Onomondo DPA v1.0.1

between

Customer

the Controller – hereinafter referred to as the Customer –

and

Onomondo ApS
H.C. Hansens Gade
2300 Copenhagen
Denmark

the Processor - hereinafter referred to as the **Supplier** -

February 24, 2025
Authored by Jacob Jagger, Head of Information Security
Reviewed by Asbjørn Reissmann, Sr. Legal Council

onomondo

Contents

SCOPE

This Data Processing Agreement ("DPA") and its Annexes is incorporated into, and forms part of, the Terms of Service between the Supplier and the Customer (the "Agreement"). This DPA reflects the parties' agreement with respect to (i) the Processing of Customer Personal Data by us as a Processor on your behalf, and (ii) the Processing of Controller Personal Data by each party as a Controller in connection with our network products and your use of the Supplier's application.

In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over other terms in the Agreement to the extent of such conflict or inconsistency.

The Processor-to-Controller terms apply solely to the extent that the Supplier is a Processor of Customer Personal Data in connection with the Subscription Services.

The Supplier occasionally updates these terms. If the Customer has an active subscription, the Customer shall be informed via email. These updates are conditional on the Customer having subscribed to email notifications via the link in our General Terms.

The term of this DPA will follow the term of the Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

1. DEFINITIONS

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

"Controller Personal Data" means Personal Data that each party Processes as a Controller in connection The Supplier's Network Services, and each party is considered a Controller under Data Protection Laws.

“Customer Personal Data” means Personal Data contained within Customer Data that the Supplier Processes as a Processor on behalf of the Customer.

“Customer Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data that is; transmitted, stored, or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Subscription Services. "Customer Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to the Processing of Personal Data under the Agreement, including without limitation European Data Protection Laws, the California Consumer Protection Act (“CCPA”), and other applicable U.S. federal and state privacy laws; in each case as amended, repealed, consolidated, or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

"Europe" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

“European Data” means Customer Personal Data that is subject to the protection of European Data Protection Laws.

"European Data Protection Laws" means data protection laws applicable in Europe, including: (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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); and (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR").

“Instructions” means the written, documented instructions issued by Customer to the Supplier, and directing the Supplier to perform a specific or general action with regard to Customer Personal Data (including, but not limited to, depersonalizing, blocking, deletion, and making available).

"Permitted Affiliates" means any of your Affiliates that (i) are permitted to use the Subscription Services pursuant to the Agreement, but have not signed their own separate agreement with us and are not a “Customer” as defined under the Agreement, (ii) qualify as a Controller of Customer Personal Data or Controller Personal Data, and (iii) are subject to European Data Protection Laws.

“Personal Data” means any information relating to an identified or identifiable individual where such information is protected similarly as personal data, personal information, or personally identifiable information under Data Protection Laws.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process,” “Processes,” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

"Restricted Transfer” means transfer of Personal Data originating from Europe to a country that does not provide an adequate level of protection within the meaning of applicable European Data Protection Laws.

“Standard Contractual Clauses” means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021 currently found at https://eur-lex.europa.eu/eli/dec_impl/2021/914, as may be amended, superseded, or replaced.

“Sub-Processor” means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the Processing of Customer Personal Data under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any employee or consultant of the Supplier.

2. CUSTOMER RESPONSIBILITIES

2.1 Compliance with Laws. Within the scope of the Agreement and your use of the services, you will be responsible for complying with all requirements that apply to you under Data Protection Laws with respect to your Processing of Personal Data.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Personal Data and the means by which you acquired such data; (ii) complying with all necessary transparency and lawfulness requirements under Data Protection Laws for the collection and use of Customer Personal Data, including providing adequate notices, obtaining any necessary consents and authorizations, and honouring opt-out preferences; (iii) ensuring you have the right to transfer, or provide access to, the Customer Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); and (iv) ensuring that your use of Controller Personal Data complies with Data Protection Laws and is strictly limited to the purposes set out in the Agreement (including this DPA). You will inform us without undue delay if you are not able to comply with your responsibilities under this 'Compliance with Laws' section or Data Protection Laws.

2.2 Customer Instructions. You are responsible for ensuring that your Instructions to us regarding the Processing of Customer Personal Data comply with applicable laws, including Data Protection Laws. The parties agree that the Agreement (including this DPA), together with your use of the Subscription Service in accordance with the Agreement, constitute your complete Instructions to us in relation to the Supplier's Processing of Customer Personal Data, so long as you may provide additional instructions during the Subscription Term that are consistent with the Agreement and the nature and lawful use of the Subscription Service.

2.3 Security. You are responsible for independently determining whether the data security provided for in the Subscription Service adequately meets your obligations under Data Protection Laws. You are also responsible for your secure use of the Subscription Service, including protecting the security of Personal Data in transit via the Subscription Service.

3. THE SUPPLIER'S OBLIGATIONS AS A PROCESSOR

3.1 Compliance with Instructions. The Supplier will only Process Customer Personal Data for the purposes described in this DPA, or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. The Supplier is not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to the Supplier.

4. TYPES OF DATA

4.1 **The Subject Matter** of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories):

4.1.1 **Personal Master Data** (Key Personal Data): username and User ID (numeric ID), permission type, user creation data, name, address, email address, phone number, IP-address, when accessing the Supplier's portal, phone data (International Mobile Equipment Identity, IMEI lock, international mobile subscriber identity, integrated circuit card identifier),

4.1.2 **Contact Data of Customer's employees:** Email-address, phone number, position, department, organizational assignment.

4.2 **Categories of Data Subjects**

4.2.1 The Categories of Data Subjects comprise: Customers

5. TECHNICAL AND ORGANIZATIONAL MEASURES

5.1 Before the commencement of processing. The Supplier shall document the execution of the necessary Technical and Organizational Measures, set out in advance of a Purchase Order, specifically with regard to the detailed execution of the contract as outlined in the Terms of Service. These documented measures shall become the foundation of the contract. Amendments shall be implemented by mutual agreement.

5.2 Security Requirements. The Supplier shall establish security in accordance with Article 28, Paragraph 3, Point c, and Article 32 GDPR; in particular in conjunction with Article 5, Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32, Paragraph 1, GDPR must be taken into account.

5.3 Technical and Organisational Measures. The Supplier is permitted to implement alternative adequate measures in the pursuit of technical progress and further development. In doing so, the security level of the defined measures must not be reduced. Substantial changes must be documented.

6. RECTIFICATION, RESTRICTION, AND ERASURE OF DATA

6.1 Data Deletion. The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Customer, but only on documented instructions from the Customer. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Customer.

6.2 Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Customer without undue delay.

7. QUALITY ASSURANCES AND OTHER DUTIES OF THE SUPPLIER

7.1 In addition to complying with the rules set out in this Agreement, the Supplier shall comply with the statutory requirements outlined in Articles 28-33 GDPR; in particular with respects to:

7.1.1 Appointed Data Protection Officer. A Data Protection Officer shall be appointed who performs his/her duties in compliance with Articles 38 and 39 GDPR. Their details shall be made available and easily accessible on the website of the Supplier.

7.1.2 Confidentiality. In accordance with Article 28, Paragraph 3, Sentence 2, Point b, and Articles 29 and 32 Paragraph 4 GDPR. The supplier entrusts employees with the data processing conditionally upon having been bound to confidentiality and familiarised with the data protection provisions pertinent to their work. Further, the Supplier, and any persons acting under its authority, shall not process data to which they are provided access unless on the instructions of the Customer, including the powers granted in this contract, unless compelled to do so by law.

7.1.3 Implementation of, and compliance with, all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28, Paragraph 3, Sentence 2 Point c, Article 32 GDPR [details in Appendix 1]:

a) The Customer and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

b) The Customer shall be informed immediately of any inspections and measures conducted by a supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

c) Insofar as the Customer is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by

a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Customer.

7.1.7 The Supplier shall conduct periodical monitoring and review of internal processes relating to the Technical and Organisational Measures. Ensuring compliance with applicable data protection laws.

7.1.8 Facilitate and substantiate the conduct of supervisory powers of the Customer as outlined in Article 9 of this Agreement.

8. SUBCONTRACTING

8.1 Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of principal services.

Ancillary services, such as postal and/or transport services, maintenance and user support services, as well as other measures to ensure the confidentiality, availability, integrity and resilience of assets, are not included in this scope.

However, the Supplier shall be obliged to make appropriate, and legally binding, contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Customer's data, even in the case of outsourced ancillary services.

8.2 The supplier may commission subcontractors (additional contract processors) only once prior explicit written or documented consent is obtained from the Customer.

8.2.1 The Customer agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28, paragraphs 2-4 GDPR:

Company subcontractor	Address	Service / Task
Amazon Web Services	38 Avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg.	Hosting of data and the Supplier's Core Network
Clerk	Clerk, Inc. 660 King Street Unit 345 San Francisco, CA 94107	Identity Management and User Access
Comfone	Mingerstrasse 12, 3014 Bern, Switzerland	Carrier for SS7+GTP traffic
Fathom	2261 Market Street #4156, San Francisco, CA 94114 United States	Training and AI transcription platform for customer meetings
Grafana Cloud	165 Broadway, 23rd Floor New York, NY 10006 United States	Monitoring and logging storage and visualisation of services
Hotjar	Hotjar Ltd Dragonara Business Centre 5th Floor, Dragonara Road, Paceville St Julian's STJ, 3141 Malta	Analytics on product use
IBM Cloud	17 Avenue de l'Europe, Bois-Colombes Cedex, 92275 Paris, France	Hosting of data and the Supplier's Core Network
Intercom	124 St Stephen's Green Dublin 2, D02 C628, Ireland	Customer support management

Kigen	Kigen (UK) Limited Mishcon de Reya, Four Station Square, Cambridge, Cambridgeshire, England, CB1 2GE	SIM Cards
Startdeliver	Klarabergsgatan 60, 111 21 Stockholm Sweden	Customer Success management platform.
Syniverse	15, Rue Edmond Reuter, L-5326 Contern, Grand Duchy of Luxembourg	Carrier for IPX
Thales	Thales 26 Av. Jean François Champollion, 31100 Toulouse, France	SIM Cards
Valid	Avenida de Manoteras, 20 Edificio Tokyo - Panta Baja Madrid, 28050	SIM Cards

8.3 The transfer of personal data from the Customer to the subcontractor and the subcontractor's commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

8.4 If the subcontractor provides the agreed service outside of the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Article 8.1.

8.5 Further outsourcing by the subcontractor requires the express consent of the Supplier. All contractual provisions in the contract chain shall be communicated to and agreed with each additional subcontractor.

9. SUPERVISORY POWERS OF THE CUSTOMER

9.1 The Customer has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. Further, the Customer has the right to convince itself of the compliance with this agreement by the Supplier in their business operations by means of random checks, which are ordinarily to be announced in good time.

9.2 The Customer bears the full cost of such inspections, and the Supplier may claim remuneration for enabling Customer inspections.

9.3 The Supplier shall ensure that the Customer is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Customer the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

9.4 Evidence of such measures, shall be provided by:

- Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, Information Security and Technology department, data privacy auditor, quality control auditor)
- A suitable certification by IT security or data protection audit or ISO 2701 ISO/IEC 27001.

10. COMMUNICATION IN THE CASE OF INFRINGEMENTS BY THE SUPPLIER

10.1 The Supplier shall assist the Customer in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32-36 of the GDPR. These include:

10.1.1 Ensuring an appropriate level of protection through Technical and Organisational Measures that consider the circumstances and purposes of processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

10.1.2 The obligation to report a personal data breach to the Customer within 72 hours of the Supplier becoming aware of an incident. This notification shall provide:

- Indication if the incident is suspected of being caused by unlawful or malicious acts.
- Information concerning severity, impact, and if available, indicators of compromise.
- Outline which types of data have been compromised.

10.1.2.1 A final report concerning said breach shall be provided to the Customer no later than one month after incident notification. The final report shall include:

- Detailed description of the incident, including severity and impact.
- Types of threat or route cause likely to have triggered the incident.
- Where applicable, mitigation measures in place to prevent future incidents.

10.1.3 The duty to assist the Customer about the Customer's obligation to provide information to the Data Subject concerned and to immediately provide the Customer with all relevant information in this regard.

10.1.4 Supporting the Customer with its data protection impact assessment

10.1.5 Supporting the Customer with regard to prior consultation of the supervisory authority

10.2 The Supplier may claim remuneration for support services utilised which are not explicitly outlined as part of the Supplier's Terms of Service, and which are not attributable to failures, network degradation, or network failures on part of the Supplier.

11. AUTHORITY OF THE CUSTOMER TO ISSUE INSTRUCTIONS

11.1 The Customer shall immediately confirm instructions at a minimum in text form.

11.2 The Supplier shall inform the Customer immediately if they consider that an instruction violates Data Protection Regulations. The supplier shall then be entitled to suspend the execution of relevant instructions until the Customer confirms or changes them.

12. DELETION AND RETURN OF PERSONAL DATA

12.1 Copies or duplicates of data shall never be created without the knowledge of the Customer, expect for back-up purposes, as well as to ensure that the Supplier meets regulatory requirements.

12.2 After conclusion of the contracted work, or earlier upon request by the Customer, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Customer, or-upon request- destroy all documents, processing and utilisation results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant, and discarded material.

Appendix 1 - Technical and Organisational Measures

1. Confidentiality (Article 32, Paragraph 1, Point b GDPR)

a) Physical Access Control:

Onomondo has physical access controls in place. These are:

- Access Control System (RFID)
- Video surveillance
- Regulations for visitors and guests
- Secure areas limited by additional access controls
- Smoke detectors and sprinkler systems
- Clean agent fire suppression systems
- Data centre operations outsourced

b) Electronic Access Control:

Onomondo has electronic access controls in place. These are:

- Password policies defining complexity
- Use of a password manager
- Enforcement of secure passwords
- Multi-Factor authentication in accordance with NIST Special Publication 800-63-3
- Automatic blocking (e.g. wrong password, timeout)
- Usage of Mobile Device Management
- Full-disk encryption of mobile devices and monitored via MDM
- Usage of cryptographic methods
- Regulation of data organization

c) Internal Access Control (permissions for user rights of access to and amendment to data):

Onomondo has the following internal controls in place:

- Role-based access control in applications and cloud platforms
- Periodical review of access permissions
- Differentiated access rights (e.g., profiles, and roles)
- Concept / Documentation of access rights which could be audited
- Full-disk encryption for laptop hard disks
- Onomondo does not use physical storage media outside of laptops

d) Isolation Control

Onomondo has the following measures of isolation controls:

- separation of development and production systems
- Network micro segmentation in production systems
- Separated networks, e.g. guest networks, unprivileged corporate network, privileged corporate network, production based on zero-trust / end-to-end encryption

e) Pseudonymization (Article 32, Paragraph 1, Point A GDPR; Article 25, Paragraph 1 GDPR);

This control does not apply to the services provided by Onomondo due to the nature of the data processed.

2. Integrity (Article 32, Paragraph 1, Point b GDPR)

a) Data Transfer control

The measures of data transfer control are:

- Full-disk encryption of laptop hard disks.
- Secure deletion or destruction of media.
- Secure storage of SIM card key material through GPG-based encryption in a seperate cloud-based environment. This environment is further controlled through rigiourous Access Control principles which require National Security Clearance as a pre-requisit.
- Application-specific firewall rules through AWS Security Groups.
- Periodiodical review of network configuration and ports open to the Internet.

b) Data Entry Control

The measures of data entry controls are:

- Logging and reporting systems

3. Availability and Resilience (Article 32, Paragraph 1, Point b GDPR)

a) Availability Control

The measures of availability control controls are:

- Data centre operations outsourced
- Recovery Point Objective for critical data and other data
- Recovery Time Objective for critical data and other data
- Backups for corporate IT data
- Backups for production databases
- Utilisation of database clusters
- Utilisation redundant interconnect points
- Incident Response Policy
- Disaster Recovery Plan
- Regular Test Alerts
- Virus scanners on Windows computers

b) Rapid Recovery (Article 32, Paragraph 1, Point c GDPR);

Description of measures taken by the processor:

- Incident-Response Management with 24/7 on-call support

- Disaster Recovery Plans
- Fixed restart plan
- Defined responsibilities on per-service basis
- Defined responsibilities, processes, and procedures

4. Procedures for regular testing, assessment and evaluation (Article 32, Paragraph 1, Point d GDPR; Article 25, Paragraph 1 GDPR)

a) Data Protection Management

Description of measures and processes undertaken by the processor:

- Company data protection is an ongoing compliance process
- Appointment of an internal Information Security Officer
- Ongoing update sessions regarding changes of new data protection regulations
- Establishment of company data protection guidelines; and
    - continuous improvement processes
    - records of processing activities
    - information
    - contract management
    - IT Secure Policies
    - internal regular Data Protection Awareness Training
    - internal regular Information Security Awareness Training and Enablement
    - secure Working Practices and awareness guidelines
    - processes for data breaches
    - incident Response Management Processes
    - data protection is included in vendor management processes and supplier security policy

b) Incident Response Management

Description of measures and processes undertaken by the processor:

Onomondo has implemented an Incident Response Policy which outlines a set of requirements for responding to a technical, availability, and/or security incidents whereby the roles and responsibilities for responding to any incident are clearly defined. The main categories for Incident Response are as follows:

- Assess, Communicate, and Respond
- Containment and Eradication
- Recovery, Evidence Collection, and Learning
- Resolution, RCA, and Post Incident Activities and Awareness
- Internal Information Security Officer and Crisis Management

c) Data Protection by Design and Default (Article 25, Paragraph 2, GDPR)

Description of measures and processes undertaken by the processor:

- Data retention policies and processes
- System configuration can be restored through infrastructure as code
- Usage of database clusters with built-in replication
- Developers are trained in safe programming techniques and practices

d) Order or Contract Control

Onomondo has no third-party data processing as per Article 28 GDPR without corresponding instructions from the Customer.

Description of measures and processes undertaken by the processor:

- Unequivocal wording of the contract
- Formal commissioning
- Criteria for selecting Processors and Service Providers
- Control checks and alignment with Data Processing Policies

Change Log:

Date	Reviewer	Notes
25.02.2025	Jacob Jagger	First draft.
17.02.2025	Jacob Jagger	Clarifications on quality assurances.
11.06.2025	Asbjørn Reissmann	Language updates for Supplier and Onomondo.
19.06.2025	Jacob Jagger	Updated and corrected sub supplier information.