Refined

Refined's Data Processing Agreement

(DPA)

Effective Starting: July 7, 2023.

Table of Contents

Cloud version of the Product
For the cloud version of the Product, all of the DPA, including the appendices, are applicable.

On-Prem version of the Product
For the on prem version of the Product, the processor (i.e. Refined) will only process personal data if the Customer choose to give the processor access to personal data during a support case. The Customer itself decides if any personal data is shared with the processor. The DPA, including the appendices, only apply in relation to such processing of personal data.

1. Background and Interpretation

1.1. RefinedWiki AB ("Refined"), a Swedish company with org. No. 556827-1760, will upon performance of the Agreement process personal data on behalf of the Customer, in the capacity of the Customer's processor. Refined will process personal data for which the Customer is the controller as defined in the "GDPR".

1.2. This DPA forms an integral part of the Agreement. The purpose of this DPA is to ensure a secure, correct and legal processing of personal data and to comply with applicable requirements for data processing agreements as well as to ensure adequate protection for the personal data processed within the scope of the Agreement.

1.3. If the Customer acts as processor of personal data on behalf of a third-party such third-party is the controller and Refined is a sub-processor. In such case the Customer shall always notify Refined of any controller so that Refined can comply with the GDPR. The obligations that Refined has towards the Customer under this DPA shall apply towards such company that is the controller, insofar as is necessary in order to comply with existing data protection laws, including the GDPR.

1.4. Any terms used in this DPA, e.g. processing, personal data, data subjects, supervisory authority, etc., shall primarily have the meaning as stated in the GDPR and otherwise in accordance with the Agreement, unless otherwise clearly indicated by the circumstances. The terms "processing" and "personal data" refer exclusively to such processing and such personal data that Refined processes on behalf of the Customer in accordance with this DPA.

1.5. In light of the above, the Parties have agreed as follows.

2. Refined's obligations

2.1. Refined shall notify the Customer without undue delay, if, in Refined's view, an instruction infringes the GDPR. In addition, Refined is to immediately inform the Customer of any changes affecting Refined's obligations pursuant to this DPA. Refined may not take any action which may result in that the Customer can be deemed to be in violation of the GDPR.

2.2. When processing personal data, Refined shall:

a) only process personal data in accordance with the Customer's documented instructions, which at the time of the Parties entering into this DPA are set out in Appendix 1A, including transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which Refined, or party that process personal data

[1]Regulation 2016/679 of the European parliament and of the Council.

as sub-processor to Refined ("Sub-processor"), is subject to. In such a case, Refined or the Sub-processor shall inform the Customer of that legal requirement before processing, unless the law prohibits such information in important grounds of public interest;

b) ensure confidentiality according to section 5;

c) maintain an adequate level of security for the personal data by implementing all technical and organizational measures set out in Article 32 of the GDPR in the manner set out in section 4 below;

d) respect the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging a Sub-processor;

e) taking into account the nature of the processing, assist the Customer by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

f) assist the Customer in ensuring compliance with the obligations pursuant to Articles 32-36 of the GDPR, taking into account the nature of the processing and the information available to Refined;

g) at the choice of the Customer, delete or return all the personal data to the Customer sixty (60) days after the Customer removes the Product in the Third Party Platform, to make sure that the Customer e.g. not has removed the Product by mistake, and delete existing copies, unless EU law or applicable national law of an EU Member State requires storage of the personal data; and

h) make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this DPA and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor agreed upon by the Parties.

3. The Customer's obligations

3.1. The Customer is required to provide clear and documented instructions to Refined regarding the processing of personal data by Refined under this DPA. The type of personal data and categories of data subjects processed by Refined under this DPA and the purpose, nature, duration and objects of this processing, are described in the instructions on processing of personal data in Appendix 1A. The Customer shall ensure that Refined is not able to process additional categories of personal data or personal data in relation to other data subjects than those specified in Appendix 1A.

3.2. The Customer is responsible for ensuring that the instructions provided by the Customer to Refined are in accordance and compliance with the requirements of the GDPR and the supervisory authority's binding decisions, recommendations and guidelines, practices in the field of data protection, supplementary local adaptation and legislation as well as sector-specific legislation in relation to data protection.

3.3. The Customer undertakes to comply and keeping up to date with the GDPR. The Customer shall in particular:

a) be contact person towards data subjects and i.e. respond to their inquiries regarding the processing of personal data;

b) ensure the lawfulness of the processing of personal data, provide information to data subjects pursuant to Articles 13 and 14 of the GDPR and maintain a record of processing activities under its responsibility;

c) provide Refined with documented instructions for Refined's processing of personal data, including instructions regarding the subject-matter, duration, nature and purpose of the processing as well as the type of personal data and categories of data subjects;

d) immediately inform Refined of changes that affect Refined's obligations under this DPA;

e) immediately inform Refined if a third party takes action or lodges a claim against the Customer as a result of Refined's processing of personal data; and

f) immediately inform Refined if anyone else is the Customer or joint Customer with the Customer of the personal data.

4. Security

4.1. Refined shall implement technical and organisational security measures in order to protect the personal data against destruction, alteration, unauthorised disclosure and unauthorised access. The technical and organisational measures Refined implements shall meet the requirements of the GDPR and the Agreement, taking into account the state of the art, the costs of implementation, the nature, scope, context and purpose of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

4.2. Refined shall notify Customer of accidental or unauthorised access to personal data or any other personal data breach without undue delay after becoming aware of such data breach and pursuant to Article 33 of the GDPR. Such notification shall not in any manner imply that Refined has committed any wrongful act or omission, or that Refined shall become liable for the personal data breach.

5. Confidentiality

5.1. In addition to what follows from the Agreement, Refined shall not without the Customer's prior written consent, disclose or otherwise make available personal data to any third party, except (i) to the Sub-processors that have been engaged in accordance with this DPA, or (ii) if the data is ordered to be shared with the supervisory authority or should be disclosed according to the GDPR or another statutory obligation.

5.2. Refined undertakes to ensure that persons authorized to process the personal data have committed themselves to confidentiality for such processing or are under an appropriate statutory obligation of confidentiality.

6. Disclosure of Personal Data and Contact with Supervisory Authority

6.1. If Refined receives a request from a data subject, supervisory authority or any other third party regarding obtaining access to personal data that Refined processes on behalf of the Customer, Refined shall immediately forward the request to the Customer. Refined, or persons under Refined's supervision, shall not disclose personal data or any other information related to the processing of the personal data without explicit, documented instruction from the Customer, unless Refined is required to do so subject to the GDPR. In the event that Refined is required to disclose personal data sub-

ject to the GDPR, Refined shall take all actions to request confidentiality in connection with the requested information and immediately inform the Customer of the disclosure, in so far as Refined is not prevented from doing so under the GDPR.

6.2. Refined shall without undue delay inform the Customer of any contacts from the supervisory authority regarding the processing of personal data and provide the Customer, to the extent permitted by law, with all information relevant in this regard. Refined is not entitled to represent or act on the Customer's behalf in relation to the supervisory authority.

7. Sub-processors and Transfer

7.1. Refined may engage Sub-processors in its processing of personal data. The Customer hereby grants Refined a general authorisation to engage Sub-processors. Sub-processors, at the conclusion of the Agreement, are listed in the list of sub-contractors in Appendix 1B. All Sub-processors shall be bound by written agreements in which the Sub-processor is imposed to the same data protection obligations as Refined is imposed to under this DPA.

7.2. Refined shall inform the Customer of any intended changes concerning the addition or replacement of sub-processors, thereby giving the Customer the opportunity to object to such changes. Such objection shall be made in writing and within thirty (30) days after Refined has informed the Customer about the intended changes. If the Customer objects to Refined engaging a sub-processor and the Parties are unable to agree within a reasonable time, Refined shall have the right to terminate the DPA and/or relevant parts of the Agreement in whole or in part with thirty (30) days' notice.

7.3. In case a Sub-processor fails to perform its undertakings, Refined is fully responsible towards the Customer for the due performance of the Sub-processor's undertakings.

8. Transfers to Third Countries

8.1. The Processor shall, as a main principle, not intentionally, nor unintentionally transfer personal data outside the EU/EEA.

8.2. However, in some cases, the use of certain services, despite what is stated above, could entail processing of personal data outside the EU/EEA. If Refined and/or Sub-processors transfers personal data outside the EU/EEA, such transfer shall always, as far as possible, comply with the applicable data protection requirements according to the GDPR.

9. Compensation

9.1. If not explicitly stated in this DPA Refined is not entitled to any additional compensation for the processing of personal data in accordance with this DPA, instead the compensation provided pursuant to the Agreement also encompasses the measures in this DPA.

9.2. In addition to the above, Refined is entitled to reasonable compensation for additional costs as a result of special adjustments for the Customer if such adjustments is due to the Customer's instructions, the compensation shall include any costs relating to hiring third parties to make the relevant adjustments. However, the compensation shall only be paid if Refined has notified the Customer in advance of such compensation and the Customer has given its approval.

10. Limitation of Liability

10.1. Each Party shall be responsible for any damages and administrative fines imposed to it under articles 82 and/or 83 of the GDPR.

10.2. Notwithstanding any limitation of liability in the Agreement and what is stated in this clause 10, Refined's liability under this DPA shall be limited to direct damages and an amount corresponding to the fees paid by the Customer to Refined under the Agreement for a period of twelve (12) months before the damage occurred.

10.3. Under no circumstances shall a Party be liable for any loss of profits or other indirect damage caused to the other Party, unless such damage is the result of intent or gross negligence. Furthermore, the Party is only entitled to compensation for damage provided that:

a) the aggrieved Party immediately, and no later than within thirty (30) days, notify the other Party in writing after the aggrieved Party has become aware of the damage; and

b) the aggrieved Party seeks to reduce the extent of the damage as much as possible through cooperation with the other Party.

11. Term and Termination

11.1. The DPA is valid from the time the Agreement is entered into.

11.2. Upon termination of the DPA, for whatever reason, Refined shall, in accordance with the Customer's instructions and at the expense of the Customer, delete or return all personal data to the Customer or the person responsible for personal data and then delete existing copies, unless personal data storage is required under Union or Member State law. However, the above requirements for deletion do not apply to deletion of backups, which occurs in accordance with the current backup routine, and that is thus not something that Refined can affect manually.

11.3. This DPA remains in force as long as Refined processes personal data on behalf of the Customer, including by deletion or returning of personal data according to section 11.2 above. This DPA shall thereafter cease to apply.

11.4. Sections 5, 10 and 13 shall continue to apply even after this DPA has been terminated.

12. Amendments

12.1. If provisions of the GDPR change or if a supervisory authority issues guidelines, decisions or regulations regarding the application of the GDPR during the term of this DPA, with the result that this DPA does not meet the requirements for a data processor agreement, the Parties shall change this DPA to meet the requirements.

12.2. Refined is at any time entitled to change the DPA by notifying the Customer.

12.3. Changes in accordance with section 12.1 or 12.2 above shall enter into effect no later than thirty (30) days after the party's amendment notification, unless the other party has objected to such proposed change or new version of the DPA. If a party makes such an objection and the parties are unable to agree within a reasonable time, Refined shall have the right to terminate the DPA and/or relevant parts of the Agreement in whole or in part with thirty (30) days' notice.

12.4. If Refined would choose to adapt to the Customer's objection, Refined shall be entitled

to reasonable compensation from the Customer for the costs that Refined incurs as a result of such adaptation.

13. Miscellaneous

13.1. This DPA supersedes and replaces all data processor agreements between the Parties potentially existing prior to this DPA.

13.2. If a Party assigns the Agreement (according to the terms in the Agreement), this DPA shall also be deemed assigned to the assignee of the Agreement. However, this DPA may still apply between the original Parties. No Party shall assign this DPA separately from the Agreement.

13.3. Should any clause in this DPA or part thereof be void or invalid, the other provisions of the DPA shall remain in force and the clause may be amended to the extent such invalidity materially affects the rights or obligations of either Party under this DPA.

13.4. In the event of deviating provisions between the Agreement and this DPA, the provisions of this DPA shall prevail with regards to processing of personal data and nothing in the Agreement shall be deemed to restrict or modify obligations set out in this DPA.recommendations and guidelines, practices in the field of data protection, supplementary local adaptation and legislation as well as sector-specific legislation in relation to data protection.

GDPR - Instructions on processing of personal data (Appendix 1A)

Cloud version of the product

Purposes

1. Refined processes personal data under the DPA for the purpose of providing any and all Products as well as fulfilling its obligations under the agreement in relation to providing the Product ("To provide the Product and fulfil the Agreement").

2. Refined also processes personal data under the DPA for the purpose of providing support to the Customer ("Support")

Types of personal data

The types of personal data that are processed are:

To provide the Product and fulfil the Agreement

- Internet protocol (IP) address.

The following personal data can be processed within the Product, however never stored as part of the Product or by Refined:

- E-mail address – If a user searches for another user within the Product and uses an e-mail address in the search function.

- Display names and avatar – If a user does not actively set up GDPR security at Atlassian, Refined can process the display name (first and last name) and any personal profile pictures (avatar).

- Content – If a user chooses to post or share any content in the Product that contains personal data.

Support

The types of personal data that are processed will be dependent on what the Customer shares with Refined during support. Refined will only process such personal data that the Customer may show during the support or that Refined is otherwise given access to.

If Refined asks the Customer to provide a HAR file it may include, for example, the first and last name of the user who generated the file. The Customer should review the content of the file and remove any personal or sensitive information before sending the file to Refined.

Categories of data subjects

The categories of data subjects include:

To provide the Product and fulfil the Agreement

Users who access any website built by using the Product.

Support

The categories of data subjects which the Customer shares personal data about during support, e.g. the Customer's employees.

Retention time

The personal data is stored for the following periods of time:

To provide the Product and fulfil the Agreement

IP addresses: 2 weeks

Support

The other personal data is deleted as soon as the support matter is resolved.

Processing operations

The processing operations includes:

To provide the Product and fulfil the Agreement

The processing and storing of personal data are done in order to provide a reliable service and block possible malicious or unintended use of the Product.

Support

Reading the information that the Customer provides, e.g. by screen sharing.

Storing the information that the Customer sends, e.g., in case Refined needs to review the information in detail to handle a support case

On-prem version of the product

Purposes

Refined only processes personal data under the DPA for the purpose of providing support to the Customer.

Types of personal data

The types of personal data that are processed will be dependent on what the Customer shares with Refined during support. Refined will only process such personal data that the Customer may show during the support or that Refined is otherwise given access to.

If Refined asks the Customer to provide a HAR file it may include for example the first name and last name of the user who generated the file. The Customer should review the content of the file and remove any personal or sensitive information before sending the file to Refined.

Categories of data subjects

The categories of data subjects which the Customer shares personal data about during support, e.g. the

Customer's employees.

Retention time

The personal data is deleted as soon as the support matter is resolved.

Processing operations

- Reading the information that the Customer provides, e.g. by screen sharing.

- Storing the information that the Customer sends, e.g. in case Refined needs to review the information in detail to handle a support case.

GDPR - List of sub processors (Appendix 1B)

Heroku (Salesforce.com, Inc.)

Geographical location: USA
Purpose: Cloud service provider
Mechanism for transfer to third country (outside of EU/EEA): Standard Contractual Clauses

LogDNA

Geographical location: USA
Purpose: Log management
Mechanism for transfer to third country (outside of EU/EEA): Standard Contractual Clauses

Cloudflare, Inc.

Geographical location: USA
Purpose: DNS/CDN/Security
Mechanism for transfer to third country (outside of EU/EEA): Standard Contractual Clauses

Amazon Web Services, Inc.

Geographical location: USA, EU (EU is currently available to select customers. General availability will be released in 2023).
Purpose: File storage
Mechanism for transfer to third country (outside of EU/EEA): Standard Contractual Clauses

Atlassian

Geographical location: USA or other (not all data is geographically pinned, see here)
Purpose: Customer support management
Mechanism for transfer to third country (outside of EU/EEA): Standard Contractual Clauses

GDPR - Technical and organizational measures

For the cloud versions of the product all measures applies. For our On-Prem (Data Center) products, the sections that say cloud only do not apply.

Data Access Control

The organisation uses a password manager to ensure that strong and unique passwords are used by personnel. In general all passwords are stored in the encrypted vault of the password manager.

Use of Multi Factor Authentication is enforced for critical high risk systems.

Principle of Least Privilege is followed to make sure that people only have access to the data they need to access. Request for access, authorization and any changes to these are done through an IT service portal. The request is expected to be done by a senior personnel member or a manager. Requests are approved by IT. When employees leave the company, access to systems is revoked during an off-boarding process. A bi-annual access review is performed for all systems.

Secure software development practises

All code is regularly scanned for vulnerabilities using Snyk. All code changes are reviewed by at least one other software engineer and all changes are introduced via pull requests.

All code changes are tested both programmatically and manually.

Awareness and training

IT policies are documented and easily discoverable by personnel. Regular sessions are organized for personnel to make sure that personnel is aware of the requirements and expectations. Training is organized for all new employees as part of the on-boarding process.

Security Incident Management

We follow Atlassian's Security Incident Management Guidelines. In case of a security incident, we notify our customers via email, using the technical email address provided to us through Atlassian Marketplace. We also publish the security advisories publicly on help.refined.com.

Refined follows coordinated vulnerability disclosure model. This gives customers at least two weeks to take action before the security advisory is published publicly. On cloud, the customers don't generally need to take any action unless otherwise communicated.

Data transmission (cloud only)

Refined's Cloud Services follow best practises and recommendations for secure data transmission. All products ensure that traffic is encrypted at transit using minimum TLS 1.2 protocol.

We only use reliable cloud service providers who are certified and provide detailed information about compliance, processes and measures.

Cloud Incident Management (cloud only)

24/7 incident management process is in place to ensure that Refined's Cloud services are available and working as expected. Incident management process covers all Refined's Cloud Services. Process and responsibilities are documented.

Incident management process is automated where possible and confirmations and escalations are done by on-call engineers. Incidents are are visible on Refined's status page.