

Data Processing Agreement — Midori

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

(the "**Company**")

and

Midori Global Consulting Kft.

(the "**Data Processor**")

(together the "Parties")

WHEREAS

- a) The Company acts as a Data Controller.
- 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 current legal framework in relation to data processing and with the 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) and with the 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.
- d) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "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;

1.1.3 "Contracted Processor" means a Subprocessor;

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data

protection or privacy laws of any other country;

1.1.5 "EEA" means the European Economic Area;

1.1.6 "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.

1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.8 "EUIDPR" means EUI Data Protection Regulation 2018/1725;

1.1.9 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.

1.1.10 "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.

1.1.11 "Subprocessor" means service providers contracted by the Processor to process End-User Data on behalf of the Company in connection with the Agreement.

2. Processing of Company End-User Data

2.1 Processor shall:

2.1.2 not Process Company End-User Data other than on the relevant Company's documented instructions.

2.1.3 The Company instructs Processor to process Company End-User Data.

2.1.4 The Company and the service provider - acting as a processor - acknowledge and agree with the clauses set up in the Annex and its annexes in regards to the processing of personal data on behalf of [customer] by the processor and its sub-processors.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company End-User Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company End-User Data.

Processor shall ensure that all persons authorized to process Company End-User Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Processor

shall ensure that equivalent confidentiality obligations are imposed on all sub-processors engaged in accordance with Section 5.

4. Security

4.1 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.

5. Subprocessing

5.1 The Company provides the Processor with general written authorisation to engage sub-processors for the processing of Company End-User Data. The current list of authorised sub-processors is set out in Annex IV.

5.2 The Processor shall inform the Company in writing of any intended changes to the list of sub-processors (additions or replacements) at least 30 days before the engagement of the new or replacement sub-processor, thereby giving the Company sufficient time to object.

5.3 If the Company has a reasonable, legitimate objection to the engagement of a new or replacement sub-processor, the Company shall notify the Processor in writing within the 30-day notice period. The Parties shall discuss the objection in good faith with a view to achieving a commercially reasonable resolution. If no resolution can be reached, the Company may terminate the affected services by written notice.

5.4 The Processor shall impose on each sub-processor, by way of a written contract, data protection obligations no less protective than those set out in this Agreement. The Processor shall remain fully liable to the Company for the performance of each sub-processor's obligations.

6. Data Subject Rights

6.1 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 the Data Protection Laws.

6.2 Processor shall:

6.2.1 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

6.2.2 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.

7. End-User Data Breach

7.1 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.

7.2 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.

8. 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.

9. Audit and Inspection Rights

9.1 Processor shall make available relevant certifications and independent third-party audit reports (including SOC 2 Type II) to demonstrate compliance with this Agreement. The Company agrees to first review such documentation before exercising any further audit rights.

9.2 If, after reviewing the documentation in 9.1, the Company has a specific, substantiated reason to conduct a further audit, the Company may request such an audit no more than once per calendar year, at the Company's expense, with at least 60 days' prior written notice. Such audit shall be conducted primarily through remote means (document review, questionnaires, video conference). On-site inspection shall only be permitted where remote methods are demonstrably insufficient.

9.3 Any auditor mandated by the Company shall be bound by appropriate confidentiality obligations and shall not be a competitor of the Processor.

10. Deletion or return of Company End-User Data

10.1 Subject to this section 9 Processor shall upon request delete and procure the deletion of all copies of those Company End-User Data.

10.2 Processor shall provide written certification to Company that it has fully complied with this section.

11. Data Transfer

11.1 By using/installing software products made by the Processor, Controller consents to the transfer of Data to countries outside the EU and/or the European Economic Area (EEA). If End-User data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the End-User data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU-approved standard contractual clauses for the transfer of personal data.

12. Modification and review

A joint review of the clauses set up in the Annex and its annexes shall be undertaken by the parties whenever such review is necessary or when new standard contractual clauses on data protection are issued by the European Commission and/or European Data Protection Supervisor.

13. General Terms

13.1 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.

13.2 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.

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

[COMPANY NAME]

Signature _____
Name: _____
Title: _____
Date Signed: _____

Midori Global Consulting Kft.
Signature _____
Name _____
Title _____
Date Signed _____

ANNEX

STANDARD CONTRACTUAL CLAUSES CONTROLLER - PROCESSOR

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 29(3) and (4) of 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].
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5
Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II
OBLIGATIONS OF THE PARTIES

Clause 6
Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7
Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (b) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (c) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (d) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

- (a) **OPTION 2: GENERAL WRITTEN AUTHORISATION:** The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.
- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations. The processor shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in Articles 33 and 36 to 38 of Regulation (EU) 2018/1725.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 34(3) of Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available,

subsequently be provided without undue delay.

- (c) in complying, pursuant to Article 35 of Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.
- (d) Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I
List of parties

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:
- *Categories of personal data processed*
 - Pseudonymous user name and mail address

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- No sensitive data is processed

Nature of the processing

- The processing only uses read-type operations on Jira data (i.e. against the Jira Cloud REST API). The app is not able to modify data in Jira. The selected Jira data to be exported is sent to AWS (located in EU-WEST1). The data in transit is encrypted with HTTPS.
- All the PDF exportation run in their own fully-isolated environments. Therefore, data integrity cannot be violated at those levels. The produced PDF document is sent back to the client's browser using HTTPS. Finally, the processing environment is erased from the AWS server. No Jira data is stored.

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

-

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
 - o Email communications
- Personal data processed
 - o Email address
 - o Full Name
- Processing location
 - o United States
- Duration of the processing
 - o As long as the app is installed/deletion is requested

Subprocessor: AWS

- Description of the processing

- Compiling a PDF document based on a template scripts using raw Jira data sent for processing from the Jira Cloud user interface.
- Personal data processed
 - Jira data / Not necessarily personal data
- Processing location
 - Ireland
- Duration of the processing
 - 10-30 seconds, depending the amount of the data processed.

Subprocessor: Zendesk

- Description of the processing: Customer support ticketing and communications
- Personal data processed: Email address, Full Name, any personal data included in support requests
- Processing location: United States
- Duration of the processing: As long as the app is installed/deletion is requested

ANNEX III

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

Description of the technical and organisational 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 pseudonymisation 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
- AWS DynamoDB Encryption at Rest is enabled
- 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 app doesn't store Jira data. There is nothing to restore in connection with personal data/Jira data processing.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational 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 authorisation

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

Measures for the protection of data during transmission

- Data in transit is encrypted with HTTPS.

Measures for the protection of data during storage

- AWS DynamoDB Encryption at Rest is enabled

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.

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/midori-global.com/trust/9c7xkk6odljhiame0nmwf>

Measures for ensuring data minimisation

- The app relies on Jira regarding what data is transferred for processing.

Measures for ensuring data quality

- The app relies on Jira regarding data quality transferred for processing.

Measures for ensuring limited data retention

- Midori complies with special data deletion requests sent to info@midori-global.com. Personal data (Jira data) is not stored.

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.

Additional binding organisational 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 the Company on a regular basis and upon request
- 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 organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

A) Amazon Web Services

Technical and organisational 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
 - o Control access management.
 - o DDOS mitigation in place.
 - o data centers manage physical security 24/7 with biometric scanners.
- Protection from Data Loss and Corruption
 - o 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

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

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 Services.

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: 181 S. Fremont St., Suite 100, San Francisco, CA 94105, USA

Contact person's name, position and contact details: Privacy Team, Email: privacy@zendesk.com

Description of the processing: Providing customer support ticketing and communication services