This Data Processing Agreement ("Agreement") is made between

[DATA CONTROLLER] (“Controller”)

and

Midori Global Consulting Kft.
(the “**Data Processor**”)
(together the “Parties”)

WHEREAS

a) The Company acts as a Data Controller, pursuant to Art. 4 Nr. 7 GDPR.
b) The Company wishes to install and use apps provided by Processor through the Atlassian Marketplace or contact the Processor’s support service, which all imply the processing of End-User data.
c) The Parties seek to implement a data processing agreement that complies with the requirements of the GDPR and, where applicable, other Data Protection Laws..
d) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. **Definitions and Interpretation**
    1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
        1. "Agreement" means this Data Processing Agreement and all Schedules;
        2. "Company End-User Data" means any End-User Data Processed by the Processor or a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;
        3. "Contracted Processor" means a Subprocessor;
        4. "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
        5. "EEA" means the European Economic Area;
        6. "EU Data Protection Laws" 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 End-User data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as well its transposed domestic legislation by the member states and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
        7. "GDPR" means EU General Data Protection Regulation 2016/679;
        8. “EUIDPR” means EUI Data Protection Regulation 2018/1725;
        9. Standard Contractual Clauses means the contractual clauses adopted by the Commission Implementing Decision 2021/914 of 4 June 2021 ensuring appropriate data protection safeguards that can be used as a ground for data transfers from the EU to third countries and Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.

10. "Data Transfer" means a transfer of Company End-User Data from the Company to Processor; or an onward transfer of Company End-User Data from Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor.
11. "Subprocessor" means service providers contracted by the Processor to process End-User Data on behalf of the Company in connection with the Agreement.

2. Subject matter of the contract, nature and purpose of the processing
    1. The subject matter of the Agreement is the processing of Company End-User Data by the Processor on behalf of the Company in connection with the installation and use of the Processor´s apps (“Better Content Archiving and Analytics for Confluence” and related support services as set out in Annex II.
    2. In all other respects, the subject matter of the contract is set out in the main contract dated [date].
    3. The Processor’s own processing of personal data (i.e. via AWS) shall take place exclusively within the territory of the Federal Republic of Germany, in a Member State of the European Union or in another State party to the Agreement on the European Economic Area. Certain Subprocessors disclosed in Annex II and Annex IV (currently Mailchimp and Zendesk) process limited personal data outside the EEA; this Agreement constitutes the Company’s advance notice of that processing, its location, and the Subprocessor concerned, and such processing takes place only where the conditions of Articles 44–48 of the GDPR are met (including, where applicable, the Standard Contractual Clauses referenced in Annex II) or an exception under Article 49 of the GDPR applies.
3. Subject Matter, Nature, Purpose, Categories of Data and Data Subjects, Duration

These points are set out in Annex II to this Agreement.

4. Duration of the Agreement

The duration of this Agreement (term) corresponds to the term of the main contract.

5. **Processing of Company End-User Data**
    1. The Data Processor shall process personal data only on documented instructions from the Company, unless there is an obligation to the contrary under Union law or the law of the Member State to which the Data Processor is subject. In the event of such an obligation, the Data Processor shall inform the Company of the relevant legal requirements without delay prior to processing.
    2. If the Data Processor considers that an instruction infringes data protection regulations, it shall inform the Company without delay in accordance with Article 28(3), third sentence, of the GDPR. Until the relevant instruction is confirmed or amended, the Data Processor is entitled to suspend the execution of the instruction.
6. **Processor Personnel**

In carrying out the work, the Data Processor shall only employ staff who have been bound to confidentiality in accordance with Article 28(3), second sentence, point (b) of the GDPR and who have previously been made familiar with the data protection provisions relevant to them. The Data Processor and any person subordinate to the Data Processor who has access to personal data may process such data exclusively in accordance with the Company’s instructions, including the powers granted in this contract, unless they are legally obliged to process it..

7. **Security**
    1. Processor shall in relation to the Company End-User Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

2. The contracting parties agree to the specific data security measures set out in Annex 1 “Technical and Organisational Measures” to this agreement.
3. The Data Processor shall inform the Company without delay of any inspections and measures taken by the supervisory authority, insofar as they relate to this contract. The Data Processor undertakes to inform the Company without delay of the withdrawal of a certification pursuant to Article 42(7) of the GDPR.

8. **Subprocessing**
    1. The Company grants the Data Processor general authorisation to engage further data processors. The Data Processor shall inform the Company prior to engaging or replacing any subcontractors. The subcontractors approved by the Company at the time of conclusion of the contract are listed in Annex IV to this Agreement. For the purposes of this provision, subcontractors are defined as data processors commissioned by the Data Processor whose services relate directly to the provision of the main service. This does not include ancillary services which the Data Processor utilises, such as telecommunications services, postal/transport services and cleaning.
    2. The Company shall have the right, in individual cases, to object to the engagement of a further data processor. The Company shall exercise the right of objection with regard to the respective Contractor only on objective grounds, exercising reasonable discretion, without delay and at the latest within a period of 45 days of receiving the information. An objective reason shall be deemed to exist in particular if the data processing is to take place in a third country and the requirements of Articles 44 et seq. of the GDPR are not met . The objection must be made in writing and must state all the reasons which, in the Company’s opinion, preclude the engagement of the subcontractor. In the event that the use of the subcontractor is necessary to rule out the risk of a significant impairment of the interests of a contracting party or the data subjects, the respective contractor is entitled to provisionally engage the subcontractor, regarding whose use the Company has been informed, even before the expiry of the objection period. In such cases, the provisional engagement of the subcontractor shall cease upon the Company’s objection, which must be made in good faith and comply with the aforementioned requirements regarding form and justification. Significant impairments within the meaning of the above provision shall be deemed to exist, for example, where the engagement of a subcontractor is necessary for data security reasons or where, without the use of the subcontractor, the Data Processor would incur disproportionately high costs or damage.
    3. If the Data Processor assigns tasks to subcontractors, it is the Data Processor’s responsibility to transfer its data protection obligations under this Agreement to the subcontractor. The parties agree that this requirement is met if the contractual arrangement with the subcontractor provides a level of protection equivalent to that set out in this Agreement and imposes on the subcontractor the obligations laid down in Article 28(3) of the GDPR.
9. **Data Subject Rights**
    1. Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under Art. 12-22 GDPR (Art. 28 (3) (e) GDPR) and otherapplicable Data Protection Laws.
    2. In particular, the Processor shall:
        1. promptly notify Company if it receives a request from a Data Subject under

any Data Protection Law in respect of Company End-User Data; and

2. ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

10. Assistance with Compliance Obligations

10.1 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Company in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR (security of processing, notification of data breaches, data protection impact assessments and prior consultations), insofar as such obligations relate to the processing of Company End-User Data on behalf of the Company.

10.2 The Processor shall assist the Company with all information at its disposal if the Company is subject to administrative offence or criminal proceedings, liability claims by data subjects or third parties, or other claims in connection with the processing of Company End-User Data by the Processor.

11. **End-User Data Breach**
    1. Processor shall notify Company without undue delay upon Processor becoming aware of a End-User Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
    2. Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such End-User Data Breach.

12. **Data Protection Impact Assessment and Prior Consultation**

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company End-User Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

13. **Deletion or return of Company End-User Data**
    1. Upon the Company's request or upon termination or expiry of the Principal Agreement (whichever occurs first), the Processor shall, at the choice of the Company:
        1. delete all Company End-User Data processed on behalf of the Company; or
        2. return such data to the Company and delete existing copies,

unless Union or Member State law requires storage of the personal data.

2. The Processor shall, without being asked, provide written confirmation specifying the date on which all data carriers and other documents containing personal data have been handed over or deleted in accordance with data protection requirements, and that no Company End-User Data remains in its possession.
3. Documentation serving as proof of contractually compliant and proper data processing may be retained by the Processor beyond the end of the Agreement for as long as required by applicable law or for the establishment, exercise or defence of legal claims. Such documentation may be handed over to the Company upon termination of the Agreement for the purpose of exoneration.

14. **General Terms**
    1. Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement

("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

1. Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by email to the address or email address set out in the Privacy Policy of Processor.

15. **Artificial Intelligence and Machine Learning**

1. Processor shall not use Company End-User Data to train, fine-tune, or otherwise improve any artificial intelligence or machine learning model, whether proprietary to Processor or provided by a third party, without Company's prior written consent.
2. As of the effective date of this Agreement, the App does not include or rely on any artificial intelligence or machine learning functionality that processes Company End-User Data.
3. Should Processor introduce AI-powered functionality that processes Company End-User Data (including, without limitation, functionality integrating with Atlassian Rovo or similar AI platforms), Processor shall provide Company with prior written notice and shall not enable such functionality for Company's instance without Company's prior written consent. The Parties shall agree on appropriate governance terms for any such functionality by way of a written amendment to this Agreement before it is enabled.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

[DATA CONTROLLER]
Signature Name:
Title: Date Signed:
Midori Global Consulting Kft.
Signature Name Title Date Signed

ANNEX I

List of parties

Controller:
1. Name:
Contact person's name, position and contact details:
Signature and accession date: . . . . . .

Controller:
1. Name:
Contact person's name, position and contact details:
Signature and accession date: . . . . . .

Controller:
1. Name:
Contact person's name, position and contact details:
Signature and accession date: . . . . . .

Controller:
1. Name:
Contact person's name, position and contact details:
Signature and accession date: . . . . . .

Controller:
1. Name:
Contact person's name, position and contact details:
Signature and accession date: . . . . . .
. . . . . .

Controller:
1. Name:
Contact person's name, position and contact details:
Signature and accession date: . . . . . .
. . . . . .

Controller:
1. Name:
Contact person's name, position and contact details
Signature and accession date: . . . . . .
. . . . . .

Processor(s):
1. Name: *Midori Global Consulting Kft*
Address: Egressy u. 31-33. D/303, 1149 Budapest, HUNGARY
Contact person's name, position and contact details:
Levente Szabo, Marketing Manager, levente.szabo@midori-global.com
Signature and accession date: . . . . . .
. . . . . .

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

- Users: Employees and other authorized users of the controller's Confluence instance
- *Categories of personal data processed*
- Client key – Technical metadata, not personally identifiable
- Instance URL - Technical metadata, not personally identifiable
- Basic information about the installation status (installed/not-installed/creation date)
- Email address of the technical contact, installing the app
- Content lifecycle management rule configurations (schemes)
- User IDs (number of contents owned per user ID - used for charts)
- Space ID and space key (for showing job execution problems - stored for 14 days)
- No further, special categories of personal data within the meaning of Art. 9 GDPR are processed.
- No Confluence page body content, attachments, or comments are read, transmitted, or stored by the App.

Nature of the processing

- The App operates exclusively within the Controller's Confluence Cloud instance via the Atlassian Connect framework and the Confluence Cloud REST API. The body content of Confluence pages is not read, transmitted, or processed by the App. Data in transit is encrypted with HTTPS. The App's actual data-processing operations are set out in full immediately below.
- **In practice, the App::**
  - reads pages, spaces, and content **metadata** (e.g. titles, labels, space keys, last-modified dates, author identifiers) to support content lifecycle workflows, including CQL-driven searches and space exclusion management
  - reads and writes Confluence content properties (content properties are a Confluence metadata mechanism comparable to labels, and distinct from a page's body content) in order to store and manage content lifecycle statuses

(e.g. “archived”, “under review”) and to apply such statuses through content hierarchies (child/descendant pages) by inheritance
  - sends notifications about outdated content and assigns content ownership to individual users or groups. For outdated-content notifications, the App retrieves the relevant recipient's email address from Confluence at the moment the notification is sent and uses it solely to deliver that email; the address is not stored, logged, or retained by the App beyond that immediate operation.
  - executes automations that can trash or delete Confluence content strictly according to conditions configured by the Controller’s own administrators, and does not delete content on its own initiative outside of these customer-defined rules
  - reads, but does not modify, space permissions in order to detect restrictions that would interfere with the App’s core functionality, which can then be bulk-fixed at the explicit request of the Controller’s space or site administrator
  - because the App’s backend is hosted on AWS rather than within Atlassian’s infrastructure, requires the “Access and interact with your data from outside of Atlassian” permission in order to operate at all.

Justification of specific Marketplace-listed permission scopes

- As explained above, Atlassian grants Connect app permissions per API scope rather than per individual capability. The following scopes appear on the Atlassian Marketplace “Permissions” tab; this Annex II — not the Marketplace tab — is the authoritative description of how each is actually used by the App:
  - **Modify space permissions:** used exclusively for the disclosed bulk-fix capability described above, whereby the App can correct a space permission restriction that is interfering with its own core functionality, and only at the explicit request of the Controller’s space or site administrator. The App does not otherwise modify space permissions.
  - **Read page content:** Atlassian’s Confluence content API does not offer a scope that grants access to a page’s metadata and content properties without also bundling access to the page’s body content field. The App’s own code never requests or processes that field; as stated above and reaffirmed here, page body content is not read, transmitted, or stored by the App.
  - **View all user email addresses regardless of visibility settings:** required for the disclosed outdated-content notification feature, so that a notification can be delivered to the correct recipient regardless of that user’s personal visibility preference for their own email address. Atlassian does not offer a narrower scope limited to “send a notification without viewing the address.”
  - **Create and modify spaces:** not exercised by any feature described in this Annex II. It is granted automatically as an artifact of the broader, coarse-grained Confluence space-related API scope needed for the App’s disclosed space exclusion management and space permission features. Midori does not use this scope to create or modify spaces, and will remove it if and when Atlassian’s platform permits requesting a narrower scope grant.
- The App does not read, transmit, modify, or store Confluence page body content. Data in transit is encrypted with HTTPS. The data listed under “Categories of personal data processed” above is stored on AWS (EU-WEST-1, Ireland), with one exception: the installing/administrative contact’s email address is processed and stored by Mailchimp for communications purposes (see the Mailchimp sub-processor entry below), not by AWS. No other Confluence content or end-user data is stored by Midori.

Purpose(s) for which the personal data is processed on behalf of the controller

- The purpose of the processing operation is to support content governance and lifecycle management within the collaboration tool Confluence (Atlassian). Specifically, the app

enables administrators to enforce content quality standards, identify stale or redundant content, and manage archiving workflows according to the organisation's retention policies.
- Confluence (Atlassian) is a cloud-based collaboration and documentation platform. Better Content Archiving and Analytics is an app from the Atlassian Marketplace, installed on Confluence Cloud.

Duration of the processing

- The processing is on continued basis.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

Subprocessor: Mailchimp

- **Description of the processing:** Email communications
- **Personal data processed:**
  - Email address of the technical contact
  - Technical contact full name
- **Processing location:** United States
- **Duration of the processing:** As long as the app is installed/deletion is requested

Subprocessor: AWS

- **Description of the processing:** Storing app configuration data (archiving job definitions, rules, and schedules) and the limited data described in Annex II, and serving the App's backend logic. No Confluence page body content, attachments, or comments are stored.
- **Personal data processed:** Same categories as listed above under "Categories of personal data processed", with the exception of the installing/administrative contact's email address (processed by Mailchimp, not AWS — see below). This includes Atlassian user IDs, which constitute personal data, alongside the technical/organisational data (client key, instance URL, installation status/date, content lifecycle rule configurations, space ID/space key)
- **Processing location:** Ireland
- **Duration of the processing:** As long as the app is installed

Subprocessor: Zendesk

• Description of the processing: Customer support ticketing and communication
• Personal data processed:
– Contact name and email address of the person submitting a support request
– Content of the support request, including any diagnostic information voluntarily shared to help resolve the issue
• Processing location: United States
• Duration of the processing: For as long as necessary to resolve the support request, in accordance with Zendesk's data retention policy

Subprocessor: Google Ireland Limited (Google Analytics)

• Description of the processing: Website usage analytics for midori-global.com. This does not relate to, and does not process, Company End-User Data processed through the App.
• Personal data processed: Website visitor identifiers (e.g. cookie/device identifiers) collected in connection with visits to Midori's public website only
• Processing location: European Economic Area, with transfers to the United States covered by Standard Contractual Clauses
• Duration of the processing: Per Google Analytics' standard data retention settings

ANNEX III

Technical and organizational measures including technical and organizational measures to ensure the security of the data

Description of the technical and organizational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security,

taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

Measures of pseudonymization and encryption of personal data:

- Data in transit is encrypted with HTTPS.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Access to infrastructure accounts is continuously monitored
- Each EC2 instance's attached Security Groups set up to restrict public ports
- AWS GuardDuty Intrusion detection system is enabled

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- The application datastore (AWS RDS) has automated backups with point-in-time recovery enabled, allowing restoration of the limited data described in Annex II in the event of a physical or technical incident.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

- Key infrastructure elements, like AWS account access, intrusion attempts, system performance are monitored continuously. Relevant teams have response and recovery plans.
- Midori's policies, like the Operations Security Policy, Data Management Policy and Secure Development Policy are reviewed annually.

Measures for user identification and authorization

- N/A, the app doesn't authorize users, Confluence does.

Measures for the protection of data during transmission

- Data in transit is encrypted with HTTPS.

Measures for the protection of data during storage

- Data at rest in the application datastore (AWS RDS) is encrypted using an AWS-managed KMS key, consistent with the AWS DynamoDB encryption used elsewhere. The database also runs in a private AWS Virtual Private Cloud (VPC) subnet with no direct public accessibility, reachable only by the App's own backend services, and gated by security groups and least-privilege IAM policies.

Measures for ensuring physical security of locations at which personal data are processed

- We use AWS services, physical security is provided by AWS.

Measures for ensuring events logging

- AWS accounts have CloudTrail enabled.
- Application-level logs capture only operational/event metadata needed for monitoring and troubleshooting — for example, that a given archiving automation ran and its duration, that an automation sent a number of notification emails, or that a background job updated a number of content statuses. These logs do not contain Confluence content or personal data beyond what is listed in Annex

Measures for ensuring system configuration, including default configuration

- Access to infrastructure accounts is continuously monitored
- Changes to system configuration are monitored

Measures for internal IT and IT security governance and management

- Change management procedures enforced
- Application changes reviewed by senior developer
- Author is not the reviewer of pull requests
- Midori has an SOC2 compliant Operations Security Policy
- Bitbucket repository visibility has been set to private
- CI/CD system is in use

Measures for certification/assurance of processes and products

- Midori is SOC2 compliant: https://app.vanta.com/doc/trust?id=659bc97f0dbf4869c7b0a1ef&r=9c7xkk6odljhiame0nmwf

Measures for ensuring data minimization

- The App only requests the Confluence REST API scopes required for its content lifecycle management features and only stores the limited data categories listed in Annex II. No Confluence page body content is read or stored.

Measures for ensuring data quality

- The App relies on Confluence as the source of truth for content and space metadata; the App does not independently alter the accuracy of this source data.

Measures for ensuring limited data retention

- Data is retained only for as long as the App remains installed and is automatically deleted within 90 days of uninstallation; space ID and space key data is retained for a maximum of 14 days regardless of installation status. Midori complies with special/early data deletion requests sent to info@midori-global.com.

Measures for ensuring accountability

- Application change management is enforced
- AWS events are logged
- AWS accounts and access rights are monitored

Measures for allowing data portability and ensuring erasure]

- Any data erasure right can be executed by request through the support service.
- Administrators can review the App's action history (job type and status, trigger, timestamps, duration, and per-job metrics such as spaces processed, content statuses changed, notification emails sent, and items archived/deleted) at any time via the App's Job Audit Log, available at both site and space level within Confluence. The App does not currently offer a dedicated bulk-export function for this history; administrators wishing to retain a copy should do so via the Job Audit Log before uninstalling.

Additional binding organizational measures:

- All staff of the service provider and of its sub-processor/s will comply with the service provider policies, procedures, etc.;
- All cases where personal data can be either accessed from a third country or transferred to a third country shall be documented by the processor;
- The processor shall make these documents access or transfers available to [customer] on a regular basis and upon request of [customer]
- Midori provides technical support and assistance to the data controller through the support service.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

A) *Amazon Web Services*

Technical and organizational measures:

- Data is encrypted in transit via HTTPS REST API requests
- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018
- Network inspection to detect and protect the workloads from malicious or unauthorized traffic.
- Agents that detect and protect against malware and other threats found on your operating system or host. Includes AV, EDR, EPP, FIM, and HIDS.
- Protection of data via encryption.
- Logging, Monitoring, Threat Detection, and Analytics.
- Identity and Access Control

- Vulnerability and Configuration Analysis
- Application Security: Assesses code, logic, and application inputs to detect software vulnerabilities and threats.

B) *Mailchimp*

Technical and organisational measures:

- Internal communications are encrypted with TLS and WPA2128 bits.
- External communications, mobile apps and API are encrypted with VPN (256 bits.
- **Data Center Security:**
  - Control access management.
  - DDOS mitigation in place.
  - data centers manage physical security 24/7 with biometric scanners.
- **Protection from Data Loss and Corruption:**
  - User accounts are segregated from each other through multiple layers of logic which prevent corruption and overlap
  - MailChimp's technology infrastructure includes network devices such as firewalls, and IDS/IPS tools which are strategically placed to control and monitor network traffic for data loss and corruption
  - Account data is mirrored and regularly backed up off site)
- **Application-Level Security:**
  - Mailchimp account passwords are hashed. Our own staff can't even view them. If you lose your password, it can't be retrieved—it must be reset.
  - All login pages (from our website and mobile website) pass data via TLS 1.2 or higher.
  - The entire Mailchimp application is encrypted with TLS 1.2 or higher.
  - Login pages and logins via the Mailchimp API have brute force protection.
  - We provide the ability to enable email or SMS notifications about key activity.
  - We provide the ability to enable two-factor (2FA) authentication to your Mailchimp account.
  - We perform regular external and internal security penetration tests throughout the year using different vendors. The tests involve high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.
  - The findings of our pen-testing results are kept strictly confidential. We can confirm that any findings are addressed and repaired.
- **Internal IT Security:**
  - Mailchimp offices are secured by keycard access and biometrics, and they are monitored with infrared cameras throughout.
  - Mailchimp facilities have at least one staffed guard station/receptionist area on premise.
  - Our office network is heavily segmented and centrally monitored.
  - We have a dedicated internal security team that constantly monitors our environment for vulnerabilities. They perform penetration testing and social engineering exercises on our environment and our employees. Our security team includes OSCP and CISSP certified members.
- **Employee Security & Safeguards:**
  - We continuously train employees on best security practices, including how to identify social engineering, phishing scams, and hackers.
  - Employees on teams that have access to customer data (such as tech support and our engineers) undergo criminal history and credit background checks prior to employment.
  - All new hires and contingent workers are required to sign Non-Disclosure and

Confidentiality Agreements. Additionally, they are required to attend and certify completion of training on Intuit's Code of Conduct and information security policies including acceptable use.
    - In order to protect our company from a variety of different losses, Mailchimp has established a comprehensive insurance program. Coverage includes, but is not exclusive to: coverage for cyber incidents, data privacy incidents (including regulatory expenses), general error and omission liability coverage, excess cyber liability coverage, property and business interruption coverage, as well as international commercial general liability coverage.
- SOC II & III Compliant and PCI DSS Certification
- ISO 27001 Certification

ANNEX IV

List of sub-processors

The controller has authorised the use of the following sub-processors: [*Identity and contact details of the sub-processor(s) and, where applicable, of the sub-processor's data protection officer]*

1. Name: Amazon Web Serivces.
Address: One Burlington Plaza, Burlington Road, Dublin 4, Do4 Rh96, Ireland
Contact person's name, position and contact details: dataprivacyframework@amazon.com https://aws.amazon.com/contact-us/compliance-support/
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Providing computing services

2. Name: Mailchimp (The Rocket Science Group LLC d/b/a Mailchimp Intuit Inc.)
Address: Intuit Inc. 2700 Coast Ave, Mountain View, CA 94043.
Contact person's name, position and contact details: Liza Schmitt, Sr. Manager of Privacy & Data Protection, Email: liza_schmitt@intuit.com, Phone: (650) 282-0634

3. Name: Zendesk, Inc.
Address: 989 Market Street, San Francisco, CA 94103, USA
Contact person's name, position and contact details: Zendesk Privacy Team, Email: privacy@zendesk.com
Description of the processing: Customer support ticketing and communication platform

4. Name: Google Ireland Limited (Google Analytics)
Address: Gordon House, Barrow Street, Dublin 4, Ireland
Contact person's name, position and contact details: Google Data Protection Office, via https://support.google.com/policies/troubleshooter/7575787
Description of the processing: Website usage analytics for midori-global.com only; not used in connection with Company End-User Data processed through the App