ROGER365.io

LEGAL · GDPR

Data Processing Agreement

ROGER365.io B.V.

Version 1.0 · June 2026

COMPRISED OF

Part 1 Data Pro Statement

Part 2 Standard Clauses for Data Processing

Based on NLdigital Standard Clauses (March 2025), with amendments.
Privacy review: 15 June 2026.

Confidential

PART 1

Data Pro Statement

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

General information

1 This Data Pro Statement was drawn up by the following Data Processor (*verwerker*): ROGER365.io B.V., Elektronicaweg 37, 2628 XG Delft, The Netherlands. Registered with the Dutch Chamber of Commerce (*Kamer van Koophandel*) under number 82264996.

> CONTACT If you have any queries about this Data Pro Statement or data protection in general, please contact: dataprotection@roger365.com.

2 This Data Pro Statement shall enter into force on the date on which the Agreement becomes effective. The Agreement, of which this Data Processing Agreement forms an integral part, is concluded electronically during online enrolment, when an authorised administrator (a Microsoft Entra ID Global Administrator of the client's tenant, or a partner acting on the client's behalf with such rights) accepts the Privacy Policy and the Terms of Service. No separate agreement is signed or required.

We regularly revise the security measures described in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. If this document is updated, we shall notify you of the revised versions through our regular channels. Revised versions are communicated through our regular channels, including the ROGER365 partner community, and the published version on our website.

3 This Data Pro Statement applies to the following products and services provided by data processor: The ROGER365.io platform, a multi-tenant, omnichannel Contact Center as a Service (CCaaS) integrated with Microsoft Teams, including the Contact Center and Attendant Console products and related modules. This Data Pro Statement applies to the platform as a whole. The Agreement between Data Processor and client specifies which products/services have been purchased.

4 **Description of product(s)/service(s).** The ROGER365.io platform enables organisations to handle inbound and outbound customer communication (voice, webchat, WhatsApp and supported social channels) within Microsoft Teams. It provides queue-based and skill-based routing, presence-based call handling, an attendant/transfer experience, reporting and analytics, and optional AI-driven functionality. The platform is built on the Microsoft Teams Extend and Unify model and is intended for business use by SMB and enterprise organisations. A more detailed functional description is set out in the Agreement and the product documentation at doc.roger365.io.

5 **Intended use.** Product/service is designed and built to process the following types of data: The platform is designed to process: agent and supervisor identifiers (name, User Principal Name, Microsoft Entra ID Object ID); contact and interaction data relating to customer communications (such as caller line identification, channel identifiers, queue and routing data, timestamps and interaction metadata); the content of customer communications handled through the platform (e.g. chat messages, and, where enabled by the client, call recordings and transcriptions); where the client chooses to enable this, transcriptions of recorded calls stored in the platform database and linked to the relevant interaction (including the caller's telephone number and any imported CRM data), so that they can be presented to an agent during a subsequent contact; and optional CRM data that the client chooses to make available to the platform. The specific personal data processed is determined by the client's configuration and use of the platform at the client's sole responsibility.

> The potential processing of sensitive personal data of client, including special categories of personal data, data regarding criminal convictions and offences or national identification numbers, has not been separately assessed in the context of this product/service. It is the client's sole responsibility as controller of personal data to assess and determine whether the platform is appropriate for the processing of such data in accordance with applicable law, including but not limited to data protection laws such as the General Data Protection Regulation (GDPR).

6 **Privacy by design/privacy by default.** While the client, as controller of personal data, remains responsible for applying privacy by design and privacy by default in its own use of the platform, Data Processor has implemented a number of supporting measures by default. These include:

- data minimisation: tenant databases hold only agent identifiers and the data the client chooses to provide, and no special categories of personal data are stored by design;
- encryption by default (AES-256 at rest and TLS 1.2+ in transit);
- logical tenant isolation;
- least-privilege, need-to-know access controls;
- configurable data retention: the client sets the retention period for call detail records and the content of customer communications, including stored transcriptions; the default retention period is 180 days, and configurable between a minimum of 1 day and a maximum of 12 months. Other platform data used for monitoring, security logging and billing is retained for its own fixed periods and is not client-configurable); and
- the use of synthetic, non-production data sets for all development and testing so that client data is never copied into non-production environments.

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

8 Data processor processes personal data within the Microsoft Azure region that is determined by the client's Microsoft 365 tenant. This region may be within the EU/EEA or, depending on the client's tenant and configuration, outside the EU/EEA (for example the United States, the United Kingdom or Australia). It is therefore possible that personal data is processed (partially) outside the EU/EEA. Data processor has ensured in the following way that the personal data shall be protected to an appropriate standard, being:

- either the country/area/industry/international organisation is subject to an adequacy decision by the European Commission; for transfers to the United States, the platform sub-processor Microsoft Corporation is certified under the EU-U.S. Data Privacy Framework (and the UK Extension and Swiss-U.S. DPF), which the European Commission recognises as providing an adequate level of protection; or
- adequate level of protection, which can be verified at https://dataprivacyframework.gov/
- the Standard Contractual Clauses (SCC's) apply as incorporated in the Microsoft Products and Services Data Protection Addendum (Microsoft DPA);

9 Data processor uses the following sub-processors:

SUB-PROCESSOR	PURPOSE	LOCATION
Microsoft	Platform hosting & operation (Azure, M365)	EU / US / AU per client region
Atlassian (JIRA)	Support	EU
Exact Online	Billing & Administration	EU

For EU-region clients all processing remains within the EU/EEA; for non-EU regions, safeguards apply as described in point 8. Data processor will inform the client through its ROGER365 partner of any addition or replacement of a sub-processor, allowing a reasonable period to object on data protection grounds in accordance with Part 2 (Article 8).

10 **Data processor shall support their clients in the following way when they receive requests from data subjects:** The client can, through the ROGER365 administration portal, view the personal data within its own tenant and configure and manage its own data, including configuration, schedule times, callflows, agent settings and the data retention period, and can export data through the platform API. This enables the client to respond to access and data portability requests, and to correct administrative and configuration data, itself.

For recorded data such as call detail records and the content of customer communications, the following applies. The client cannot delete individual call detail records before the configured retention period has been reached; such data is automatically removed once that threshold is met. The client cannot delete the database as a whole. Where erasure or rectification of this recorded data is required, the client can request it through its ROGER365 partner or by contacting Data Processor at dataprotection@roger365.com, and Data Processor will provide reasonable assistance within the applicable statutory time limits. As this data constitutes a factual record, rectification is given effect by deleting the inaccurate data rather than by altering the recorded content.

On termination of the subscription, the client can request deletion of its data; Data Processor carries such deletion out within four weeks (see point 12). Data processor does not respond to data subjects directly but refers them to the client as controller of personal data.

11 **Data processor shall support their clients with Data Protection Impact Assessments (DPIA) in the following manner:** Data processor will, cooperate with a Data Protection Impact Assessment (DPIA) in accordance with Part 2 (Article 7). Data processor may charge reasonable costs for such assistance.

12 Once the Agreement with a client has been terminated, Data Processor shall delete personal data they process on behalf of client within four weeks, in such a manner that the data can no longer be used and shall be rendered inaccessible.

Each client's personal data is stored in a dedicated Azure SQL database within data processor's Azure subscription. On termination, the customer environment and the customer-specific database are removed by means of approved deletion scripts, rendering the data inaccessible. Because the backups of an Azure SQL database are bound to that database, deleting the database also removes its associated backups; once the database service is deleted, no backup of it can be restored. No separate backup of the client's data is retained after deletion, save where a statutory retention obligation applies to data processor.

13 **Returning of personal data once the Agreement has been terminated.** The client can, prior to termination of the Agreement, export its data itself through the ROGER365 administration portal in a machine-readable format. No separate arrangements for the return of personal data by Data Processor after termination are in place; after termination the data is deleted in accordance with point 12.

Security policy

Data processor has implemented the following security measures to protect their product or service: The platform is operated entirely on Microsoft Azure PaaS under the Microsoft shared responsibility model. Data processor maintains an Information Security Management System (ISMS) based on ISO/IEC 27001:2022; the full security policy is documented in that ISMS, of which the measures below are a summary. Key measures include: encryption of all data in transit (TLS 1.2+) and at rest (AES-256), with keys managed in Azure Key Vault; identity and access management via Microsoft Entra ID with mandatory multi-factor authentication, Conditional Access and least-privilege, need-to-know role design; logical isolation of tenant data and full separation of development, test, acceptance and production environments across separate Azure tenants; corporate endpoints managed via Microsoft Intune with BitLocker full-disk encryption and Microsoft Defender; centralised security logging (Entra sign-in and audit logs retained 90 days) with monitoring via Azure Monitor and Log Analytics; vulnerability management through automated scanning (OWASP, dependency and quarterly NMAP scans) with remediation tracked in Azure DevOps; a secure software development lifecycle with mandatory peer review and four-eyes release approval; annual independent penetration testing and external ISO 27001 audits; and continuous security awareness training (including phishing simulations).

The following points apply on a comply-or-explain basis:

Pseudonymisation: tenant databases hold only limited agent identifiers (such as the Microsoft Entra ID Object ID) and the data the client chooses to provide; no special categories of personal data are stored by design. No production data is used in non-production environments, which rely on synthetic data sets only.

Encryption: personal data is stored encrypted at rest using AES-256 and transmitted only over encrypted connections (TLS 1.2+). Backups are likewise encrypted at rest.

Confidentiality, integrity, availability and resilience are ensured through least-privilege access controls, MFA and Conditional Access, logical tenant isolation, encryption, comprehensive logging and monitoring, and a serverless, multi-region Azure PaaS architecture with priority-based failover between paired regions.

In the event of an incident, availability of and access to personal data is restored through automated Azure SQL backups (point-in-time and long-term retention), geo-redundant replication to a paired Azure region, multi-region failover, and a documented incident response and business continuity plan that is tested annually through tabletop exercises.

Data processor conforms to the principles of the following Information Security Management System (ISMS): ISO 27001 (ISO/IEC 27001:2022).

Data processor has obtained the following labels and certificates:

ISO 27001 (ISO/IEC 27001:2022) Microsoft 365 App Certification NIS2 SC30 Quality Mark

Data breach protocol

In the event something does go wrong, Data Processor shall follow the following data breach protocol to ensure that clients are notified of incidents: Data processor operates an Information Security Incident Response Plan as part of its ISMS. Security events are detected through continuous monitoring and internal reporting, and are classified by severity from low (0) to major (3), with escalation timelines ranging from one hour to five days depending on impact. If Data Processor becomes aware of a personal data breach within the meaning of Article 4(12) GDPR affecting client data, it notifies the affected client in accordance with Part 2 (Article 4) without undue delay.

Notification is made through the client's established partner channel and, where applicable, via the ROGER365 status page or the relevant partner Teams channel. The notification includes all information reasonably known to data processor at the time of notification to the client, which, to the extent available, comprises: a description of the nature of the incident; the categories and approximate number of data subjects and records concerned; the likely consequences; and the measures taken or proposed to address the breach and mitigate its effects. Assessment of whether the breach must be reported to the Dutch Data Protection Authority and/or to data subjects remains the responsibility of the controller (the client or its customer); Data Processor does not make such notifications itself but supports the controller on request. The data breach protocol is described in more detail in data processor's ISMS.

PART 2 · VERSION MARCH 2025

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:

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

GDPR
The General Data Protection Regulation.

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

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

Data Subject
A natural person who can be identified, directly or indirectly.

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

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

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

Data Processing Agreement

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

Article 2 · General provisions

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

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

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

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

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

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

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

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

Article 3 · Security

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

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

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

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

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

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

Article 4 · Data breaches

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

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

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

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

Article 5 · Confidentiality

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

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

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that their employees comply with the requirements described in this article.

Article 6 · Term and termination

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

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

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data they currently store and which they have obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been rendered inaccessible. Client can, prior to the expiry of the aforementioned timeframe, export its data itself in a machine-readable format.

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

Article 7 · Rights of Data Subjects, DPIAs and auditing rights

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

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so, by making available the relevant information about the platform's security measures and processing characteristics that is necessary for the assessment or consultation. Data processor may charge reasonable costs for such assistance.

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

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

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

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

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

Article 8 · Sub-processors

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

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

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

Article 9 · Other provisions

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