



Data Processing Agreement uWebChat

Part 1. Data Pro Statement uWebChat · Part 2. Standard Clauses for Data Processing

Version	2.0 / 01-08-2026
Applies to	uWebChat: live chat, virtual assistant and the WhatsApp channel for websites and Microsoft Teams
Data processor	Universal IT B.V., trading as uWebChat Nieuwe Stationsstraat 10, 6811 KS Arnhem, the Netherlands KvK 09156724
Contact	Security Officer, so@universal.cloud
Certification	ISO/IEC 27001:2022, Kiwa Nederland B.V., certificate K-0221887

This data processing agreement constitutes the agreement within the meaning of Article 28(3) GDPR between the client and the data processor for the use of uWebChat. Part 2 contains the NLdigital Standard Clauses for Data Processing (version November 2023).

Part 1: Data Pro Statement uWebChat

Along with the Standard Clauses for Data Processing (Part 2), this Data Pro Statement constitutes the data processing agreement for uWebChat, provided by Universal IT B.V. (hereafter: uWebChat or the data processor).

General information

1. This Data Pro Statement was drawn up by Universal IT B.V., trading as uWebChat, Nieuwe Stationsstraat 10, 6811 KS Arnhem, the Netherlands (KvK 09156724). If you have any queries about this Data Pro Statement or data protection in general, please contact the Security Officer at so@universal.cloud.
2. This Data Pro Statement enters into force on 1 August 2026. It is reviewed at least once a year and whenever uWebChat functionality, sub-processors or security measures change significantly. Clients are notified of a new version by e-mail to the administrator registered for their uWebChat licence; the current version is always published at www.uwebchat.com.
3. This Data Pro Statement applies to uWebChat, including:
 - the uWebChat chat widget and chat window for websites;
 - the uWebChat app for Microsoft Teams, through which agents answer conversations;
 - the virtual assistant (AI agent), real-time translation and speech to text;
 - MeetNow (video and voice calls through Microsoft Teams), media sharing, transfer, leave a message, transcripts and archiving;
 - visitor authentication, the ban function and the country blocklist;
 - the WhatsApp Business channel, when activated by the client;
 - uWebChat licence and configuration management.uWebChat Voice (contact centre and telephony) is not covered by this statement.
4. A description of uWebChat and its functions is available at www.uwebchat.com.
5. **Intended use.** uWebChat is designed and equipped to process the following types of data:
 - *Website visitors:* the name a visitor enters, optional custom fields chosen by the client (such as e-mail address, phone number, company and country), the content of chat messages and shared files and images, the visitor's IP address (used for the ban function and the country blocklist), browser language and a randomly generated chat user ID.
 - *Visitor authentication:* the e-mail address or phone number of the visitor and the one-time verification code, when the client activates this function.
 - *Agents:* the Microsoft Teams identity of agents (name, profile picture or avatar, presence status) and their language settings.
 - *WhatsApp:* phone number, profile name and messages of WhatsApp users, only when the client activates the WhatsApp channel.
 - *Administration:* the client's Microsoft 365 tenant ID and organisation name, licence keys, licensed domains, uWebChat configuration, the configuration of virtual assistants (name,

description, system prompt and the e-mail address of the person who created it) and the endpoint and key of the client's own Azure OpenAI resource.

When uWebChat 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 it will use uWebChat to process such data, to inform its agents and visitors accordingly and to take additional measures where needed.

6. Privacy by design. When uWebChat was designed, the privacy-by-design approach was applied in the following manner:

- *No conversation archive.* uWebChat relays messages between the visitor and Microsoft Teams in the client's own Microsoft 365 tenant. Conversations are stored in the client's Teams environment and are subject to the client's own Microsoft 365 retention, eDiscovery and Purview settings. uWebChat does not build an archive of conversations: during a conversation it keeps the session and the conversation history only to continue the chat across pages and to produce the transcript. The conversation history used for the transcript is held only in the working memory of the uWebChat service, never in a database or file, and is removed as soon as the conversation ends. Conversations that are not ended properly are removed automatically after at most eight hours of inactivity. The session data (such as visitor name, contact details and IP address) is removed when the conversation is disconnected, and in any case after one day of inactivity. After a conversation, uWebChat only keeps technical metadata (conversation ID, agent, start and end time) for licence administration and reporting; this metadata contains no message content.
- *Transcripts and archiving* are delivered to the client's own OneDrive, to the visitor (as a download) or by e-mail, as configured by the client. Images can be left out of transcripts. Conversations with the virtual assistant are only saved when the client switches on "Save Conversation History"; they are then offered to the group owner and can be saved to the client's OneDrive.
- *Minimal storage in the browser.* The chat widget stores nothing in the visitor's browser before a chat is started. When a chat starts, a randomly generated chat user ID is stored in local storage. When an agent connects, two functional cookies (uWebChatToken and uWebChatDomain) are set with a lifetime of 30 minutes, so the conversation continues when the visitor opens another page. All three are removed when the session ends. The chat window contains no analytics or tracking, and all scripts it uses are hosted by uWebChat or Microsoft, so no visitor data is sent to other third parties.
- *AI in the client's own environment.* The virtual assistant uses Azure OpenAI resources in the client's own Microsoft Azure tenant. Prompts and answers are processed under the client's own agreement with Microsoft and are not used by uWebChat to train AI models. AI functions only process data for the function the client has activated. Real-time translation (Azure AI Translator) and speech to text (Azure AI Speech) run on Azure resources of uWebChat in the West Europe region; they are only used when the client has activated these functions. Text is sent for translation without being stored; spoken input is sent directly from the visitor's browser to Azure AI Speech.
- *Data minimisation.* The client decides which custom fields visitors are asked to fill in, whether visitor authentication is required and whether channels such as WhatsApp are

activated.

- *Hosting in the EU.* The uWebChat service and its licence administration run on Microsoft Azure in the West Europe region (the Netherlands), including data storage, key management and logging. Azure Bot Service, which delivers messages to Microsoft Teams, is a global Microsoft service that does not store message content and falls under the Microsoft EU Data Boundary.
- *Content safety.* Images and files shared in a conversation are checked with Microsoft Azure AI Content Safety before delivery.
- *Isolation.* Each client is identified by its Microsoft 365 tenant. Conversations are only delivered to agents in the tenant and domains registered for the licence.
- *Access.* Access to the uWebChat platform is limited to authorised engineers, protected by multi-factor authentication and Conditional Access, and granted on a least-privilege basis. Changes to production are approved and logged.
- *Encryption.* Data is encrypted in transit (TLS) and at rest (Microsoft Azure platform encryption).

7. The data processor adheres to the Standard Clauses for Data Processing in Part 2 of this document. Personal data is processed within the EU/EEA. Processing outside the EU/EEA only takes place where a sub-processor listed in item 9 requires it, and always under the safeguards in item 8.

8. If personal data is processed outside the EU/EEA, it is protected as follows:

- Microsoft: the Microsoft Products and Services Data Protection Addendum, the EU Data Boundary and the EU Standard Contractual Clauses.
- Other sub-processors: the EU Standard Contractual Clauses and, where applicable, the EU-US Data Privacy Framework, as stated in the table below.

9. The data processor uses the following sub-processors:

Sub-processor	Purpose	Location and safeguards
Microsoft Ireland Operations Ltd.	Hosting of the uWebChat service and licence administration on Microsoft Azure, Azure Bot Service for message delivery to Microsoft Teams, Azure AI Content Safety for shared images and files, Azure AI Translator and Azure AI Speech (when activated), Azure Maps for determining the country of an IP address (country blocklist), application logging	EU; Microsoft DPA, EU Data Boundary, SCCs
Bird B.V. (formerly MessageBird), the Netherlands	Connection to the WhatsApp Business Platform, only when the client activates the WhatsApp channel	EU
Meta Platforms Ireland Ltd. (WhatsApp Business Platform)	WhatsApp channel, only when activated by the client	EU; Meta data processing terms, SCCs
Microsoft Ireland Operations Ltd. (Azure Communication Services)	Sending verification codes by e-mail and SMS (visitor authentication)	EU (data location Europe); Microsoft DPA, EU Data Boundary, SCCs. SMS messages are delivered through the telecom carrier of the recipient.

Microsoft 365, Microsoft Teams, OneDrive and Azure OpenAI resources in the client's own tenant are contracted by the client directly and are not sub-processors of uWebChat. Changes to this list are announced by e-mail to the licence administrator at least 30 days in advance.

10. **Data subject requests.** Because conversations are stored in the client's own Microsoft 365 environment, the client can fulfil most requests from data subjects (access, export, correction, deletion) itself, using Microsoft Teams, OneDrive and Microsoft Purview. For data held by uWebChat, such as licence administrator details and data in application logs, uWebChat assists within ten working days of a request. Requests can be sent to so@universal.cloud.
11. **End of agreement.** Within three months after the agreement has ended, uWebChat deletes the personal data it processes on behalf of the client, in such a manner that it can no longer be used:
 - licence, domain and configuration data of the client, including virtual assistant settings and the stored Azure OpenAI endpoint and key;
 - application logs, at the end of their retention period. Logs are used for error handling, troubleshooting and security, and may contain technical details of a conversation at the moment of an error, such as the display name of a visitor or agent, an agent's e-mail address and a visitor's IP address. The content of chat messages is not logged. Logs are stored in Microsoft Azure (West Europe) and deleted automatically after at most 90 days.

Conversations, transcripts and archives stored in the client's own Microsoft 365 tenant remain under the control of the client.

Security policy

12. uWebChat is developed and operated by Universal IT B.V. under an Information Security Management System (ISMS) certified against ISO/IEC 27001:2022 by Kiwa Nederland B.V. (certificate K-0221887, valid until 16 December 2027). The scope of the certificate includes "development, maintenance and management of cloud-based hosting environments and intelligent data driven communication systems". Internal audits are carried out annually, an external audit is carried out every year by the certification body, and a management review is performed by the management and the Security Officer.
13. The following measures apply to uWebChat in particular:
 - access control with multi-factor authentication, Conditional Access, least privilege and periodic access reviews;
 - secure development: code review, dependency and vulnerability scanning and approval before deployment to production;
 - abuse protection: agents can ban visitors, and the client can block countries;
 - visitor authentication with a one-time code before a conversation starts, when activated by the client;
 - logging and monitoring of the uWebChat platform with Microsoft Defender;
 - suppliers and sub-processors are assessed at least once a year.
14. The data processor conforms to the principles of the ISO/IEC 27001:2022 Information Security Management System.
15. The data processor has obtained the following certificate: ISO/IEC 27001:2022 (Kiwa Nederland B.V., certificate K-0221887, valid until 16 December 2027).

Data breach protocol

16. If the data processor detects a (suspected) personal data breach affecting a client, it notifies the client without undue delay and where possible within 48 hours after establishing the breach, by e-mail and phone to the licence administrator. The notification contains as much relevant information as possible: a description and the nature of the breach, the categories of personal data and data subjects involved, an estimate of the number of data subjects and records affected, when the breach occurred and was discovered, and the measures taken. The client, as controller, assesses the consequences and decides whether the breach must be reported to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and to data subjects. The data processor does not make such reports itself, but supports the client in doing so. After an incident the parties consult on measures to limit damage and prevent recurrence. Every incident, its cause and the corrective actions are recorded in the ISMS.

Part 2: Standard Clauses for Data Processing

Version: November 2023 (NLdigital Standard Clauses for Data Processing). 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 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 times, 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.