Enonic Cloud
Data Processing and Security Terms

Last modified: 17 December 2018

The customer agreeing to these terms ("Customer"), and Enonic AS or any other entity that directly or indirectly controls, is controlled by, or is under common control with Enonic AS (as applicable, "Enonic"), have entered into an agreement under which Enonic has agreed to provide Enonic Cloud (as described at https://enonic.com/cloud) and related technical support to Customer (as amended from time to time, the "Agreement").

These Data Processing and Security Terms, including their appendices (the "Terms") will be effective and replace any previously applicable data processing and security terms as from the Terms Effective Date (as defined below).

1. Introduction

These Terms reflect the parties' agreement with respect to the terms governing the processing and security of Customer Data under the Agreement.

2. Definitions

2.1 Capitalized terms used but not defined in these Terms have the meanings set out in the Agreement. In these Terms, unless stated otherwise:

- Additional Security Controls means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines, including the Admin Console and other features and/or functionality of the Services such as encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- Agreed Liability Cap means the maximum monetary or payment-based amount at which a party's liability is capped under the Agreement, either per annual period or event giving rise to liability, as applicable.
- Audited Services means the Services indicated as being in-scope for the relevant certification or report at https://enonic.com/cloud, as may be updated by Enonic from time to time, provided that the Service has been discontinued.
- Customer Data has the meaning given in the Agreement or, if no such meaning is given, means data provided by or on behalf of Customer or Customer End Users via the Services under the Account.
- Customer End Users has the meaning given in the Agreement or, if not such meaning is given, has the meaning given to "End Users" in the Agreement.
- Customer Personal Data means the personal data contained within the Customer Data.

- Data Incident means a breach of Enonic's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Enonic. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- EEA means the European Economic Area.
- European Data Protection Legislation means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).
- GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Enonic's Third Party Auditor means a Enonic-appointed, qualified and independent third party auditor, whose then-current identity Enonic will disclose to Customer.
- Enonic XP means Enonic's core software platform
- ISO Certification means an ISO 9001:2015 certification or a comparable certification for the Audited Services
- Notification Email Address means the email address(es) designated by Customer in the Admin Console, or in the Order Form or Ordering Document (as applicable), to receive certain notifications from Enonic.
- Security Documentation means all documents and information made available by Enonic under Section 7.5.1 (Reviews of Security Documentation).
- Security Measures has the meaning given in Section 7.1.1 (Enonic's Security Measures).
- OWASP Report means an executive summary of the extensive penetration and security test following the Open Web Application Security Project framework.
- SOC 2 Report means a confidential Service Organization Control (SOC) 2 report (or a comparable report) on Enonic's systems examining logical security controls, physical security controls, and system availability, as produced by Enonic's Third Party Auditor in relation to the Audited Services.
- SOC 3 Report means a Service Organization Control (SOC) 3 report (or a comparable report), as produced by Enonic's Third Party Auditor in relation to the Audited Services.
- Subprocessors means third parties authorized under these Terms to have logical access to and process Customer Data in order to provide parts of the Services and TSS.
- Term means the period from the Terms Effective Date until the end of Enonic's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Enonic may continue providing the Services for transitional purposes.
- Terms Effective Date means the date on which Customer accepted, or the parties otherwise agreed to, these Terms.
- TSS means the Technical Support Services provided by Enonic.

2.2 The terms “personal data”, “data subject”, “processing”, “controller”, “processor” and “supervisory authority” as used in these Terms have the meanings given in the GDPR.

3. Duration of these Terms

These Terms will take effect on the Terms Effective Date and, notwithstanding expiry of the Term, will remain in effect until, and automatically expire upon, deletion of all Customer Data by Enonic as described in these Terms.

4. Scope of Data Protection Legislation

The parties acknowledge and agree that the European Data Protection Legislation will apply to the processing of Customer Personal Data if, for example:

a. the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA; and/or
b. the Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behaviour in the EEA.

5. Processing of Data

5.1 Roles and Regulatory Compliance; Authorization.

5.1.1 Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

a. the subject matter and details of the processing are described in Appendix 1;
b. Enonic is a processor of that Customer Personal Data under the European Data Protection Legislation;
c. Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Legislation; and
d. each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.1.2 Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Enonic that Customer’s instructions and actions with respect to that Customer Personal Data, including its appointment of Enonic as another processor, have been authorized by the relevant controller.

5.2 Scope of Processing.

5.2.1 Customer's Instructions. By entering into these Terms, Customer instructs Enonic to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and TSS; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the Agreement, including these Terms; and (d) as further documented in any other written instructions given by Customer and acknowledged by Enonic as constituting instructions for purposes of these Terms.

5.2.2 Enonic's Compliance with Instructions. Enonic will comply with the instructions described in Section 5.2.1 (Customer's Instructions) unless EU or EU Member State law to which Enonic is subject requires other processing of Customer Personal Data by Enonic, in which case Enonic will inform Customer (unless that law prohibits Enonic from doing so on important grounds of public interest) via the Notification Email Address.

6. Data Deletion

6.1 Deletion by Customer. Enonic will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be fully accessed by Customer, this use will constitute an instruction to Enonic to delete the relevant Customer Data from Enonic's systems in accordance with applicable law. Enonic will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

6.2 Deletion on Termination. On expiry of the Term, Customer instructs Enonic to delete all Customer Data (including existing copies) from Enonic's systems in accordance with applicable law. Enonic will, after a recovery period of up to 30 days following such expiry, comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the Term expires, any Customer Data it wishes to retain afterwards.

7. Data Security

7.1 Enonic's Security Measures, Controls and Assistance.

7.1.1 Enonic's Security Measures. Enonic will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Enonic's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Enonic may

update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

7.1.2 Security Compliance by Enonic Staff. Enonic will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3 Additional Security Controls. In addition to the Security Measures, Enonic will make the Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4 Enonic's Security Assistance. Customer agrees that Enonic will (taking into account the nature of the processing of Customer Personal Data and the information available to Enonic) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Enonic's Security Measures);
b. making the Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);
c. complying with the terms of Section 7.2 (Data Incidents); and
d. providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the Agreement including these Terms.

7.2 Data Incidents

7.2.1 Incident Notification. If Enonic becomes aware of a Data Incident, Enonic will: (a) notify Customer of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Enonic recommends Customer take to address the Data Incident.

7.2.3 Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Enonic's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

7.2.4 No Assessment of Customer Data by Enonic. Enonic will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements.

Without prejudice to Enonic's obligations under this Section 7.2 (Data Incidents), Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

7.2.5 No Acknowledgement of Fault by Enonic. Enonic's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Enonic of any fault or liability with respect to the Data Incident.

7.3 Customer's Security Responsibilities and Assessment.

7.3.1 Customer's Security Responsibilities. Customer agrees that, without prejudice to Enonic's obligations under Section 7.1 (Enonic's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):

a. Customer is solely responsible for its use of the Services, including:
    i. making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;
    ii. securing the account authentication credentials, systems and devices Customer uses to access the Services;
    iii. backing up its Customer Data as appropriate; and
b. Enonic has no obligation to protect copies of Customer Data that Customer elects to store or transfer outside of Enonic's and its Subprocessors' systems (for example, offline or on-premises storage), or to protect Customer Data by implementing or maintaining Additional Security Controls except to the extent Customer has opted to use them.

7.3.2 Customer's Security Assessment.

a. Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and Enonic's commitments under this Section 7 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation.
b. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Enonic as set out in Section 7.1.1 (Enonic's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4 Security Certifications and Reports. Enonic will do the following to evaluate and help ensure the continued effectiveness of the Security Measures:

a. maintain the ISO Certification; and
b. update the OWASP reports by a third party security expert for every major release of Enonic XP and Enonic Cloud.

7.5 Reviews and Audits of Compliance

7.5.1 Reviews of Security Documentation. In addition to the information contained in the Agreement (including these Terms), Enonic will make available for review by Customer the following documents and information to demonstrate compliance by Enonic with its obligations under these Terms:

a. the certificates issued in relation to the ISO Certification;
b. the then-current OWASP Report for Enonic XP; and
c. the then-current OWASP Report for Enonic Cloud, following a request by Customer in accordance with Section 7.5.3(a).

7.5.2 Customer's Audit Rights.

a. If the European Data Protection Legislation applies to the processing of Customer Personal Data, Enonic will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Enonic's compliance with its obligations under these Terms in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Enonic will contribute to such audits as described in Section 7.4 (Security Certifications and Reports) and this Section 7.5 (Reviews and Audits of Compliance).
b. Customer may also conduct an audit to verify Enonic's compliance with its obligations under these Terms by reviewing the Security Documentation (which reflects the outcome of audits conducted by Enonic's Third Party Auditor).

7.5.3 Additional Business Terms for Reviews and Audits.

a. Customer must send any requests for reviews of the OWASP Report under Section 7.5.1(c) or audits under Section 7.5.2(a) to Enonic's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).
b. Following receipt by Enonic of a request under Section 7.5.3(a), Enonic and Customer will discuss and agree in advance on:
    - (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the OWASP Report under Section 7.5.1(b) or 7.5.1(c); and
    - (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a)
c. Enonic may charge a fee (based on Enonic's reasonable costs) for any review of the OWASP Report under Section 7.5.1(b) and/or audit under Section 7.5.2(a). Enonic will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.
d. Enonic may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) if the auditor is, in Enonic's reasonable opinion, not suitably qualified or independent, a competitor of Enonic, or otherwise manifestly unsuitable. Any such objection by Enonic will require Customer to appoint another auditor or conduct the audit itself.

8. Impact Assessments and Consultations

Customer agrees that Enonic will (taking into account the nature of the processing and the information available to Enonic) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

a. providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation); and
b. providing the information contained in the Agreement including these Terms.

9. Data Subject Rights; Data Export

9.1 Access; Rectification; Restricted Processing; Portability. During the Term, Enonic will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Enonic as described in Section 6.1 (Deletion by Customer), and to export Customer Data.

9.2 Data Subject Requests

9.2.1 Customer's Responsibility for Requests. During the Term, if Enonic receives any request from a data subject in relation to Customer Personal Data, Enonic will advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 Enonic's Data Subject Request Assistance. Customer agrees that Enonic will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

a. providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls); and
b. complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Customer's Responsibility for Requests).

10. Data Storage

10.1 Data Storage and Processing Facilities Customer may select where certain Customer Data will be stored (the "Data Location Selection"), and Enonic will store it there in accordance with the Service Specific Terms. If a Data Location Selection is not covered by the Service Specific Terms (or a Data Location Selection is not made by Customer in respect

of any Customer Data), Enonic may store and process the relevant Customer Data anywhere in the EEA where Enonic or its Subprocessors maintains facilities.

10.2 Data Center Information. Information about the locations of Enonic data centers is available at: https://enonic.com/cloud/third-party-suppliers (as may be updated by Enonic from time to time).

11. Subprocessors

11.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement as Subprocessors of: (a) those entities listed as of the Terms Effective Date at the URL specified in Section 11.2 (Information about Subprocessors); and (b) all other Enonic Affiliates from time to time. In addition, Customer generally authorizes the engagement as Subprocessors of any other third parties ("New Third Party Subprocessors").

11.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at: https://enonic.com/cloud/third-party-suppliers (as may be updated by Enonic from time to time in accordance with these Terms).

11.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Enonic will:

a. ensure via a written contract that:
    i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Terms); and
    ii. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in these Terms, are imposed on the Subprocessor; and
b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 Opportunity to Object to Subprocessor Changes.

a. When any New Third Party Subprocessor is engaged during the Term, Enonic will, at least 30 days before the New Third Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address.
b. Customer may object to any New Third Party Subprocessor by terminating the Agreement immediately upon written notice to Enonic, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 11.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any New Third Party Subprocessor.

12. Cloud Data Protection Team; Processing Records

12.1 Enonic's Cloud Data Protection Team. Enonic's Cloud Data Protection Team can be contacted at privacy@enonic.com (and/or via such other means as Enonic may provide from time to time).

12.2 Enonic's Processing Records. Customer acknowledges that Enonic is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Enonic is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to Enonic via the Admin Console or other means provided by Enonic, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.

13. Third Party Beneficiary

Notwithstanding anything to the contrary in the Agreement, where Enonic is not a party to the Agreement, Enonic will be a third party beneficiary of Section 7.5 (Reviews and Audits of Compliance) and Section 11.1 (Consent to Subprocessor Engagement) of these Terms.

14. Effect of These Terms

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between these Terms and the remaining terms of the Agreement, these Terms will govern.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter
Enonic's provision of the Services and TSS to Customer.

Duration of the Processing
The Term plus the period from the expiry of the Term until deletion of all Customer Data by Enonic in accordance with the Terms.

Nature and Purpose of the Processing
Enonic will process Customer Personal Data for the purposes of providing the Services and TSS to Customer in accordance with the Terms.

Categories of Data
Data relating to individuals provided to Enonic via the Services, by (or at the direction of) Customer or by Customer End Users.

Data Subjects
Data subjects include the individuals about whom data is provided to Enonic via the Services by (or at the direction of) Customer or by Customer End Users.

This document is based on the Google Cloud data processing terms, adapted to Enonic Cloud. Source: https://cloud.google.com/terms/data-processing-terms