

DATA PROTECTION AGREEMENT (DPA)

This Data Processing Agreement ("DPA"), in accordance with Art. 28 (3) of the EU-GDPR, forms part and is an exhibit of the Master Services Agreement with Otinue ("Agreement"), to the extent applicable to Customer, under which the processing of personal data on behalf of the Customer as a data controller. This DPA will be effective as of the Effective Date of the Agreement. This DPA applies to Otinue's Processing of Customer Personal Data as a Processor in connection with the provision of the services under the Agreement ("Services"), provided that the Processing of such Customer Personal Data is subject to Data Protection Legislation. This DPA is intended to address requirements of Data Protection Legislation, including Article 28(3) of the GDPR and CCPA. This DPA shall be effective for the term of the Agreement or until deletion or return of Customer Personal Data as instructed by Customer under this DPA, whichever is earlier.

In this DPA, defined terms shall have the meaning set out in the Agreement unless otherwise defined. In this DPA, the following terms shall have the following meaning:

"**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Law;

"**Applicable Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and the UK Data Protection Act 2018 ("**UK DPA**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the CCPA, and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

"**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018.

This Addendum details the Parties' obligations in respect of the processing of Customer's personal data (the "**Data**") for the purpose of fulfilling obligations under the Agreement ("**Contract Processing**").

1. SCOPE, DURATION AND SPECIFICATION OF CONTRACT PROCESSING OF DATA

- a) The scope and duration and the detailed terms and conditions on the type and purpose of Contract Processing shall be governed by the relevant Order, if the provisions of this DPA do not result in additional obligations.
- b) The nature and purpose of the processing are specified in relevant Order. The categories of data subjects are persons who are in business or private contact with Customer and its employees via IT systems (Data traffic between the corporate network and the Internet). Mainly as follows:

- ☒ Employees
- ☒ Prospective Clients
- ☒ Suppliers
- ☒ Clients
- ☒ Other:

All persons who are in business or private contact with the company and its employees via IT systems (data traffic between the corporate network and the Internet).

- c) The categories of the data are as follows:

All data relating to data traffic between Customer network and the internet. This includes IP addresses, emails (sender / recipient, content, attachments), content from the Internet (URLs, website payloads, search queries), financial data, etc.

Special categories of personal data: Data on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric and health data, and data on sex life and sexual orientation, etc. can be accessed depending on whether the Customer holds them and whether they are affected within the scope of the Services.

2. SCOPE OF APPLICATION AND RESPONSIBILITIES

- a) Customer instructs Otinue to process Data on its behalf. In respect of such Contract Processing, Customer shall be the controller of the Data and Otinue shall be a processor. Such Contract Processing shall include all activities detailed in the respective Service Order. Within the scope of this DPA, Customer shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Otinue and the lawfulness of having Otinue process Data on behalf of Customer. Customer shall be the «**controller**» in accordance with Art. 4 no. 7 GDPR.

- b) Customer's individual instructions on Contract Processing shall, initially, be as detailed in the respective Order. Customer shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modify, amend or replace such individual instructions by issuing such instructions to the point of contact designated by Otinue. Instructions not foreseen in or covered by the respective Order shall be treated as requests for changes to the Order. Customer shall, without undue delay, confirm in writing or in text form any instruction issued orally.

3. OTINUE'S OBLIGATIONS

- a) Except where expressly permitted by Applicable Data Protection Law, Otinue shall, as a processor, process data subjects' Data only within the scope of the respective Order and the instructions issued by Customer. Where Otinue believes that an instruction would be in breach of applicable law, Otinue shall notify Customer of such belief without undue delay. Otinue shall be entitled to suspending performance on such instruction until Customer confirms or modifies such instruction.
- b) Otinue shall, within Otinue's scope of responsibility, organise Otinue's internal organization so it satisfies the specific requirements of data protection. Otinue shall implement technical and organizational measures to ensure the adequate protection of Customer's Data, which measures shall fulfil the requirements of Art. 32 GDPR or Art. 8 (rev)DSG (each as applicable). Otinue shall implement technical and organizational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services in accordance with the agreement. Customer is familiar with these technical and organizational measures in accordance with ISO 27001, and it shall be Customer's responsibility that such measures ensure a level of security appropriate to the risk. Otinue reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.
- c) Otinue shall support Customer, insofar as is agreed upon by the Parties, and where possible for Otinue, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Art. 33 to 36 GDPR or corresponding provisions of the Swiss Data Protection Act (each as applicable).
- d) Otinue warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.
- e) Otinue shall notify Customer, without undue delay, if Otinue becomes aware of breaches of the protection of Data within Otinue's scope of responsibility. Otinue shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Otinue shall coordinate such efforts with Customer without undue delay.
- f) Otinue warrants that Otinue fulfils, if applicable, its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- g) Subject to i) below; Otinue shall correct or erase Data if so instructed by Customer and where covered by the scope of the instructions permissible. Where an erasure, consistent with requirements under Applicable Data Protection Laws, or a corresponding restriction of processing is impossible, Otinue shall, based on Customer's instructions, and unless agreed upon differently in the Agreement destroy, in compliance with requirements under Applicable Data Protection Laws, all carrier media and other material or return the same to Customer. In specific cases designated by Customer, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.
- h) Subject to i) below; Otinue shall, upon termination of Contract Processing and upon Customer's instruction, and unless agreed upon differently in the Agreement, return all Data, carrier media and other materials to Customer or delete the same. Customer bears additional costs, that arise due to deviating instructions for the return or deletion of the Data.
- i) The requirement to delete Data shall not apply to the extent that Otinue is required by any applicable EU (or any EU Member State) or UK law to retain some or all of the Data, in which event Otinue shall isolate and protect the Data from any further processing except to the extent required by such law until deletion is possible.
- j) Where a data subject asserts any claims against Customer in accordance with Art. 82 GDPR or under the Applicable Data Protection Laws (each as applicable), Otinue shall support Customer in defending against such claims, where possible.
- k) Customer agrees that services of Otinue due to individual instructions according to Section 2 b), due to demands, requests and inquiries, in particular according to the above paragraphs c), g), h), and i), Section 4 b) as well as Section 5 and due to inspections of Customer, of data subjects and of data protection authorities are to be remunerated at the respective applicable standard rates of Otinue for Consulting Services (if the charges incurred are substantial, a prior approval of the costs by Customer is required).

4. CUSTOMER'S OBLIGATIONS

- a) Customer shall notify Otinue, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Customer in the results of Otinue's work.
- b) Where a data subject asserts any claims against Otinue in accordance with Art. 82 GDPR or other Applicable Data Protection Law, Customer shall support Otinue in defending against such claims, where possible.
- c) Customer shall notify to Otinue the point of contact for any issues related to data protection arising out of or in connection with the Agreement. If not designated, Otinue will use the point of contract identified in the Agreement, Quote or other record identifying a Customer point of contact.
- d) Data Protection Officer of Otinue is:

Dr. C. Schäfer, Active Assets A2 GmbH, Gottlieb Daimler Str. 5, D-78467 Constance
privacy@otinue.com

Otinie shall notify the Customer in text form of any changes to the DPO.

5. ENQUIRIES BY DATA SUBJECTS

Where a data subject asserts claims for rectification, erasure or access against Otinue, and where Otinue is able to correlate the data subject to Customer, based on the information provided by the data subject, Otinue shall refer such data subject to Customer. Otinue shall forward the data subject's claim to Customer without undue delay. Otinue shall support Customer, where possible, and based upon Customer's instruction insofar as agreed upon. Otinue shall not be liable in cases where Customer fails to respond to the data subject's request in total, correctly, or in a timely manner.

6. OPTIONS FOR DOCUMENTATION

- a) Otinue shall document to Customer Otinue's compliance with the obligations agreed upon in this DPA by appropriate measures. Evidence of the implementation of such measures, which not only relate to the specific service, can be provided by submitting a current certification report, reports or report extracts from independent bodies (e.g. financial auditors, internal auditors, data protection officer, IT security department, data protection auditors, quality auditors) or a suitable certification by audits on information security or data protection.
- b) Where, in individual cases, audits and inspections by Customer or an auditor appointed by Customer are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Otinue's operations, upon prior written notice and observing an appropriate notice period. Customer shall ensure all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organizational measures and safeguards implemented. Otinue shall be entitled to reasonably reject auditors which are competitors of Otinue.
- c) Otinue shall be entitled to request remuneration for Otinue's support in conducting inspections. Otinue's time and effort for such inspections shall be limited to one day per calendar year, unless agreed upon otherwise.
- d) Where a data protection supervisory authority or another supervisory authority with statutory competence for Customer conducts an inspection to the extent that such audits and inspections are permitted under the applicable law, section (b) above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

7. SUBPROCESSORS

- a) Otinue may use subprocessors in accordance with the following provisions, provided that Otinue obligates them in accordance with the requirements of Article 28 (3) of the GDPR or Article 9 (rev)DSG or equivalent requirements under Applicable Data Protection Laws (each as applicable). The relevant data processing agreements may deviate from this Agreement, in particular in the case of providers of standard services; in this case, only the agreements concluded with such subprocessors shall apply, for example with regard to the audit rights.
- b) Customer hereby grants its general consent to the involvement of subprocessors which (i) are listed on Otinue's website (posted at <https://www.otinue.com/subprocessors-and-affiliated-operational-entities/>) with the tasks relating to them (and with links to their subprocessors, if applicable), and which (ii) are each affiliate of Otinue. These subprocessors may be located outside of Switzerland, the UK and the EU. Otinue shall ensure that any transfers of Data to subprocessors located outside the UK, EU and/or Switzerland is made in accordance with requirements under Applicable Data Protection Laws and to the extent such transfer is a Restricted Transfer it shall be made pursuant to Standard Contractual Clauses entered into between the relevant exporter and importer of the Data.
- c) The Customer further gives its consent to the involvement of further subprocessors, provided that the following procedure is complied with: At least 20 days prior to the engagement of a new subprocessor by Otinue, the aforementioned list of subprocessors will be updated and Otinue will provide the Customer with a mechanism to obtain notice of such updates. Customer shall be entitled to object in writing to any new subprocessor within 10 days on substantial data protection grounds. If Customer does not object to such new subprocessor within such period, Customer shall be deemed to have given its written consent to such subprocessor. If there is a substantial reason under data protection law for such objection and no amicable agreement is reached between the Parties, Otinue may use such subprocessor, but the Customer shall be entitled to terminate the affected Service(s) extraordinarily and without termination fee.

8. OBLIGATIONS TO INFORM, MANDATORY WRITTEN FORM

- a) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Otinue's control, Otinue shall notify Customer of such action without undue delay to the extent Otinue is permitted to do so. Otinue shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Customer's sole property and area of responsibility, that data is at Customer's sole disposition, and that Customer is the controller in the sense of the GDPR. To the extent legally permissible, and in the absence of other written instructions, Otinue shall, at the expense and risk of the Customer, attempt to prevent access by governmental authorities or other third parties by legal means.
- b) In case of any conflict, the provisions of this DPA shall take precedence over the any provisions of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this appendix shall not be affected.

Ontinue (as «**Processor**») undertakes to comply of technical and organizational measures («**TOMs**») according to the respective national legal requirements according to:

- EU- GDPR Art 32 –Security of processing personal data,
- Swiss data protection Act, Art 7 (2) – Data protection through technology and data protection-friendly default settings, and Art. 8,
- Canada PIPEDA, Schedule 4.7 – Safeguards,
- USA, California, CCPA, Cal. Civ. Code §1798.150(a)(1),
- and all further national laws as applicable.

In addition to the legal requirements, Ontinue undertakes to maintain an information security management system (ISMS) in accordance with ISO 27001. The design and implementation of the TOMs for the appropriate protection of personal data takes place within the framework of this ISMS. They are listed in extracts below.

The TOMs are monitored annually by an independent, accredited audit company as part of the certification of Ontinue for ISO 27001 information security. The certificate is enclosed with the TOMs.

The TOMs are taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as The TOMs are updated by Ontinue if necessary.

1. POLICY INFORMATION SECURITY AND OTHER POLICIES

Top management has established an information security policy and a derived set of further policies for information security. The policies contain the objectives and principles to guide all activities relating to the confidentiality, availability and integrity of information.

The policies for information security are reviewed at least annually or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

2. ORGANIZATION OF INFORMATION SECURITY

Responsibilities and authorities for roles relevant to information security are assigned and communicated.

Ontinue has introduced the following roles, among others:

- a CISO
- a person responsible for the ISMS
- a legal department
- a Data Protection Officer

3. INFORMATION SECURITY ASSESSMENT AND TREATMENT

Information security risks are analyzed and assessed according to a defined process. The risk assessment is performed at least once a year or when significant changes are proposed or occur. Based on this, a information security risks treatment plan is drawn up and implemented.

4. HUMAN RESOURCE SECURITY

Prior to employment background verification checks are carried out on candidates for employment. All employees sign a supplemental agreement to their work contract to comply with confidentiality and data protection. This agreement remains valid after termination of employment.

During employment, employees receive regular training and further education on information security and data protection.

5. INTERNAL AUDITS

In addition to the audits of the certification company, a program for internal audits is established, planned and maintained. Thereafter, internal audits are carried out at least once a year according to the criteria and scope defined in the program. The results of the audit are reported to the relevant management.

6. ACCESS CONTROL

A formal process for registering and deregistering users is implemented to allow assignment of access rights. The assignment and use of privileged access rights is restricted and controlled.

Access to networks, applications, and information is restricted and controlled through a secure login process.

User access rights are reviewed at regular intervals.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

The physical security for offices, rooms and facilities is secured by physical access controls (e.g. iris scan, keys, etc.) and is partly monitored by video. Some of the offices and rooms are additionally protected by a security service.

Separate secure areas are only accessible with explicit access authorization.

8. PROTECTION FROM MALWARE

Detection, prevention and recovery controls to protect against malware are implemented, combined with appropriate user awareness.

9. BACKUP

Backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy.

10. LOGGING AND MONITORING

Event logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed. System administrator and system operator activities are logged and the logs protected and regularly reviewed.

11. SUPPLIER RELATIONSHIPS

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

The supplier service delivery is monitored and regularly reviewed.

12. MANAGEMENT OF INFORMATION SECURITY INCIDENTS

Responsibilities and procedures are established and are applied to ensure a quick, effective and orderly response to information security incidents.

13. BUSINESS CONTINUITY MANAGEMENT

Processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented and tested at regular intervals.

Status: 1st of february 2024 (the processor can adjust this schedule as required)



Building
trust
together.

Certificate

SQS has issued an IQNET recognized certificate that the organization:

Ontinue AG
Räffelstrasse 29
8045 Zürich Switzerland

has implemented and maintains a
Information Security Management System

for the following scope:

**Managed Detection and Response (MDR) and professional advisory support services,
which provide a platform basis for information and cyber security protections, executed
according to agreement with the customer**

which fulfils the requirements of the following standard:

ISO/IEC 27001:2022

Issued on: **05.01.2024**

Expires on: **24.04.2027**

Registration Number: **CH-H47611**

Alex Stoichitoiu
President of IQNET

F. Müller
CEO SQS



This attestation is directly linked to the IQNET Member's original certificate and shall not be used as a stand-alone document

IQNET Members*:

AENOR Spain **AFNOR Certification** France **APCER** Portugal **CCC** Cyprus **CISQ** Italy **CQC** China **CQM** China **CQS** Czech Republic
Cro Cert Croatia **DQS Holding GmbH** Germany **EAGLE Certification Group** USA **FCAV** Brazil **FONDONORMA** Venezuela **ICONTEC**
Colombia **ICS** Bosnia and Herzegovina **INTECO** Costa Rica **IRAM** Argentina **JQA** Japan **KFQ** Korea **LSQA** Uruguay **MIRTEC** Greece
MSZT Hungary **Nemko AS** Norway **NSAI** Ireland **NYCE** México **PCBC** Poland **Quality Austria** Austria **SII** Israel **SIQ** Slovenia **SIRIM**
QAS International Malaysia **SQS** Switzerland **SRAC** Romania **TSE** Turkey **YUQS** Serbia

* The list of IQNET Members is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com



Certificate

The SQS herewith attests that the organisation named below has a management system that meets the requirements of the normative basis mentioned.



Ontinue AG
Räffelstrasse 29
8045 Zürich
Switzerland

Further sites according to appendix

Scope

Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer

Normative basis

ISO/IEC 27017:2015

Extension to ISO/IEC 27001 certificate: Reg. No. H47611
Code of practice for information security controls for cloud computing services

Statement of applicability / Version 1.0

Reg. no. H47613
 Page 1 of 2

Validity 05.01.2024–04.01.2027
 Issue 05.01.2024

6261_2/November2022_Version 3.1



A. Grisard
 A. Grisard, President SQS

F. Müller
 F. Müller, CEO SQS

Swiss Association for Quality and Management Systems (SQS)
 Bernstrasse 103, 3052 Zollikofen, Switzerland





Appendix

Appendix of main certificate H47613



Ontinue AG
Räffelstrasse 29
8045 Zürich
Switzerland

Central Function	Scope	Norm / Revision	Reg. no.	Validity
Ontinue AG Räffelstrasse 29 8045 Zürich Switzerland	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27017:2015	H47613	05.01.2024 04.01.2027
Locations	Scope	Norm / Revision	Reg. no.	Validity
Ontinue Inc. 450 Maple Street Redwood City, CA 94063 United States of America	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27017:2015	H47613	05.01.2024 04.01.2027
Ontinue Canada Inc. 6060-3080 Yonge Street Toronto ON M4N 3N1 Canada	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27017:2015	H47613	05.01.2024 04.01.2027
Ontinue UK Ltd. Westgate House, 9 Holborn London, EC1N 2LL United Kingdom	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27017:2015	H47613	05.01.2024 04.01.2027
Cybersecurity Ontinue GmbH Speditionstrasse 21 40221 Düsseldorf Germany	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27017:2015	H47613	05.01.2024 04.01.2027
Ontinue Austria GmbH Mariahilfer Strasse 36/6 1070 Wien Austria	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27017:2015	H47613	05.01.2024 04.01.2027
Ontinue Private India Ltd. APAC Office 7th Floor Plot A/8A Knowledge Boulevard Block A, Industrial Area, Sector 62 Noida 201309 India	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27017:2015	H47613	05.01.2024 04.01.2027

Reg. no. H47613
Page 2 of 2

Validity 05.01.2024–04.01.2027
Issue 05.01.2024

6261_2/November2022_Version 3.1



A. Grisard
A. Grisard, President SQS

F. Müller
F. Müller, CEO SQS

Swiss Association for Quality and Management Systems (SQS)
Bernstrasse 103, 3052 Zollikofen, Switzerland



Member of





Certificate

The SQS herewith attests that the organisation named below has a management system that meets the requirements of the normative basis mentioned.



Ontinue AG
Räffelstrasse 29
8045 Zürich
Switzerland

Further sites according to appendix

Scope

Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer

Normative basis

ISO/IEC 27018:2019

Extension to ISO/IEC 27001 certificate: Reg. No. H47611
Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
 Statement of applicability / Version 1.0

Reg. no. H47614
 Page 1 of 2

Validity 05.01.2024–04.01.2027
 Issue 05.01.2024

6271_2/November2022_Version 3.1



sqs.ch

A. Grisard
 A. Grisard, President SQS

F. Müller
 F. Müller, CEO SQS

Swiss Association for Quality and Management Systems (SQS)
 Bernstrasse 103, 3052 Zollikofen, Switzerland





Appendix

Appendix of main certificate H47614



Ontinue AG
Räffelstrasse 29
8045 Zürich
Switzerland

Central Function	Scope	Norm / Revision	Reg. no.	Validity
Ontinue AG Räffelstrasse 29 8045 Zürich Switzerland	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27018:2019	H47614	05.01.2024 04.01.2027
Locations	Scope	Norm / Revision	Reg. no.	Validity
Ontinue Inc. 450 Maple Street Redwood City, CA 94063 United States of America	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27018:2019	H47614	05.01.2024 04.01.2027
Ontinue Canada Inc. 6060-3080 Yonge Street Toronto ON M4N 3N1 Canada	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27018:2019	H47614	05.01.2024 04.01.2027
Ontinue UK Ltd. Westgate House, 9 Holborn London, EC1N 2LL United Kingdom	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27018:2019	H47614	05.01.2024 04.01.2027
Cybersecurity Ontinue GmbH Speditionstrasse 21 40221 Düsseldorf Germany	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27018:2019	H47614	05.01.2024 04.01.2027
Ontinue Austria GmbH Mariahilfer Strasse 36/6 1070 Wien Austria	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27018:2019	H47614	05.01.2024 04.01.2027
Ontinue Private India Ltd. APAC Office 7th Floor Plot A/8A Knowledge Boulevard Block A, Industrial Area, Sector 62 Noida 201309 India	Managed Detection and Response (MDR) and professional advisory support services, which provide a platform basis for information and cyber security protections, executed according to agreement with the customer	ISO/IEC 27018:2019	H47614	05.01.2024 04.01.2027

Reg. no. H47614
Page 2 of 2

Validity 05.01.2024 – 04.01.2027
Issue 05.01.2024

6271_2/November2022_Version 3.1



A. Grisard
A. Grisard, President SQS

F. Müller
F. Müller, CEO SQS

Swiss Association for Quality and Management Systems (SQS)
Bernstrasse 103, 3052 Zollikofen, Switzerland

