantgegevens exporteren of via een API gegevens doorsturen. In het geval dat een betrokkene een verzoek tot uitoefening van zijn/haar wettelijke rechten richt aan data processor, zal data processor het verzoek doorsturen aan opdrachtgever, en dient opdrachtgever het verzoek verder af te handelen. Data processor mag de betrokkene daarvan op de hoogte stellen.

11. Data processor ondersteunt opdrachtgever op de volgende manier bij Data Protection Impact Assessments (DPIA's):

Indien opdrachtgever daartoe verplicht is, zal data processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een Data Protection Impact Assessment (DPIA) of een daarop volgende voorafgaande raadpleging, zoals bedoeld in artikel 35 en 36 AVG.

Een verzoek hiertoe kan worden gericht aan privacy@teqa.eu. Data processor stelt daarbij de informatie ter beschikking die in redelijkheid van hem verwacht mag worden, zoals een beschrijving van de verwerkingen binnen i-Reserve, de getroffen technische en organisatorische beveiligingsmaatregelen (bepaling 14), de ingeschakelde sub-processors (bepaling 9) en de locatie van de verwerking (bepaling 8).

Data processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij opdrachtgever, conform artikel 7.7 van de Standaardclausules voor verwerkingen.

12. **Na beëindiging van de Overeenkomst met een opdrachtgever verwijdt data processor de persoonsgegevens die hij voor opdrachtgever verwerkt binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**
Dit geldt ook voor back-ups: back-ups worden eveneens binnen 3 maanden na beëindiging van de Overeenkomst verwijderd.
13. **Retourneren van persoonsgegevens na beëindiging van de Overeenkomst**
Na beëindiging van de overeenkomst met opdrachtgever kan data processor op verzoek alle persoonsgegevens die hij voor opdrachtgever verwerkt binnen 3 maanden aanleveren op een door opdrachtgever aangeleverde datadrager.

Beveiligingsbeleid

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

Alle gegevens worden verwerkt binnen de EU/EER

- Programmacode in eigen beheer
- Mogelijkheid tot twee-staps-verificatie voor toegang tot i-Reserve
- Minimumeisen aan samenstelling wachtwoorden
- Veilige HTTPS verbinding met SSL certificaat
- Versleuteling van informatie
- Web Application Firewall (WAF)
- IP adres whitelisting voor beheerfuncties
- Slowdown en lockdown mechaniek
- Scans en backups
- Mogelijkheid om persoonsgegevens automatisch te anonimiseren, door opdrachtgever in te stellen (zie bepaling 6)
- Hostingpartners voldoen aan ISO 9001, ISO 27001
- Medewerkers van data processor zijn gehouden aan een geheimhoudingsplicht
- Medewerkers van data processor worden getraind op informatiebeveiligingsbewustzijn

Een samenvatting en meest actuele stand van de beveiligingsmaatregelen vindt u op:

<https://support.i-reserve.net/nl/algemene-informatie/wat-doet-i-reserve-aan-beveiliging-en-privacy-van-persoons-gegevens/>

15. **Data processor heeft zich geconformeerd aan een Information Security Management System (ISMS):**

- ISO 27001
- ISMS NLdigital

16. **Data processor heeft de volgende verificaties en certificeringen:**

- Data Pro Verified

Datalekkenprotocol

17. In geval er toch iets mis gaat, hanteert data processor het volgende datalekkenprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:

- In het geval van een inbreuk in verband met persoonsgegevens zal data processor u daarover zonder onredelijke vertraging informeren. Data processor spant zich naar beste kunnen in om ervoor te zorgen dat de verstrekte informatie volledig, correct en accuraat is.
- Opdrachtgever beoordeelt zelf of hij de toezichthoudende autoriteiten en/of betrokkenen zal informeren of niet.
- De melding van data processor behelst in ieder geval het melden van het feit dat er een lek is geweest, alsmede, voor zover de informatie voorhanden is:
 - wat de (vermeende) oorzaak is van het lek;
 - contactgegevens voor de opvolging van de melding;
 - bij benadering: het aantal betrokkenen en registers van persoonsgegevens;
 - wat is het (vooralsnog bekende en/of te verwachten) gevolg;
 - wat is de (voorgestelde) oplossing;
 - wat de reeds ondernomen maatregelen zijn.

Data processor gebruikt de volgende monitoring tools/werkwijze om potentiële beveiligingsincidenten te signaleren: De monitoring wordt gedaan door Leaseweb, het hostingbedrijf van onze servers. Leaseweb is ISO27001 gecertificeerd, hierin wordt de informatiebeveiliging / monitoring onderbouwd.