ROL Intelligent Office™

DATA, SECURITY & PRIVACY POLICIES (EU)

JANUARY 01, 2023

Acknowledged by:

..... Authorized Signatory/Authorized Representative

..... (Full name)

..... (Title)

..... (Date)

Doc: ROLiO/SDP/1222
v 0.8

1. ROL INTELLIGENT OFFICE SECURITY ARCHITECTURE

1.1 The ROL Intelligent Office service is a multiplatform client/server setup consisting of multiple data and user applications and clients for the web, smart phones, and embedded devices. Software and hardware combined form the complete offering that is ROL Intelligent Office.

1.2 The ROL Intelligent Office Core service is hosted as a scalable cloud application on Google Cloud and Microsoft Azure, using databases and cache solutions provided by Google and Microsoft. The application and data is stored securely and encrypted. Access to the cloud is handled exclusively by a dedicated ISO27001 certified operations team. Updates and fixes and handled in a secure hand over, and at no point does any uncertified personnel have access to any of the data or storage.

1.3 All communication from and to the ROL Intelligent Office Core service is handled through both a REST and WebSocket API, using HTTPS (SSL/TLS 1.3) with latest security patches applied. The server is also backwards compatible with older TLS standards through a proxy to support older hardware and software like Internet Explorer 7 and Android 4.0, handling all attempted attacks in an environment separated from the core application. Certificates are provided by DigiCert and encrypted with SHA256 with RSA (2048 bits).

1.4 Applications are authenticated using an array of alternatives with everything from traditional form authentication to OAuth 2.0, OpenID and SAML. ROL Intelligent Office is interoperable with the latest standards from Microsoft, Google, and other third party authentication providers, and enforces the existing password strength and restrictions used by the selected authentication provider. The user data is stored encrypted and secure in the Google Cloud and only available through authenticated user requests. Users are divided into secure realms and hierarchies to separate the data and prevent data leakage or rights elevation problems.

1.5 ROL Intelligent Office syncs calendar data from Office365 using the Microsoft Graph API. The sync service uses SHA 256 with RSA 2048 bits encryption and the latest SSL/TLS 1.3. All calendar and user data in the ROL Intelligent Office cloud is hosted in datacenters compliant with the latest ISO27001 and SoC 1/2/3 standards.

1.6 The virtual servers hosting ROL Intelligent Office is mainly resided in western Europe. Since Google uses distributed servers, data is sometimes tunnelled through different countries to ensure maximum uptime and availability. All ROL Intelligent Office services follow the European GDPR standard. User data can be removed on demand by the appointed company admin or by the ROL Intelligent Office team through the compliance of the DPA

1.7 Employees working with ROL Intelligent Office are governed by a strict documented IT security policy covering secure software development and handling of system data and encryption. For more information, about the handling of private data and the ROL privacy policy, visit https://www.rolgroup.com/gdpr/.

2. DATA SERVICES

2.1 ROL will provide the Data Service in accordance with the Site Services Proposal, as elected by the Client.

2.2 The ROL Software will generate certain base data during the performance of the Services (such base data being the "**Client Data**"). The Client will own the Client Data and ROL may process Client Data on behalf of the Client for the purpose of providing the Services and in accordance with each Site Services Proposal.

2.3 ROL will process the Client Data and compute from it certain extracted and pseudonymised data (such extracted data being the "**Derived Data**"). ROL shall, if requested, provide analytic reporting generated from the Derived Data to the Client (the final reports generated by ROL being the "**Data Reports**"). The Parties shall discuss and agree the format, content and frequency of any reporting of the Derived Data. ROL shall use the Derived Data solely for the provision of Services to Client and not in any way for itself other than as permitted under Clause 2.4.

2.4 Derived Data may be aggregated to provide analytics (the output of this aggregation and pseudonymisation process being the "**Aggregated Data**"). The Aggregated Data shall not contain any Confidential Information nor personal data and shall not in any way be traceable to the Client.

2.5 ROL will own all Intellectual Property Rights in the Aggregated Data, and any Intellectual Property Rights in and to the Aggregated Data and any structuring of such Aggregated Data will vest automatically with ROL upon creation. To the extent that the Client selects to receive the Data Service in respect of such Aggregated Data, ROL hereby grants a non-transferable licence of the Aggregated Data for the duration of this Agreement to the Client, solely for the purpose of receiving such Data Service (other than in accordance with the "The Client shall be entitled to transfer or sub-license the rights granted to it…" within the "Intullectual Property" clause in the "*General Client Agreement*").

2.6 ROL may use the Aggregated Data for its own internal and external business purposes, including without limitation to produce aggregated datasets and reporting across multiple customers of ROL.

2.7 ROL may also gather anonymized usage analytics relating to users' experience of the ROL Intelligent Office Platform and may use these usage analytics for the purposes of service improvement and for its internal and external business purposes.

3. DATA PROTECTION

3.1 For the purposes of this Clause 3 and Clause 4 (Processing, Personal Data, and Data Subjects), the terms "**controller**", "**processor**", "**data subject**", "**personal data**", "**personal data breach**" and "**processing**" shall have the meaning given to them in the EU GDPR.

3.2 Each Party will comply with all Applicable Data Protection Laws to the extent applicable to them. ROL shall be responsible for ensuring that it complies with Applicable Data Protection Laws in its performance of the Services in accordance with this Agreement. The Client shall be responsible for ensuring that it complies with Applicable Data Protection Laws in its use of the Services in accordance with this Agreement.

3.3 Subject to Clause 3.4, ROL shall process personal data in connection with the Services as a processor on behalf of the Client (the controller), and the Parties' responsibilities are set out in Clause 4 titled "Processing, Personal Data and Data Subjects" of this Policy. Clause 8 titled "Data Processing Instructions" of this Policy, sets out the scope, nature and purpose of processing, the duration of the processing and the types of personal data and categories of data subject.

3.4 With respect to the converting by ROL of Derived Data to Aggregated Data including geolocation data collected by ROL via sensors in provision of the services, the Parties acknowledge that in limited circumstances, it may be technically possible to deduce from such data the identity of named individuals and that such data should therefore be treated as personal data. With respect to such processing:

(a) ROL will be a controller insofar as such data constitutes personal data;

(b) ROL will not take steps to deliberately identify individuals from such data;

(c) ROL will process the personal data as an independent controller in accordance with the Applicable Data Protection Laws; and

3.5 Client shall inform relevant data subjects about the activities undertaken by ROL in delivering the Services by providing the User Rules that contain a link to the ROL Privacy Notice. The Client shall indemnify ROL and ROL shall indemnify Client against all liabilities, costs, expenses, damages and losses (including any direct losses, all interest, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by ROL or Client arising out of or in connection with the Client's or ROL's breach of this Clause 3 and/or the Applicable Data Protection Laws to which the Client and ROL are subject.

4. PROCESSING, PERSONAL DATA AND DATA SUBJECTS

4.1 For the purposes of this Clause 4, Client is referred to as "**Controller**" and ROL is referred to as "**Processor**".

4.2 In the performance of the Agreement the Processor will process personal data on behalf of the Controller and the parties have entered the following Data Processing Agreement ("**DPA**"), which is incorporated into and forms part of the Agreement.

4.3 This DPA specifies the terms and conditions applicable to the processing of personal data performed by the Processor under the Agreement. The DPA applies to all processing activities by the Processor on behalf of Controller.

4.4 Roles under GDPR and Communication;

(a) To the extent the Controller has invited other Affiliates to use the Services provided by the Processor in accordance with the Agreement, the Controller is responsible for obtaining instructions from the Affiliates for the Processor's processing of personal data under this DPA.

(b) The Processor is only obliged to communicate with the Controller regardless of the number of affiliates that are invited to use the Services under the Agreement. Any notification or communication under this DPA shall be made by using contact details specified in the Agreement.

5. CONTROLLER'S CERTAIN OBLIGATIONS

5.1 Controller undertakes to:

(c) Ensure that there is a legal basis for the processing of personal data and keep a record of this.

(d) Notify the Processor of incorrect, corrected, updated, or deleted personal data which is subject to Processor's processing.

(e) Document and, upon Processor's, request, inform about the categories of registered persons and categories of personal data that will be processed.

(f) Provide, if necessary, documented instructions to the Processor regarding the Processor's processing of personal data.

(g) Ensure that all instructions to the Processor are in accordance with Applicable Data Protection Laws and do not result in the Processor breaching Applicable Data Protection Laws or its obligations under this DPA.

(h) Comply with Applicable Data Protection Laws.

6. PROCESSOR'S CERTAIN OBLIGATIONS

6.1 Processor undertakes to:

(a) Process the personal data only in accordance with Applicable Data Protection Laws, this DPA and communicated and documented instructions from the Controller unless required to do so by Union or Member State law to which the processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information. Initial instructions are set out in Clause 8 of this Policy titled "Data Processing Instructions" . The Controller confirms that any written instructions included in this DPA or separately communicated in accordance with this DPA constitutes complete and full instructions to the Processor.

(b) Ensure that persons authorized to process the personal data have received training and instructions regarding the processing of personal data and have undertaken to observe confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) Take all measures required pursuant to Article 32 of the GDPR, to protect personal data as described in Clause 1 of this Policy titled "ROL Intelligent Office Security Architecture".

(d) Considering the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights.

(e) Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Processor.

(f) Provide Controller with all information required to demonstrate that the obligations set forth in this DPA have been fulfilled and enable and contribute to audits, including inspections carried out by the Controller, or by another third party authorized by the Controller. Such third party shall be bound by a confidentiality obligation and not be a competitor of the Processor. Such inspection shall not include any access to other customers' data. The Controller shall notify the Processor at least forty-eight (48) hours prior to such audit in order to provide the Processor with a reasonable amount of time to compile information. An inspection will take place during normal working hours. The costs of the audit shall be borne by the Controller, unless the audit determines that the Processor has breached any of its obligations under this Agreement or Applicable Data Protection Laws.

(g) Inform the Controller if it becomes aware that the DPA or the documented instructions conflict with Applicable Data Protection Laws, or any change in legislation applicable to the Processor or the Controller is likely to have a substantial adverse effect on the obligations in this DPA;

(h) Inform the Controller without undue delay if it becomes aware of a personal data breach (as in the meaning of Art. 33-34 GDPR) concerning personal data processed on behalf of the Controller. The notification shall contain, to the best of Processor's knowledge, information about the nature of the breach, the categories and number of data subjects and personal data items affected, the likely consequences of the incident, and a description of the measures Processor has taken (if any) to limit any negative effects of the personal data breach. The Processor will provide information as it becomes available, and it is acknowledged that not all information may be immediately available to the Processor. The Processor will follow up with further information without undue delay.

6.2 The Processor may only process personal data for the Purpose and to the extent necessary to fulfil Processor's obligations under this DPA and the Agreement.

6.3 The Processor shall at the choice of the Controller, delete or return all the personal data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Applicable Data Protection Laws require storage of the personal data. For the avoidance of doubt this shall not apply to any Aggregated Data.

6.4 The Processor is entitled to reasonable compensation for direct costs when assisting the Controller with obligations set out in Claus 6.1(d), 6.1(e) and 6.1(f).

7. SUB PROCESSORS

7.1 The Processor has the right to engage subcontractors as sub processors in order to provide the Services. Customer approves sub processors set out in Clause 8 of this Policy titled “Data Processing Instructions”.

7.2 The Processor shall ensure that each sub processor is bound by an agreement with substantially the same requirements regarding data protection as set out under this DPA.

7.3 The Processor shall be responsible for all actions or omissions by a subcontractor under this DPA, as though they were the Processor’s own actions or omissions.

7.4 If the Processor wishes to retain a new sub processor or replace an existing sub processor, the Controller shall be informed thereof, according to the contact information stated in the Agreement. The information shall be provided not less than one (1) month before the change is made. If the Controller does not object in accordance with this Clause 7.4 within thirty (30) days after the Processor's notification, or has not presented any legitimate reason, the change to the list of sub processor(s) shall be deemed accepted. If the change is not approved by the Controller (acting reasonably), but the Processor still chooses to retain/replace the sub processor, then the Controller has the right to terminate the Agreement and accordingly this DPA with immediate effect or, if the Controller so wishes, state a discretionary termination period of up to two (2) months, without the Processor having any liability to the Controller. The Controller shall notify its decision regarding termination of the Agreement and the chosen termination period within two (2) weeks after the Processor has given notice that it will retain/replace a sub processor despite the absence of approval by the Controller.

7.5 In case personal data is transferred to a sub processor located outside the EEA in a country that is not recognized as providing an adequate level of data protection the Processor shall ensure that appropriate safeguards are in place. Such safeguards may include, but is not limited to, data processing agreements based on EU Model Clauses (whereas Controller authorizes Processor to enter into such agreements containing EU Model Clauses on behalf of the Controller). Where agreements based on the EU Model Clauses are to be implemented, the relevant parties will execute the modules of the EU Model Clauses that are relevant to the proposed transfer. In the event that the EU Model Clauses are amended, replaced or repealed by the European Commission or under Applicable Data Protection Laws, the Parties shall, so far as relevant, work together in good faith to enter into any updated version of the EU Model Clauses or negotiate in good faith a solution to enable a transfer of personal data to be conducted in compliance with Applicable Data Protection Laws. Transfers to sub processors located outside the EEA are listed in Clause 8 the “Sub Processors” section of this document.

8. DATA PROCESSING INSTRUCTIONS

8.1 Purposes of the processing

(a) The purpose of processing personal data is to provide the Services in accordance with the Agreement and to comply with additional instructions given by the Controller to the Processor ("**Purpose**").

8.2 Processing of personal data may include:

(a) Collection, storage, calculation, organization, structuring, retrieval, anonymization or otherwise, to provide reports of compiled personal data;

(b) Derive pseudonymised data from Client Data sets (thereby becoming Derived Data), analysis of the Derived Data and providing reporting to the Controller on analytics information regarding the data subjects' use of the Controller's office space and other analytics in accordance with the Agreement and each Site Services Proposal; and

(c) Aggregate the Derived Data, thereby becoming Aggregated Data, which shall not include personal data

8.3 Sub processors

(a) Google LLC: Hosting servers, databases.

(b) Microsoft Corporation: Hosting active directory.

9. CATEGORIES OF DATA SUBJECTS

9.1 Personal data is processed for the following categories of data subjects:

(a) Employees of the Controller

(b) Other personnel hired or otherwise engaged by the Controller

(c) Other persons that are registered in the Services by the Controller.

9.2 Categories of personal data

(a) Name, email, phone number, company connection, precise and coarse location, language preferences, user ID, device ID (phones, computers), diagnostics and usage data (crashes, number of logins etc.)

(b) Utilization reports do not contain or include personal data.

(c) Anonymized reports do not contain any of the data specified above, except diagnostics and usage data (crashes, number of logins etc.).

9.3 Duration

(a) The personal data shall be processed for the duration for which the Services are provided under the General Client Agreement.

(b) Personal data is saved as long as the user is active in the system, and retained up to 30 days after deletion.

10. SERVER HOSTING AND DATA RESIDENCY

10.1 The virtual servers hosting ROL Intelligent Office resides in Western Europe and North America. As Google uses distributed servers, data may be tunneled through different countries to ensure maximum uptime and availability. All ROL Intelligent Office services follow the European GDPR standard. User data can be removed on demand by the appointed company admin or by the ROL Intelligent Office team in compliance with the data processing agreement.

10.2 Data is hosted in the following locations:

(a) Microsoft Azure

(1) Netherlands (no city specified by Microsoft)

(ii) Additional Information can be found at: https://azure.microsoft.com/en-us/global-infrastructure/data-residency/

(b) Google Cloud

(1) St. Ghislain, Belgium

(2) London, England

(3) Frankfurt, Germany

(4) Eemshaven, Netherlands

(5) Zurich, Switzerland