Data Processing Addendum

This Data Processing Addendum (**"DPA"**) supplements the General Terms, available **here**. and applicable Specific Terms or other signed agreement in place between Company and Customer covering the use and/or deployment of the onITnow Products by Customer ("Terms").

1. Definitions. Unless otherwise defined in the Terms, if names and terms are written with a capital letter in the DPA, they have the following meaning:

Controller: same meaning as the term defined under the Data Protection Laws.

Customer Personal Data: any information about an identified or identifiable natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in the Data Protection Laws, contained in any code or data provided by Customer to Company for the correct use and/or deployment of the Products that Company Processes under the Terms solely on behalf of Customer.

Data Protection Laws: any law or regulation relating to the protection of personal data, including the Algemene Verordering Gegevensbescherming ("AVG") and the EU General Data Protection Regulation 2016/679 of the European Parliament and the Council ('GDPR').

Data Subject: the data subject whose personal data will be Customer Personal Data subject to this DPA.

Processing (and Process): the same meaning as the term defined under the Data Protection Laws which Company undertakes with respect to Customer Personal Data as part of providing the Products.

Processor: the onITnow entity Processing Customer Personal Data on behalf of the Controller.

Security Incident: any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Company and/or its Sub-processors.

Sub-processor: any third party (including Company Affiliates) engaged by Company to Process Customer Personal Data.

2. Scope. Company will Process Customer Personal Data as Processor in accordance with Customer's instructions set forth in section 4 (Processing of Customer Personal Data). Details regarding the Processing of Customer Personal Data by Company are stated in the Annex to this DPA (Description of Processing).

3. Term. This DPA shall have the same duration as the Terms. Termination of the Terms at any time, does not exempt the Parties from the obligations under this DPA regarding the Processing of Customer Personal Data.

4. Processing of Customer Personal Data. Company will Process Customer Personal Data in accordance with the documented lawful instructions of Customer, as necessary to (i) provide and enable the use and/or deployment of the Products in accordance with the Documentation, (ii) investigate Security Incidents or (iii) comply with its legal obligations. Company will notify Customer without undue delay if it becomes aware, or reasonably believes, that Customer's instructions infringe Data Protection Laws. Company shall treat Customer Personal Data as Customer's Confidential Information as set forth in the Terms. Company will ensure that personnel authorized to Process Customer Personal Data are bound by a duty of confidentiality.

5. Security.

a. Measures. Company has implemented and will maintain appropriate technical and organizational measures designed to protect the security, confidentiality, integrity and availability of Customer Personal Data against Security Incidents. Customer is responsible for configuring the Products and using features and functionalities made available by Company to maintain appropriate security in light of the nature of Customer Personal Data. Customer acknowledges that the security measures are subject to technical progress and development which may be updated or modified by Company from time to time, provided that such updates and modifications do not materially decrease the overall security of the Products during its Duration. Customer shall be kept informed of updates or modifications through Company's normal channels.

b. Security Incidents. Company will notify Customer without undue delay and no later than seventy-two (72) hours after becoming aware of a Security Incident. Company will make reasonably best efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Company's reasonable control. Upon Customer's written request and taking into account the nature of the Processing and the information available to Company, Company will assist Customer by providing information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws. Company's notification of a Security Incident is not an acknowledgment by Company of its fault or liability.

6. Sub-Processing.

a. General Authorization. By entering into this DPA, Customer provides general authorization for Company to engage the Sub-processors stated in the Annex to this DPA, if any, to Process Customer Personal Data. Company will: (i) enter into an agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Customer Personal Data to the standard required by Data Protection Laws and to

the equivalent standard provided by this DPA; and – subject to the applicable section of the Terms - (ii) remain liable to Customer if such Sub-processor fails to fulfil its data protection obligations with regard to the relevant Processing activities under the Terms.

b. Notice of New Sub-processors. If Company appoints a new Sub-processor it will notify Customer in writing at least thirty (30) days prior to allowing a new Sub-processor to Process Customer Personal Data ("Sub-processor Notice Period").

c. Objection to New Sub-processors. Customer may object to Company's appointment of a new Sub-processor during the Sub-processor Notice Period as long as it has serious reasons to do so. If Customer objects, Customer, as its sole and exclusive remedy, may terminate the applicable Order for the affected Product with termination date being the expiration of the Sub-processor Notice Period. The section of the Terms applicable to the effect of expiry or termination of the Terms applies. No refund and/or reimbursement of any fee paid under the applicable Order applies.

7. Assistance and Cooperation.

a. Data Subject Rights. Taking into account the nature of the Processing, Company will provide reasonable and timely assistance to Customer to enable Customer to respond to requests for exercising a Data Subject's rights in respect to Customer Personal Data under the Data Protection Laws.

b. Assistance. Upon Customer's reasonable written request, and taking into account the nature of the Processing, Company will provide reasonable assistance to Customer in fulfilling Customer's obligations under Data Protection Laws, provided that Customer cannot reasonably fulfil such obligations independently with help of available Documentation.

c. Third Party Requests. Unless prohibited by applicable law, Company will promptly notify Customer of any law enforcement or court order compelling Company to disclose Customer Personal Data. In the event that Company receives an inquiry or a request for information from any other third party (such as a regulator or Data Subject) concerning the Processing of Customer Personal Data, Company will redirect such inquiries to Customer, and will not provide any information unless required to do so under applicable law.

8. Deletion and Return of Customer Personal Data. Subject to the applicable Documentation, (i) Customer and its Users may, through the features of the Products, access, retrieve or delete Customer Personal Data and (ii) following expiration or termination of the Terms, Company shall delete all Customer Personal Data. Notwithstanding the foregoing, Company may retain Customer Personal Data (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Company will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to retained Customer Personal Data and not further Process it, except as required by Data Protection Laws.

9. Audit. Company will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data, provided that such right may be exercised no more than once every twelve (12) calendar months. Where required by Data Protection Laws or a regulatory authority, Customer, or its authorized representatives, may, at Customer's expense, conduct audits (including inspections) during the duration of the Terms to assess Company's compliance the terms of this DPA. Any audit must (i) be conducted during Company's regular business hours, with reasonable advance written notice of at least thirty (30) calendar days (unless Data Protection Laws or a regulatory authority requires a shorter notice period); (ii) be subject to reasonable confidentiality controls obligating Customer (and its authorized representatives) to keep confidential any information disclosed that, by its nature, should be confidential; (iii) occur no more than once every twelve (12) months; and (iv) restrict its findings to only information relevant to Customer.

10. Applicable Law and Jurisdiction. The DPA is governed exclusively by Dutch law. All disputes arising out of or in connection with the DPA shall be submitted to the competent courts in The Hague (The Netherlands), without prejudice to the right of the parties to request preliminary relief. The United Nations Convention on Contracts for the International Sale of Goods will not apply.

11. Order of Precedence. If there is any conflict or inconsistency among the following documents, the order of precedence is: (1) this DPA and (2) the Terms.

Accepted and Agreed:

COMPANY	**CUSTOMER**
_____	_____
Signature	**Signature**
Name	**Name**
Title	**Title**
Date	**Date**

Annex
Data Processing Addendum

Description of Processing

Product

☐ Implementation and/or configuration of Third Party Product ("Services")
☐ Standard Support Services
☐ Clientele IT Service Management Software ("Software")

Company Security Officer

Carlo Huijbregsen, c.huijbregsen@onitnow.nl, telephone +31 (0)85 0046150.

Categories of Data Subjects

Services
Customer's User(s) and Customer's clients

Standard Support Services
Customer's User(s) and Customer's clients

Software
Customer's User(s)

Customer Personal Data Processed

☐ Full name
☐ Home address
☐ Email address (e.g. name.surname@domain.com)
☐ Phone number
☐ Identification numbers (e.g. passport, national ID, social security)
☐ IP address
☐ Other: _____

Capturing Customer Personal Data

Services
The Services provided by Company will be the means to transport Personal Data of Data Subjects to the third party platform.

Standard Support Service
Personal Data provided by Customer when reporting a Request as set forth in the onITnow Specific Terms Standard Support Services.

Software
Users of the Software are free to record data of any kind. The method of recording is up to the Users.

Sensitive Customer Personal Data

The Software and Services do not include the Processing of sensitive Customer Personal Data - such as data concerning race, ethnic origin, political opinions, religious beliefs, data concerning health, etc. - or the processing of data concerning criminal convictions and criminal offences. Processing of these data with the Software and Services by Customer shall be solely determined and controlled by Customer at its own and sole risk.

Privacy by Design

Services
With every new Services, Company carries out a Privacy by Design and Default Assessment. Registration of all steps of this assessment takes place at the GDPR Compliance Platform ("Platform") that Company has set up for its own Services and for managing GDPR requests from Customers and Data Subjects.

Standard Support Services
Not applicable

Software
The Software is not developed with privacy by design, as this is not primarily the purpose of the Software. However, there are options to protect notifications containing any Customer Personal Data through the use of data limitation. The reports that may not be viewed by every User of the Software are protected on the basis of a processing system-oriented department within the Software. By default,

it is possible to view all data. Depending on additional set-up in the Software, Users who are not members of such a department may not directly view the data.

Area

Company exclusively processes Customer Personal Data within the European Union (EU) and the European Economic Area (EEA).

Services: Germany or Ireland

Standard Support Services: The Netherlands and Germany

Software: The Netherlands or Ireland

Should Customer Personal Data have to be transferred outside the EU or EEA, then its Processing will be subject to the Standard Contractual Clauses ("SCCs") which are to be considered incorporated into this DPA.

Requests from Data Subjects

Services
The Platform registers and Processes requests from Data Subjects in accordance with Data Protection Laws.

Standard Support Services
The Platform registers and Processes requests from Data Subjects in accordance with Data Protection Laws.

Software
The Software has functionalities built in in order to meet Customer's written requests in accordance with Data Protection Laws.

Retention of Personal Data

Services
The deletion of Customer Personal Data will occur within 3 months as of the expiration or termination of the Terms unless the Data Protections Laws require a different retention period.

Standard Support Services
The deletion of Customer Personal Data will occur within 3 months as of the expiration or termination of the Terms unless the Data Protections Laws require a different retention period.

Software
Within 3 months as of expiration or termination of the Terms, Customer will instruct Company if it either wants to proceed with (i) removal and destruction of the Customer Personal Data (no copy of the databases shall be made available to Customer) or (ii) removal of the Customer Personal Data (a copy of the databases shall be made available to Customer at the one-off payment by Customer of € 250,=).

Customer shall be solely responsible for complying with applicable legislation relating to the retention period of (personal) data. Customer shall have to take this into account when choosing whether to destroy or transfer data from the SaaS environment.

Sub-processors

Services

AMAZON

Purpose of Sub-processor	Provision of AWS
Data Element Processed	Data defined in the specifications of the Services provided to Customer
Purpose of Processing	Allow the interaction of data between the third party's and Customer specific environment in a standardized platform
Data Location	EU – Central – 1 (Frankfurt, Germany)

TECHWORK

Purpose of Sub-processor	Provision of Techwork Automator Platform
Data Element Processed	Data defined in the specifications of the Services provided to Customer
Purpose of Processing	simplifying and accelerating the development and deployment of automations
Data Location	Ireland (Dublin)

XURRENT

Purpose of Sub-processor	Provision of Service Management Application
Data Element Processed	Data defined in the specifications of the Services provided to Customer
Purpose of Processing	Administrative process of the provision of Services related to Xurrent Services (Third- Party Product)
Data Location	EU – Central – 1 (Frankfurt, Germany)

AUTOM MATE

Purpose of Sub-processor	Provision of Integration, Automation and Provisioning platform.
Data Element Processed	Data defined in the specifications of the Services provided to Customer
Purpose of Processing	simplifying and accelerating the development and deployment of automations
Data Location	AWS : EU – Central – 1 (Frankfurt, Germany)

Standard Support Services

XURRENT	
Purpose of Sub-processor	Provision of Service Management Application
Data Element Processed	Data provided by Customer when reporting a Request as set forth in the onITnow Specific Terms Standard Support Services.
Purpose of Processing	Administrative process of the managing of submitted Requests related to Services, Software and/or Support Services applicable to Third- Party Products
Data Location	EU – Central – 1 (Frankfurt, Germany)
MICROSOFT	
Purpose of Sub-processor	Provision of Azure cloud environment
Data Element Processed	Data provided by Customer when reporting a Request as set forth in the onITnow Specific Terms Standard Support Services applicable to Software
Purpose of Processing	Administrative process of the managing of submitted Requests related to the Software
Data Location	The Netherlands / Ireland

Software

MICROSOFT

Purpose of Sub-processor	Provision of Azure cloud environment
Data Element Processed	Depends on Customer's requirements
Purpose of Processing	Supporting Customer's primary processes
Data Location	The Netherlands / Ireland

ELASTIC SEARCH

Purpose of Sub-processor	Provision of search- and indexation services (indexation data)
Data Element Processed	All categories of data, which are an integral part of the Software
Purpose of Processing	Making a full text search result available in a structured way
Data Location	West Europe

Security

General

Services
InfraVision ISO IEC 27001-2022
Joost-IT NEN-ISO/IEC 27001: 2017

Software
NEN-ISO/IEC 27001+C11+C1

Each a "Standard".

Following the Standard, Company has taken and formalised organisational, physical and technical security measures to protect Customer Personal Data against loss or unlawful Processing. These measures are included in the Statement of Applicability. At Customer's written request to the Company Security Officer, Customer will be provided with a copy of the Statement of Applicability.

Certification

Company is compliant with the Information Security Management System (ISMS) Standard and is also certified as such.

At Customer's written request to the Company Security Officer, Customer will be provided with a pdf. version of the Standard certificate.

Organizational Security Measures

Company has established a process for communication regarding Security Incidents.

After the implementation of the following measures, the Company Security Officer conducts checks and make rectifications, to ensure conformity with the Standard information security policy.

Security Incidents are recorded and support process optimisation, the procedure for handling Security Incidents, and the information security policy.

Confidentiality agreements are in place with all Company's employees and contractors.

Company's Information security policy is made aware to all Company's employees and, if applicable, its contractors.

Company trains Company's employees to support awareness, knowledge and responsibility with regard to privacy and information security.

Company's information security policy is improved and optimised on a regular basis of which Company's employees and contractors are informed, wherever applicable.

Physical Security Measures

The environment and location in which data are processed are periodically checked, maintained and tested for security risks.

Customer Personal Data is only processed in a closed, physically secured environment with protection against external threats.

Backups are treated as confidential and stored in an environment that is only accessible to Company's personnel appointed and authorised for that purpose.

In addition and only applicable to the Software,

- Customer Personal Data is only processed on (virtual) assets, in which connection, measures have been taken to physically and logically protect these assets and to ensure the continuity of the Software and the cloud service.
- Periodic backups are made and tested to ensure the continuity of the Software and the cloud service.

Technical Security Measures

Strict security is maintained within the network environment in which data is Processed, with separation of traffic flows, and implementation of measures against abuse and attacks.

The environment in which Customer Personal Data is Processed is monitored for availability, security and integrity.

The application infrastructure within which Customer Personal Data is Processed is set up on the basis of a standardised operations management process, security control and acceptance process.

Changes in applications and underlying systems are tested for vulnerabilities before commencement of production of the same.

The latest (security) patches are periodically installed in all components of the application infrastructure according to patch management and current internal and external security recommendations.

Application of the OWASP (Open Web Application Security Project) standard in software development. Periodic penetration tests and vulnerability assessments are conducted.

Passwords are subject to cryptographic storage and access measures.

Encrypted connections are used for login processes.

Continuity management procedure: measures relating to continuity of information security in case of threat or occurrence of fire, water damage, radiation, air pollution and/or other calamities.

Cryptographic measures are applied to every form of transport of Customer Personal Data.

In addition to the aforementioned and only applicable to the Software,

- The exchange of Customer Personal Data between Company and Customer is encrypted. This also applies to the communication between the Software installed at Customer's premises and Company's IT environment.
- The exchange of Customer Personal Data with third parties on behalf of Customer is encrypted.

Procedure Security Incident

Company shall notify Customer in writing concerning Security Incidents with the following characteristics:

- Events that may result or that have resulted in the unavailability of Customer Personal Data
- Events that may result or that have resulted in a violation of the integrity of (Customer Personal) Data
- Events that may result or that have resulted in a violation of the confidentiality of (Customer Personal) Data.

The aforementioned Security Incidents are reported to Customer via (one of) the following channels:

- By e-mail (standard)
- By telephone

The follow-up of a Security Incident via the Customer portal may be consulted by the Controller.

If possible, the notification of a Security Incident by Company to the Customer shall at least contain the following information:

- Time of notification
- Company owner incident: Contact details such as name, job title, e-mail address and telephone number of the Company employee
- Minimum and maximum number of persons whose Customer Personal Data is breached
- Description of group of persons whose Customer Personal Data is involved in the Security Incident
- Time of breach. If known: date, time, end
- Description of type of Customer Personal data involved in the Security Incident. What consequences can the breach have for the privacy of the Data Subjects?

Data Access Authorization Matrix

Access to data is only allowed if strictly necessary for the proper performance of a function /role within Company's organisation. See the matrix below:

Purpose of Processing		
Function / Role & categories of data	**Processing by Company**	**Role Company**
Account management & Sales: Customer and its employees' contact details such as name, telephone number, e-mail address, and contract details.	Recording and updating	Controller
Financial administration: Customer and its employees' contact details such as name, telephone number, e-mail address, licence and contract details.	Recording and updating, invoicing and communication of licence details	Controller
Support desk: Data on notifications that are recorded in a structured manner. Customer's User(s) contact details such as name, telephone number, and e-mail address. If applicable, other information required or made available to support the Services, the Third Party Product and the Software.	Recording and updating Customer contact details and notification of data about the Customer.	Controller
Consultants: Customer's User(s) and employee's and – if applicable – its third party's contact details such as name, telephone number, and e-mail address. If applicable, other information required or made available to support the Services, the Third Party Product and the Software.	Access to Customer environment for functional design. (Temporary) access to Customer environment at Customer's request. Limited and specific access to accounts and passwords in Customer environments.	Processor
DevOps engineers: Customer's User(s) and employee's and – if applicable – its third party's contact details such as name, telephone number, and e-mail address. If applicable, other information required or made available to support the Services, the Third Party Product and the Software.	Initial set-up of the Customer environment, migration databases, creation and modification of Customer specific account information, technical set-up and change in the Customer environment in order to realise and optimise the operation of the Third-Party Product and the Software offered. (Temporary) access to Customer environment at Customer's request. Access to databases. Access to accounts and passwords for Customer environments.	Processor