Version: October 2026

Data Processing Agreement Teqa Informatica B.V.

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard clauses for data processing

NLdigital version march 2025

This Data Processing Agreement and the standard clauses were originally drafted in Dutch. The English version is for convenience only. In case of conflict between the Dutch and the English version, the Dutch version prevails.

Part 1: Data Pro Statement

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

General information

1. **This Data Pro Statement was drawn up by the following data processor (verwerker):**
   Teqa Informatica B.V.
   Reykjavikstraat 1
   3543 KH
   Utrecht
   The Netherlands

   If you have any queries about this Data Pro Statement or data protection in general, please contact:

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

2. **This Data Pro Statement shall enter into force on** *1 October 2026*
   We regularly revise the security measures described in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. If this document is updated, we shall notify you of the revised versions through our regular channels
3. **This Data Pro Statement applies to the following products and services provided by data processor**
   i-Reserve
4. **Description of product(s)/service(s)**
   Teqa operates in the information technology sector and is the supplier of a customizable application for reservation management, called i-Reserve. Teqa supplies i-Reserve according to a Software as a Service (SaaS) model. The i-Reserve service facilitates the booking / organization of objects or activities in a wide range of sectors. Currently, Teqa's main customers are companies that offer bookable options in the areas of sports and fitness, guided tours, training, courses, meeting rooms and entertainment activities. Teqa develops, supplies and implements i-Reserve itself. The infrastructure on which i-Reserve runs is managed by Teqa or by a hosting party selected by Teqa (see provision 9). Teqa also advises and supports its customers in the use of the supplied software.
5. **Intended use**
   Product/service is designed and built to process the following types of data:
   i-Reserve software offers a variety of standard and custom fields that can be used to gather information, such as name and address data, e-mail addresses, telephone numbers, interests, education level,

preferences, appointments, invoicing data, content of e-mail traffic and other communications with the customer. Teqa does not control what information you want to collect.

Do not store special categories of personal data. Teqa strongly discourages you from recording special categories of personal data in our software. Consider: data concerning health, data revealing ethnic and/or religious origin, citizen service numbers (BSN), genetic data, etc. Technically we cannot prevent you from storing or sending special categories of personal data, since you yourself have control over this. But we strongly discourage the storage of this type of personal data.

- The processing of special categories of personal data or data regarding criminal convictions and offences or personal numbers issued by the government was not taken into account for this product/service. If you nevertheless process special categories of personal data, it is best to have your privacy officer contact us to discuss any additional options. The processing of such data with the product or service described above is always at the client's own discretion.

6. Privacy by design/privacy by default

In the development and maintenance of i-Reserve, data processor applies the principles of privacy by design and privacy by default.

This means, among other things, that:

- by default, only the fields required to make a reservation are mandatory;
- additional fields, including free-format fields, are optional and are set up and enabled by the client;
- access rights within i-Reserve can be configured on a role-based basis, ensuring that only authorized users have access to personal data;
- data transmission takes place via secure connections (HTTPS/SSL);
- functionalities are available for deleting personal data and for anonymising it automatically. The client determines which data are anonymised. Whether data can no longer be traced back to an individual afterwards depends on that setting: if, for example, date of birth and postcode are retained, a person may still be identifiable;
- logging and monitoring mechanisms are applied to detect unauthorized access;
- new functionalities are assessed in advance for privacy and security risks.

The Client is, among other things, responsible for:

- limiting the entry of personal data to what is necessary;
- correctly configuring access rights and retention periods;
- configuring additional fields and the settings for automatic anonymisation.

Data processor facilitates privacy-friendly settings but has no control over the specific configuration and use of the system by the Client.

7. Data processor uses the Data Processing Standard Clauses for data processing, which are attached to the Agreement as an addendum.

8. **Data processor shall process the personal data provided by their clients within the EU/EEA.**

9. **Data processor uses the following sub-processors:**
The most up-to-date overview can be found at https://teqa.nl/data-pro-statement

Leaseweb Netherlands B.V. – hosting of databases, web servers and file storage
Location of processing: the Netherlands (EU)
Certifications: ISO 9001, ISO 27001

Mailgun (Sinch) – sending of e-mail from i-Reserve (e.g. confirmations and notifications), via Mailgun's EU region
Location of processing: EU

Acronis – storage of backups
Location of processing: data center Frankfurt, Germany (EU)

i-Reserve can be linked with products from external parties such as Exact, King, Accountview, Cardgate, Mollie, Buckaroo, Google calendars and others. If i-Reserve is linked to products from such external parties, the Client is responsible for making agreements with these external parties regarding the processing of personal data.

10. **Data processor shall support their clients in the following way when they receive requests from data subjects:**
In i-Reserve it is possible for your customer to view, correct, delete or download his / her data. The administrator can also export customer data or send data via an API. In the event that a data subject submits a request to exercise his / her legal rights to data processor, data processor will forward the request to the client, and the client must handle the request further. Data processor may inform the data subject of this.

11. **Data processor shall support their clients in the following way with Data Protection Impact Assessments (DPIAs):**
If the client is obliged to do so, data processor shall, following a reasonable request to that effect, cooperate with a Data Protection Impact Assessment (DPIA) or any subsequent prior consultation as referred to in Articles 35 and 36 GDPR.

Such a request can be sent to privacy@teqa.eu. Data processor shall make available the information that may reasonably be expected of them, such as a description of the processing operations within i-Reserve, the technical and organisational security measures taken (provision 14), the sub-processors engaged (provision 9) and the location of the processing (provision 8).

Data processor may charge the client the reasonable costs incurred in this regard, in accordance with Article 7.7 of the Standard Clauses for Data Processing.

12. **Once the Agreement with a client has been terminated, data processor shall delete personal data they process on behalf of client within *three months*, in such a manner that the data can no longer be used and shall be rendered inaccessible.**
This also applies to backups: backups shall likewise be deleted within 3 months after termination of the Agreement.

13. **Returning of personal data once the Agreement has been terminated**
Within 3 months after termination of the Agreement with the client, data processor can, on request, deliver all personal data processed on behalf of the client to a data carrier supplied by the client.

Security policy

14. **Data processor has implemented the following security measures to protect their product or service:**

- All data is processed within the EU / EEA
- Program code is owned and managed by processor
- Possibility of two-step verification for access to i-Reserve
- Minimum requirements for composition of passwords
- Secure HTTPS connection with SSL certificate
- Encryption of information
- Web Application Firewall (WAF)
- IP address whitelisting for management functions
- Slowdown and lockdown mechanics
- Scans and backups
- Ability to anonymise personal data automatically, configurable by the client (see provision 6)
- Hosting partner complies with ISO 9001, ISO 27001
- Data processor employees are bound by a duty of confidentiality
- Data processor employees are trained on information security awareness
- Office of the data processor has an alarm system

A summary of the security measures may be found here:

https://support.i-reserve.net/en/general-information/what-does-i-reserve-do-for-security-and-privacy-of-personal-data/

15. **Data processor conforms to the principles of the following Information Security Management System (ISMS):**

- ISO 27001
- ISMS NLdigital

16. **Data processor has obtained the following labels and certificates**

- Data Pro Verified

Data breach protocol

17. **In the event something does go wrong, data processor shall follow the following data breach protocol to ensure that clients are notified of incidents:**

- In the case of a data-related infringement, the data processor will inform the client without undue delay. Data processor shall strive to do its best to ensure that the information provided is complete, correct and accurate.
- The client assesses whether he will inform the supervisory authorities and / or data subjects or not.
- The notification by data processor in any case includes reporting the fact that there has been a leak and, in so far as the information is available:
    - what the (alleged) cause of the leak is;
    - contact details for the follow-up of the report;
    - approximately: the number of data subjects and categories of personal data;
    - what the (known and / or expected) consequence is;
    - what the (proposed) solution is;
    - what measures have already been taken.

Data processor uses the following monitoring tools / methods to identify potential security incidents: The monitoring is done by Leaseweb, the company that hosts our servers. Leaseweb is ISO27001 certified, within which information security and monitoring is underpinned.

Part 2: Standard Clauses for Data Processing

Version: March 2025

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in their capacity as an ICT supplier, processes Personal Data on behalf of their Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: statement issued by Data Processor in which they provide information such as the intended use of their products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor as required under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing their products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.

2.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of

significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating their reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written agreed upon instructions provided by Client by Data Processor.

2.4 Client or their customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.

2.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data, and shall not make any decisions on the use of the Personal Data and other such matters.

2.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 Client shall guarantee Data Processor that they act in accordance with the GDPR, that they provide a high level of protection for their systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1 Data Processor shall implement the technical and organisational security measures set out in their Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of their products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 Data Processor seeks to ensure that the security measures they shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.5 Data Processor shall be entitled to adjust the security measures they have implemented if to their discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments they chooses to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honour such requests to adjust their security measures. If Data Processor makes any adjustments to their security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing. .

Article 4. Data breaches

4.1 Data Processor does not guarantee that their security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, they shall notify Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.2 It is up to the Controller (the Client or their customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or their customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet their breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.4 If Data Processor incurs any reasonable costs in doing so, they are entitled invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are

confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that their employees comply with the requirements described in this article.

Article 6. Term and termination

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data they currently store and which they have obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, they shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of their statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

7.1 Where possible, Data Processor shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, they shall refer the Data Subject to Client where possible.

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.3 Data Processor will lend their cooperation to Client's requests for the deletion of personal data insofar as Client cannot carry this out themself.

7.4 Data Processor shall be able to demonstrate their compliance with their requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.5 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at their own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with their obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to their discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures they have implemented.

7.6 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to their discretion such are appropriate, taking into account the processing risks associated with their product or service, the state of the art, the costs of implementation, the market in which they operate, and the intended use of the product or service.

7.7 Data Processor shall be entitled to invoice Client for any costs they incur in implementing the measures referred to in this article.

Article 8. Sub-processors

8.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (sub-processors) to help them process the Personal Data, and if so, which third parties.

8.2 Client hereby authorises Data Processor to hire other sub-processors to meet their obligations under the Agreement.

8.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes . Data Processor shall ensure that any third parties they hire shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.