DATA PROCESSING AGREEMENT

Universal IT B.V.

Comprised of:

Part 1. Data Processor (Data Pro) Statement

Part 2. Standard Clauses for Data Processing

Universal IT BV
WTC Arnhem
Nieuwe Stationsstraat 10
6811 KS Arnhem
The Netherlands

T +31 (0)26 20 20 020
F +31 (0)26 20 20 030

info@universal.nl
www.universal.nl

KvK 09156724
ING 4930278
IBAN NL14 ING B0004930278
BIC INGBNL2A
BTW NL815291954B01

Version **1.0 / 24-05-2018**

The Data Pro Code was 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:**

   Universal IT B.V., Nieuwe Stationsstraat 10, Arnhem, Netherlands.
   If you have any queries about this Data Pro Statement or data protection in general, please contact the Universal Security Officer (*so@universal.nl*).

2. **This Data Pro Statement will enter into force on *24-05-2018***

   We regularly revise the security measures outlined in this Data Pro Statement to ensure that we are always fully prepared and up to date regarding data protection. If this document is updated, we will notify you through our regular channels.

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

   Universal private cloud
   Hosted Skype for Business, Hosted SharePoint Server, Hosted Dynamics 365, Hosted Anywhere 365, Hosted Exchange, Universal Backup, Hosted SQL, Hosted Remote Desktop Services, Managed Virtual Server and Hosted VOIP/FAX.

   Azure/Office 365
   Including but not limited to the following licenses and products purchased through the MS Cloud Solution Provider (CSP) Program: SharePoint Online, Exchange online, OneDrive for business, Teams, Skype for business online, Azure, Intune, MS Graph, Dynamics365 and Yammer.

   Skykick
   Exchange e-mail migration to Office 365 and backup services for OneDrive for Business, SharePoint Online and Exchange Online.

4. **Description of product/services**

   Universal private cloud: *www.universal.nl*
   Office 365: *https://products.office.com/en/home*
   Anywhere 365: *https://www.workstreampeople.com/platform-element-anywhere365-core/*
   Skykick: *https://www.skykick.com/backup*
   Azure: *https://azure.microsoft.com/nl-nl/*

5. **Intended use: Product/service is designed and equipped to handle the following types of data:**
   General information that increases productivity for companies, such as emails, customer information, financial data, documents, intranet, phone calls (call detail records) and project files.

   When this product/service was designed, the possibility that it would be used to process special categories of personal data or data regarding criminal convictions and offences was not taken into account. It is up to the client to determine whether or not it will use the aforementioned product or service to process such data.

6. **When the data processor designed the product or service, it applied the privacy-by-design approach in the following manner:**
   Clients upload their own data, including attachments chosen by them, and can modify and delete these data and documents. Data Processor does not check the data and will only view data at the request of the client, for example, if necessary to deliver support services by the Universal support desk.

7. **The data processor adheres to the Data Processing Standard Clauses for Data Processing which can be found in part 2 of this document.**

8. **The data processor will process the personal data provided by its clients within the EU/EEA. If data is stored in the US, it is specifically requested by the client.**

9. **If the data are to be processed in the US: the data processor has ensured in the following way that the personal data will be protected to an appropriate standard:**

   - https://www.microsoft.com/en-us/trustcenter/privacy/default.aspx

10. **The data processor uses the following sub-processors:**

    - → *Microsoft Office 365/Azure*

      https://www.microsoft.com/en-us/trustcenter/privacy/default.aspx

    - *(optionall) IBM Cloud*

      EU Data Protection Code of Conduct for Cloud Service Providers

      - *https://www.ibm.com/blogs/policy/eu-cloud-code-of-conduct/*

11. **The data processor will support its clients in the following way when they receive requests from data subjects processor:**

    Universal it registers data in her CRM system to enable the purchasing/sales process and to support the services through the Universal Customer Portal. For this purpose, general contact information such as email and phone number are used to identify users. Clients can view which contact information is registered in the system by logging in to the online portal (https://portal.universal.nl).

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

    - **Delete back-up files**
    - **Delete production data (sites/mailboxes/virtual machines and databases).**

SECURITY POLICY

13. Data processor has implemented the following security measures to protect its product or service:

By building and maintaining an information security structure and making this demonstrable, Data processor has chosen to have the ISMS certified according to the ISO27001:2015 standard. The starting point is to comply with the Requirements and wishes of the stakeholders, applicable laws and regulations and the ISO 27001:2015 standard.

Data Processor strives to ensure continuous improvement of quality regarding information security. To guarantee this, audits are carried out regularly on the management system. Based on the outcome of these audits, an activity plan will be drawn up periodically to describe the objectives. The management review will be done by the management and the Security Officer.

Supporting documentation

The following documents support the Universal IT Information Security Policy:

- Context analysis (issues, Stakeholder, risk analysis and Compliance overview)
- Staff Manual
- User agreements
- Procedures, instructions and ISMS forms

Additional ISMS policy documentation;

- Access security Policy
- Classification of information (and processing)
- Physical and environmental protection
- Topics aimed at the end user such as:
    - Acceptable use of assets
    - 'Clear desk' and 'clear screen'
    - Mobile Devices and teleworking
    - Limitations on software installations and usage
- Back-up policy

- Information transport Policy
- Management of technical vulnerabilities policy
- Cryptographic management measures
- Communication Security Policy
- Vendor Relations Policy

14. Information Security principles

Regarding information security, the following principles are used:

A) Strive to be compliant with the NEN-ISO/IEC 27001:2015 Standard as drawn by the National Cyber Security Centre (NSCS).

B) Comply with all applicable laws and regulations. In this context, it is explicitly mentioned: General Data Protection Regulation (GDPR).

C) Information Security is part of the integral management responsibility. The Security Officer is responsible for all data processing elements.

D) When partnerships are engaged with external parties, either in terms of content or in the development or management of the information services, attention is paid to information security. Agreements on this are drawn up in writing and monitored on compliance. Data processor ensures compliance with legal and contractual obligations.

E) Business processes, information systems and data collections of the relevant components are classified according to a structured method according to the aspects of availability, integrity and confidentiality.

F) During hiring, employment and in the event of dismissal of employees, explicit attention is paid to the reliability of employees and safeguarding the confidentiality of information.

G) Data processor implements an active policy to stimulate the security awareness of management and employees.

H) Data Processor has rules of conduct for the use of (general) information Services. Compliance with these rules of conduct is monitored.

I) In case of abuse of security regulations, the Universal management may impose a sanction in accordance with the terms and conditions regarding suspension, penalties and/or contract termination in the employment contract. A sanction policy has been drawn up.

J) Measures have been taken to ensure the physical security of offices, spaces and resources.

K) All Data processor components have taken measures to ensure the security and management of operational information and communication facilities. Measures against all types of malicious software (computer viruses, spam, spyware, etc.) are an important part.

L) Measures have been taken to ensure that only authorized employees can make use of the information and communication facilities.

M) In the development and procurement of information systems and procurement of relevant resources, attention is paid to information security at all stages of the acquisition or development process.

N) Adequate measures have been taken to ensure the availability of the business processes and the information systems, both in normal and in exceptional circumstances.

O) As part of the information security policy process, internal and external parties monitor compliance with the information security policy within the Data processor.

All Data processor components have resources for reporting and handling security incidents. The evaluation of security incidents is used to improve information security. The management and the Security Officer ensure that each employee is familiar with this policy and works accordingly.

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

- ISO 27001 (Implementation goal completed Q3 2018)

16. Data processor has obtained or is working on implementing the following certificates:

- ISO 27001 (Implementation goal completed Q3 2018)

DATA LEAK PROTOCOL

17. 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:

Data processor uses firewall monitoring tools to detect potential security incidents. Recurring security audits are being performed. A procedure for internal reporting of incidents is implemented. If the data processor detects a data leak, the data processor will notify its client as soon as possible by contacting the primary contact via email or phone. Data processor provides as much relevant data as possible (IP Address, protocol, etc.), including description of the incident, nature of the infringement, nature of the personal data or categories of data subjects involved, estimation of number of effected data subjects and possibly related databases and indication when incident occurred.

For questions about an incident, the controller can contact the Security Officer (so@universal.nl) to discuss the possible consequences (what can possibly happen, what is / might be the impact). The controller then needs to assess the consequences, since the data processor does not check the supplied data and therefore is not always aware of the nature of the processed data.

After an incident, data processor and controller will consult to mitigate any damage or prevent this in the future by taking measures by the controller or data subjects concerned (which actions can be performed by data subjects, for example "monitor email traffic, change Passwords, etc.).

Notifications to clients will be done if possible within 48 hours. Data processor will not make any reports to AP or data subjects. Reporting on the issue is the responsibility of the Controller. The data processor will support the client or the controller if necessary in this reporting process.

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.