DATA PROCESSING AGREEMENT

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard Clauses for Data Processing

Version: November 2018

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**

   Teqa Informatica B.V.
   Savannahweg 60
   3542 AW Utrecht
   Nederland
   Hereafter refered to as ‘data processor’.

   If you have any queries about this Data Pro Statement or data protection in general, please contact:
   Wiljan Snijders
   Pal Maleterstraat 19
   3573 PE
   Utrecht
   Privacy@teqa.eu
   +31 030 237 3030

2. **This Data Pro Statement will enter into force on May 25th 2018**
   We regularly revise the security measures outlined 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 will notify you of the revised versions through our regular channels.

3. **This Data Pro Statement applies to the following products and services provided by the data processor**

   i-Reserve

4. **Description of product/service**

   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 product 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. The company develops, supplies and implements i-Reserve via architecture that is maintained by Teqa or maintained by a company that has been selected by Teqa. Teqa also advises and supports its customers in the use of the supplied software.

5. **Intended use**
   Product/service was 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 save sensitive personal information. Teqa strongly discourages you from recording sensitive personal data in our software. Apart from the fact that you must have explicit permission from data subjects to process their data, sensitive data poses a greater risk of adverse consequences for those involved. The GDPR refers to this type of data as ‘special category data’. Consider: medical data, meal preferences from which the ethnic and / or religious origin (in its formulation) is derivable, allergies, citizen service numbers, criminal conviction data, identity information etc. Technically we cannot force you to not store or send sensitive personal data, since you yourself have control over this. But we strongly discourage the storage of this type of personal data.

   If you still intend to process sensitive personal data, then it is best to have a PIA carried out and your privacy officer contact us to discuss additional options.

6. **The data processor adheres to the Data Processing Standard Clauses for Data Processing, which can be found below.**

7. **The data processor will process the personal data provided by its clients within the EU/EEA.**

8. **The data processor uses the following sub-processors:**
   - Mihosnet (hosting of our databases, web servers and file storage): ISO 9001, ISO 27001 certified.

   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.

9. **The data processor will support its 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 persue his / her legal rights to the Processor, the Processor will forward the request to the Controller, and the Controller will further process the request. The processor may inform the data subject of this.

10. **Once an agreement with a client has been terminated, the data processor will within three months delete the personal data it processes on behalf of the client, in such a manner that they will no longer be able to be used and will be rendered inaccessible.**

11. **Within 3 months after termination of the contract with the client, the data processor can, on request, deliver all personal data processed for the client to a data carrier supplied by the client.**

SECURITY POLICY

12. **The data processor has implemented the following security measures to protect its 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 automatically anonymize personal data
    - Hosting partner complies with ISO 9001, ISO 27001
    - Data processor is affiliated with the Netherlands ICT, which also advises on GDPR
    - 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/

13. **The data processor conforms to the principles of the following Information Security Management System (ISMS):**
    - ISO 27001

DATA LEAK PROTOCOL

14. **In the unfortunate event that something does go wrong, the data processor will 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 within 48 hours. Data processor shall strive to do its best to ensure that the information provided is complete, correct and accurate.
- The client (controller) assesses whether he will inform the supervisory authorities and / or data subjects or not.
- The duty to report 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.

- If laws and / or regulations require this, the data processor will cooperate in informing the relevant authorities and / or parties involved.

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

PART 2: STANDARD CLAUSES FOR DATA PROCESSING

Version: January 2018

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 regulatory agency outlined in Section 4.21 of the GDPR.

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

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

1.4 **Data Pro Statement**: a statement issued by the Data Processor in which it provides information on the intended use of its product or service, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects, among other things.

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

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

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

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

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, along with the 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 the Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of the Client's data processing agreements is expressly rejected.

2.2 The Data Pro Statement, and particularly the security measures outlined in it, may be adapted from time to time to changing circumstances by the Data Processor. The Data Processor will notify the Client in the event of significant revisions. If the Client cannot reasonably agree to the revisions, the Client will be entitled to terminate the data processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 The Data Processor will process the Personal Data on behalf and on behalf of the Client, in accordance with the written instructions provided by the Client and accepted by the Data Processor.

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

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

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

2.7 The Client will guarantee to the Data Processor that it acts in accordance with the GDPR, that it provides a high level of protection for its 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 the Client by the Dutch Data Protection Authority will not be able to be recouped from the Data Processor, except in the event of wilful misconduct or gross negligence on the part of the Data Processor's management team.

ARTICLE 3. SECURITY

3.1 The Data Processor will implement the technical and organisational security measures outlined in its Data Pro Statement. In implementing the technical and organisational security measures, the Data Processor will 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 operations and the intended use of its products and services, the risks inherent in processing the data and risks of various degrees of likelihood and severity to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of the Data Processor's products and services.

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

3.3 The Data Processor seeks to ensure that the security measures it will implement are appropriate for the manner in which the Data Processor intends to use the product or service.

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

3.5 The Data Processor will be entitled to adjust the security measures it has implemented if it feels that such is necessary for a continued provision of an appropriate level of security. The Data Processor will record any significant adjustments it chooses to make, e.g. in a revised Data Pro Statement, and will notify the Client of said adjustments where relevant.

3.6 The Client may request the Data Processor to implement further security measures. The Data Processor will not be obliged to honour such requests to adjust its security measures. If the Data Processor makes any adjustments to its security measures at the Client's request, the Data Processor will be allowed to invoice the Client for the costs associated with said adjustments. The Data Processor will not be required to actually implement these security measures until both Parties have agreed in writing and signed off on the security measures requested by the Client.

ARTICLE 4. DATA BREACHES

4.1 The Data Processor does not guarantee that its security measures will be effective under all conditions. If the Data Processor discovers a data breach within the meaning of Article 4.12 of the GDPR, it will notify the Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which the Data Processor will notify the Client of data breaches.

4.2 It is up to the Controller (the Client or its customer) to assess whether the data breach of which the Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (the Client or its customer) will 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. The 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, the Data Processor will provide more information on the data breach and will help the Client meet its breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information.

4.4 If the Data Processor incurs any reasonable costs in doing so, it will be allowed to invoice the Client for these, at the rates applicable at the time.

ARTICLE 5. CONFIDENTIALITY

5.1 The Data Processor will ensure that the persons processing Personal Data under its responsibility are subject to a duty of confidentiality.

5.2 The Data Processor will be entitled to furnish third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or legal order to do so issued by a government agency.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by the Data Processor to the Client, and any and all information provided by the Data Processor to the Client which gives effect to the technical and organisational security measures included in the Data Pro Statement are confidential and will be treated as such by the Client and will only be disclosed to authorised employees of the Client. The Client will ensure that its employees comply with the requirements outlined 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 will enter into force at the time of the conclusion of the Agreement and will remain effective until terminated.

6.2 This data processing agreement will end by operation of law when the Agreement or any new or subsequent agreement between the parties is terminated.

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

6.4 If the Data Processor incurs any costs associated with the provisions of Article 6.3, it will be entitled to invoice the 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 the Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such cases, the Data Processor will only continue to process the Personal Data insofar as such is necessary by virtue of its statutory obligations. Furthermore, the provisions of Article 6.3 will not apply if the 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, the Data Processor will cooperate with reasonable requests made by the Client relating to Data Subjects claiming alleged rights from the Client. If the Data

Processor is directly approached by a Data Subject, it will refer the Data Subject to the Client where possible.

7.2 If the 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, the Data Processor will cooperate with such, following a reasonable request to do so.

7.3 The Data Processor will be able to demonstrate its compliance with its 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.

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

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

7.6 The Data Processor will be entitled to invoice the Client for any costs it incurs in implementing the measures referred to in this article.

ARTICLE 8. SUB-PROCESSORS

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

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

8.3. The Data Processor will notify the Client if there is a change with regard to the third parties hired by the Data Processor, e.g. through a revised Data Pro Statement. The Client will be entitled to object to the aforementioned change implemented by the Data Processor. The Data Processor will ensure that any third parties it hires will commit to ensuring the same level of Personal Data protection as the security level the 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 requirements arising from the Agreement, including any general terms and conditions and/or limitations of liability which may apply, will also apply to the data processing agreement.

To be approved by the Controller (Client)

Name: _____ Company name: _____

Date: _____ Signature: _____

☐ **I have fully and carefully completed Appendix 1**

Appendix 1

On basis of the record keeping obligation laid down in the GDPR, the processor must keep a register of the processing activities that it has carried out for the benefit of a controller (the client). The processor's register must at least include the following data (as required by Article 28 (3) GDPR):

1 The name and contact details of the controllers and the representative of the contoller, on whose behalf the processor (and sub-processor) acts.

Controller: _____ E-mail: _____
Tel: _____

Representative: _____ E-mail: _____
Tel: _____

2 The category of processing carried out on behalf of controllers (for example: Personnel management / Visitor registration / Membership administration etc) and

3 The purpose for the processing of personal data: Personal data may only be collected for the purpose that is explicitly defined and justified by the controller. The personal data may then only be further processed for purposes compatible with that pre-defined purpose.
(for example: Registration of medical and clinical information for management purposes)

Categorie: _____
Doel:_____

(eg1 Customer Management: To answer questions and complaints from customers and refund payments / eg2 Human Resources Management: For the evaluatioin and management of employees and planning of training.)

4 Types of personal data to be processed:

_____

(The GDPR distinguishes between **directly identifiable** data (Name & address data) and **indirectly identifiable** data (citizen service number (BSN), IP addresses).
The Regulation further distinguishes between **ordinary** personal data, **sensitive** personal and **criminal** data.)

5 Categories of data subjects to which the personal data relates: (for example: Citizens / Employees / Renters / Applicants / Patients etc)

_____

6 Name and contact details of the Data Protection Officer or someone who supervises the application and compliance with the General Data Protection Regulation within the organization.

DPO: _____
E-mail: _____ Tel: _____