LOUPE DATA PROCESSING ADDENDUM

Version	2.0
Effective Date	For customers accepting the Agreement on or after publication of this DPA, the date of acceptance. For existing customers, 30 days after Gibraltar notifies the Customer Contact of the updated Terms (see Clause 1.1(l))
Supersedes	This version supersedes version 1.0 of the Gibraltar Software Data Processing Agreement, dated 20 June 2018.
Service	The hosted Loupe service, including app.onloupe.com, us.onloupe.com, europe.onloupe.com, hub.gibraltarsoftware.com and loupe.gibraltarsoftware.com

Version history

Version	Date	Summary
1.0	20 June 2018	Original GDPR Data Processing Agreement.
2.0	11 November 2026	Updated for the 2021 EU Standard Contractual Clauses, the UK International Data Transfer Addendum, the revised Swiss FADP, and US state privacy laws. Supersedes version 1.0.

This Data Processing Addendum ("DPA") is entered into between:

(1) Gibraltar Software, Inc., a Maryland corporation with its principal place of business at 4 Valleywood Court, Timonium, MD 21093, United States ("Gibraltar"); and

(2) the customer that has entered into the Agreement with Gibraltar, as identified in the Agreement, the applicable order or, where signed, the signature block below ("Customer").

This DPA forms part of, and is incorporated by reference into, the Loupe Cloud-Hosted Terms of Service at https://onloupe.com/about/loupe-service-terms-of-service/ (the "Agreement"). The current version of this DPA is published at https://onloupe.com/about/loupe-service-data-processing-addendum/. This DPA is accepted with the Agreement and is binding on both parties without signature, as set out in Clause 16.6.

1. Definitions and interpretation

1.1 Capitalised terms not defined in this DPA have the meanings given in the Agreement. In this DPA:

(a) "Applicable Data Protection Law" means all laws that apply to the processing of Customer Personal Data under the Agreement, including, where applicable: the EU GDPR; the UK GDPR and the UK Data Protection Act 2018 (each as amended, including by the Data (Use and Access) Act 2025); the Swiss Federal Act on Data Protection of 25 September 2020 ("FADP"); and US State Privacy Laws.

(b) "EU GDPR" means Regulation (EU) 2016/679. "UK GDPR" means the EU GDPR as it forms part of UK law.

(c) "Customer Personal Data" means personal data contained in Customer Data that Gibraltar processes on behalf of Customer in providing the Service. This includes log sessions and telemetry submitted by Customer's installations, Loupe user account data, and personal data that Customer provides in support requests ("Support Data").

(d) "EU SCCs" means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced.

(e) "UK Addendum" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under s.119A of the Data Protection Act 2018 (version B1.0, in force 21 March 2022), as revised from time to time.

(f) "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed by Gibraltar or its Sub-processors.

(g) "Service" means the hosted Loupe service provided by Gibraltar under the Agreement, including app.onloupe.com, us.onloupe.com, europe.onloupe.com, hub.gibraltarsoftware.com and loupe.gibraltarsoftware.com. Self-hosted Loupe Server installations operated by or for Customer are not part of the Service. However, Support Data that Customer sends to Gibraltar about any Loupe product is covered by this DPA. Gibraltar's marketing websites are not part of the Service.

(h) "Sub-processor" means any processor engaged by Gibraltar to process Customer Personal Data.

(i) "US State Privacy Laws" means the California Consumer Privacy Act as amended by the California Privacy Rights Act and its regulations ("CCPA"), and other US state consumer privacy laws to the extent they apply.

(j) "controller", "processor", "data subject", "personal data", "processing" and "supervisory authority" have the meanings given in Applicable Data Protection Law. Under the FADP, "controller" includes "controller" and "processor" includes "processor" as defined there. Under US State Privacy Laws, "controller" includes "business", and "processor" includes "service provider" and "contractor".

(k) "Customer Contact" means the billing contact that Customer maintains on my.onloupe.com or, if there is none, Customer's account owner.

(l) "Effective Date" means: (i) for a Customer that accepts the Agreement on or after the date this DPA is published, the date of that acceptance; and (ii) for a Customer whose Agreement was in force before that date, 30 days after the date on which Gibraltar notifies the Customer Contact of the updated Loupe Cloud-Hosted Terms of Service that incorporate this DPA.

1.2 Order of precedence. If there is a conflict, the following order applies: (a) the EU SCCs, the UK Addendum and the Swiss provisions in Clause 12, to the extent they apply; (b) this DPA; (c) the Agreement. On matters of data protection, this DPA prevails over the Agreement.

2. Scope and roles

2.1 Customer is the controller of Customer Personal Data, and Gibraltar is Customer's processor. Where Customer processes Customer Personal Data as a processor on behalf of its own controller(s), Gibraltar is Customer's sub-processor. In that case, Customer warrants that its controller has authorised Customer's instructions, including the appointment of Gibraltar. Customer remains Gibraltar's sole point of contact, unless the law requires otherwise.

2.2 Commercial relationship data is outside this DPA. Gibraltar processes certain personal data to run its commercial relationship with Customer, such as the names, email addresses and other contact details of Customer's purchasing, billing and administrative contacts, order, invoice and payment records (including through Gibraltar's payment provider), and correspondence about the Agreement. Gibraltar also sends its own announcements, such as news about new Loupe releases, to Loupe users who chose to subscribe to them; users added by Customer's administrators are not subscribed. Users can opt out at any time using the unsubscribe link in any announcement email or the Communication Preferences section of their profile on my.onloupe.com (https://my.onloupe.com/YourDetails). This does not affect service, security, billing or legal notices. For that data and those purposes Gibraltar acts as an independent controller, under the Loupe Cloud-Hosted Privacy Policy at https://onloupe.com/about/loupe-service-privacy-policy/. This processing is not processing on behalf of Customer, and it is not governed by this DPA. Gibraltar's service providers for that processing, including its payment provider, are not Sub-processors. Personal data that

Customer or its users submit to the Service, including Loupe user account data used to provide the Service, usage metadata (Clause 3.4) and Support Data, remains Customer Personal Data under this DPA.

2.3 Details of the processing (subject matter, duration, nature, purpose, types of personal data and categories of data subjects) are set out in Annex I.

3. Instructions and purpose limitation

3.1 Gibraltar will process Customer Personal Data only on Customer's documented instructions, including with regard to transfers to a third country, unless Union, Member State, UK, Swiss or other applicable law requires otherwise. In that case, Gibraltar will inform Customer of the legal requirement before processing, unless the law prohibits this on important grounds of public interest.

3.2 Customer's instructions are the Agreement, this DPA, Customer's configuration and use of the Service, and any further written instructions that the parties agree are consistent with the Agreement.

3.3 Gibraltar will immediately inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. Gibraltar may suspend the affected processing until the instruction is confirmed or modified.

3.4 Product analytics and aggregate statistics. Customer authorises Gibraltar to use (a) metadata about the use and operation of the Service, such as features used, pages viewed, session and event counts, data volumes, performance measurements and error rates, which may be linked to a Loupe user identifier ("usage metadata"), and (b) aggregate totals derived from that metadata, to maintain, secure and improve the Service. Usage metadata from the Loupe web application is processed by the product analytics Sub-processor listed in Annex III. Gibraltar will not use the content of log sessions or telemetry for this purpose. While usage metadata relates to an identifiable person, Gibraltar processes it as Customer Personal Data under this DPA. Only aggregate totals that are anonymised, so that they do not identify and cannot reasonably be used to identify Customer, any data subject or any device, are kept outside this DPA. Gibraltar will not attempt to re-identify them, will not use Customer Personal Data to build profiles of data subjects or to provide services to any other customer, and will not sell or share Customer Personal Data.

3.5 Customer controls what its applications log and send to the Service. Customer is responsible for the lawfulness of the Customer Personal Data and of its instructions, including having a lawful basis and giving any required notices to data subjects. Customer is also responsible for minimising the personal data its applications submit, by configuring its applications and the Loupe agent (including logging exclusions, the agent's anonymous mode where appropriate, and redaction rules). Customer will not configure its installations to submit special categories of personal data, criminal-offence data, payment card data or government identifiers unless the parties have agreed in writing. Gibraltar processes data as submitted by Customer's applications.

3.6 Customer-enabled integrations. Notifications and integrations that Customer enables and configures, such as Slack, Microsoft Teams and webhooks, send data to recipients that Customer chooses, on Customer's instructions. None is enabled by default. Those recipients are not Sub-processors, and their processing is governed by Customer's arrangements with them.

4. Gibraltar personnel

4.1 Gibraltar will ensure that every person it authorises to process Customer Personal Data (a) is bound by written confidentiality obligations or an appropriate statutory duty of confidentiality, (b) has access only as needed to perform the Service, and (c) has received appropriate data-protection and security instructions.

4.2 As of the date this version of the DPA was published, all Gibraltar personnel and contractors with access to Customer Personal Data are located in the United States. Gibraltar will notify the Customer Contact before authorising Gibraltar personnel or contractors to access Customer Personal Data from a country not previously disclosed in this DPA. Where that access is a restricted transfer, Gibraltar will ensure that an applicable transfer mechanism is in place. Contractors that act as Sub-processors remain subject to Clause 6.

5. Security

5.1 Gibraltar will implement and maintain the technical and organisational measures described in Annex II, which are designed to ensure a level of security appropriate to the risk, as required by Article 32 EU GDPR and UK GDPR and by Article 8 FADP.

5.2 Gibraltar may update Annex II from time to time, provided that the update does not materially reduce the overall level of protection of Customer Personal Data.

5.3 Customer is responsible for the security measures within its own control. These include protecting its account credentials and installation and API keys, deciding and limiting what its applications log and send to the Service, and managing which of its personnel have access to the Service.

6. Sub-processors

6.1 Customer gives Gibraltar general written authorisation to engage Sub-processors. The Sub-processors in use at the Effective Date are listed in Annex III. Gibraltar keeps the current list at https://onloupe.com/about/loupe-service-subprocessors/.

6.2 Gibraltar will impose on each Sub-processor, by written contract, data-protection obligations that are no less protective than those in this DPA, to the extent they apply to the services the Sub-processor provides. Gibraltar remains fully liable to Customer for each Sub-processor's performance of those obligations.

6.3 Gibraltar will give Customer at least 30 days' notice before a new Sub-processor (including a replacement) begins processing Customer Personal Data. Gibraltar will email the notice to the Customer Contact and will also post the change on the sub-processor page at https://onloupe.com/about/loupe-service-subprocessors/. Customer is responsible for keeping its Customer Contact current.

6.4 Customer may object to a new Sub-processor on reasonable data-protection grounds by notifying Gibraltar in writing within the 30-day notice period. The parties will discuss the objection in good faith. If they cannot resolve it within a reasonable time, Customer may terminate the affected Service by written notice, and Gibraltar will refund, on a pro-rata basis, any prepaid fees for the period after termination. This is Customer's sole remedy for an unresolved objection.

6.5 If a Sub-processor must be replaced urgently to protect the security or continuity of the Service, Gibraltar may make the replacement immediately and will notify Customer promptly afterwards. Customer's objection right under Clause 6.4 applies from that notice.

6.6 On request, Gibraltar will provide a copy of the data-protection terms it has with a Sub-processor, or a summary of them. Commercial information may be redacted.

7. Personal Data Breaches

7.1 Gibraltar will notify Customer of a Personal Data Breach without undue delay, and in any event within 48 hours after becoming aware of it.

7.2 The notice will include, to the extent known at the time: (a) the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned; (b) a contact point at Gibraltar; (c) the likely consequences; and (d) the measures taken or proposed to address the breach and mitigate its effects. Where not all of this information is available at once, Gibraltar will provide it in phases without undue further delay.

7.3 Gibraltar will take reasonable steps to contain, investigate and remediate the breach, and will cooperate with Customer so that Customer can meet its obligations to notify supervisory authorities and data subjects. Customer decides whether to make those notifications. Gibraltar will not notify a supervisory authority or data subject about a breach affecting Customer Personal Data unless Customer agrees or the law requires it.

7.4 Gibraltar will send notices under this Clause to the Customer Contact. Customer may contact Gibraltar about security and privacy at support@onloupe.com. A notice under this Clause is not an admission of fault or liability.

8. Data subject requests and assistance

8.1 If Gibraltar receives a request from a data subject relating to Customer Personal Data, it will promptly forward the request to Customer. Gibraltar will not respond to the data subject itself, except to direct them to Customer, unless Customer authorises a response.

8.2 Taking into account the nature of the processing, Gibraltar will help Customer, by appropriate technical and organisational measures and insofar as this is possible, to respond to requests by data subjects to exercise their rights. During the term, Customer can export and delete some individual items of data itself through the Service. For bulk export or bulk deletion, and where self-service is not available, Customer may send a written request to support@onloupe.com. On such a request, Gibraltar will: (a) export or delete session data sent to the Service by Customer's applications; (b) delete user records created within the Service; and (c) using the identifiers that Customer supplies, take reasonable steps to locate and delete or de-link session data and user records relating to the data subject concerned, taking into account the capabilities of the Service.

8.3 Gibraltar will give Customer reasonable assistance, taking into account the nature of processing and the information available to Gibraltar, with Customer's obligations under Articles 32 to 36 EU GDPR and UK GDPR (and the corresponding FADP provisions). This covers security, breach notification, data protection impact assessments and prior consultation with supervisory authorities. Gibraltar may charge reasonable fees for assistance that goes materially beyond its standard Service and documentation, if it notifies Customer in advance.

9. Information and audits

9.1 Gibraltar will make available to Customer all information necessary to demonstrate compliance with this DPA and Article 28 EU GDPR and UK GDPR. It will do this by providing this DPA and its Annexes, answering Customer's reasonable written security and privacy questionnaires (no more than once in any 12-month

period, except after a Personal Data Breach or at a supervisory authority's request), and providing relevant documentation.

9.2 If the information under Clause 9.1 is not sufficient to demonstrate compliance, or there are indications of non-compliance, Gibraltar will allow for and contribute to audits, including inspections, by Customer or an independent auditor mandated by Customer. Audits are subject to the following conditions: (a) at least 30 days' written notice, except after a Personal Data Breach or at a supervisory authority's request; (b) no more than once in any 12-month period, with the same exceptions; (c) during normal business hours, without unreasonable disruption, and in accordance with Gibraltar's reasonable security and confidentiality requirements; (d) any third-party auditor must be bound by confidentiality and must not be a Gibraltar competitor; (e) the audit may not give access to other customers' data; and (f) the audit is at Customer's cost. Gibraltar may charge for its time at reasonable rates notified in advance, unless the audit reveals a material breach of this DPA by Gibraltar.

9.3 Gibraltar may meet an audit request by remote review of documents and evidence where that is reasonably sufficient to demonstrate compliance.

9.4 Customer may also rely on the certifications and reports that Microsoft makes available for the Azure infrastructure, which cover the infrastructure layer of the Service.

9.5 Where the EU SCCs apply, the audit rights in Clause 8.9 of the EU SCCs will be exercised in accordance with this Clause 9, to the extent this does not conflict with the EU SCCs.

10. Government access requests

10.1 If a public authority asks Gibraltar to disclose Customer Personal Data, Gibraltar will: (a) attempt to redirect the authority to request the data directly from Customer; (b) promptly notify Customer, unless the law prohibits notification, in which case Gibraltar will use reasonable efforts to obtain a waiver; (c) review the legality of the request and challenge it where, after careful assessment, there are reasonable grounds to do so; and (d) disclose only the minimum information required by law, on a reasonable interpretation of the request.

10.2 Gibraltar will keep a record of such requests and of its responses, and will provide aggregate information about them to Customer on request, to the extent the law permits. As of the date this version of the DPA was published, Gibraltar had never received a government or law-enforcement request for Customer Personal Data.

11. Data location

11.1 Customer chooses the instance on which its log data is hosted. The US instance (us.onloupe.com) is hosted in Microsoft Azure US East 2. The EU instance (europe.onloupe.com) is hosted in Microsoft Azure West Europe.

11.2 Whichever instance Customer uses, Customer acknowledges that: (a) Loupe user account data is processed on hub.gibraltarsoftware.com, hosted in Azure US East 2; (b) Gibraltar personnel access the Service from the United States (Clause 4.2); (c) notification emails, which may contain excerpts from logs, are sent through the email Sub-processor listed in Annex III; (d) Support Data is processed in the support system listed in Annex III, which is hosted in the United States; and (e) usage metadata is processed by the product analytics Sub-processor listed in Annex III, in the United States. These activities involve transfers of personal data to the United States, which are covered by Clause 12.

11.3 Log data on the EU instance, and its backups, are stored only in Microsoft Azure regions within the EU.

11.4 Customer will not send special categories of personal data, or confidential, privileged or other sensitive personal data, through Gibraltar's support channels (including support tickets, email and attached files), except to the minimum extent necessary to resolve a support request. Where Customer needs to share logs for support, it should remove or redact personal data that is not needed first.

12. International transfers

12.1 Transfer mechanism. Transfers of Customer Personal Data to Gibraltar in the United States (or elsewhere outside the EEA, the UK or Switzerland, as applicable) are made under the EU SCCs, the UK Addendum and the Swiss provisions in this Clause 12.

12.2 EU transfers. For transfers subject to the EU GDPR, the EU SCCs are incorporated into this DPA by reference and completed as follows:

(a) Module Two (controller to processor) applies where Customer is a controller. Module Three (processor to processor) applies where Customer is a processor. Customer is the data exporter and Gibraltar is the data importer.

(b) Clause 7 (docking clause) applies.

(c) Clause 9(a): Option 2 (general written authorisation) applies, with a notice period of 30 days, as set out in Clause 6 of this DPA.

(d) Clause 11(a): the optional language does not apply.

(e) Clause 13: the competent supervisory authority is determined as set out in Annex I.C.

(f) Clause 17: Option 1 applies. The EU SCCs are governed by the law of Ireland.

(g) Clause 18(b): disputes are resolved by the courts of Ireland.

(h) Annexes I, II and III of the EU SCCs are completed by Annexes I, II and III of this DPA.

(i) Under Module Three, Gibraltar may notify Customer instead of the controller where the EU SCCs require notice to the controller, and Customer will pass the notice on to its controller as needed.

12.3 UK transfers. For transfers subject to the UK GDPR, the UK Addendum is incorporated into this DPA by reference. The EU SCCs, as completed under Clause 12.2, apply as modified by the UK Addendum, and the UK Addendum is completed as follows. Table 1: the parties' details are set out in Annex I.A. Table 2: the "Addendum EU SCCs" are the EU SCCs as incorporated and completed in Clause 12.2. Table 3: the Appendix Information is set out in Annexes I, II and III. Table 4: the Importer may end the UK Addendum as set out in its Section 19. Part 2 (Mandatory Clauses) of the Approved Addendum applies.

12.4 Swiss transfers. For transfers subject to the FADP, the EU SCCs apply as completed under Clause 12.2, with the following changes: (a) the Swiss Federal Data Protection and Information Commissioner ("FDPIC") is the competent supervisory authority for those transfers; (b) references to the EU GDPR are read as references to the FADP; (c) "Member State" in Clause 18(c) does not exclude data subjects whose habitual residence is in Switzerland from suing in their place of habitual residence; and (d) where a transfer is subject to both the FADP and the EU GDPR, the EU supervisory authority under Clause 12.2(e) remains competent for the GDPR aspects and the FDPIC for the FADP aspects.

12.5 Transfer assessments. Gibraltar will give Customer reasonable information about the laws and practices of the United States that apply to Gibraltar and its Sub-processors, and about Gibraltar's experience of public authority requests, so that Customer can carry out any transfer impact assessment or UK transfer risk assessment ("data protection test"). Gibraltar has assessed that it has no reason to believe these laws

prevent it from meeting its obligations under the EU SCCs. If that changes, it will notify Customer under Clause 14 of the EU SCCs.

12.6 Onward transfers and alternative mechanisms. Gibraltar will make onward transfers to Sub-processors only in accordance with Clause 6 and with the EU SCCs, UK Addendum and FADP, as applicable. If any mechanism in this Clause 12 is amended, replaced or invalidated, or a new mechanism becomes available (including new Commission standard contractual clauses or a Gibraltar certification under the Data Privacy Framework), the parties will rely on the replacement or new mechanism to the extent it is applicable and legally effective for the transfer and any required formalities have been completed, and Gibraltar may update this Clause 12 by notice to Customer to give effect to it.

13. Return and deletion

13.1 During the term, Customer Personal Data is retained for the retention periods that Customer configures in the Service.

13.2 On termination or expiry of the Service, Customer may, for 30 days, request a bulk export of its Customer Personal Data by writing to support@onloupe.com, and Gibraltar will provide the export on request. Customer may instead ask Gibraltar to delete its Customer Personal Data before that window ends. Within 30 days after the end of the export window, Gibraltar will delete Customer Personal Data from the Service, including its databases, queues and storage, and Loupe user accounts that are used only for Customer's subscription. Where a Loupe user account also belongs to another active subscription, Gibraltar removes the account's association with Customer's subscription and the Customer Personal Data held for it, and the account remains for that other subscription. Copies in backups are deleted as the backups expire, within 35 days after deletion from the Service. In any event, all Customer Personal Data in the Service, including backups, will be deleted no later than 95 days after the Service ends. Until then it remains protected under this DPA. On request, Gibraltar will confirm the deletion in writing.

13.3 Clause 13.2 does not apply to: (a) data that Gibraltar must retain by law; (b) the anonymised aggregate totals described in Clause 3.4; (c) Support Data: Customer instructs Gibraltar to retain Support Data as part of its support history for 3 years after the support ticket concerned is closed and then delete it, and Customer may instead choose at any time that it be deleted earlier, by writing to support@onloupe.com; and (d) usage metadata held by the product analytics Sub-processor: Customer instructs Gibraltar to retain it for 24 months after it is collected and then delete it, and Customer may instead ask at any time, including after the Service ends, that the usage metadata of its Loupe users be deleted, by writing to support@onloupe.com. Gibraltar will keep such retained data confidential, protect it under this DPA, and process it only for the purpose for which it is retained.

14. US State Privacy Laws

14.1 To the extent the CCPA or another US State Privacy Law applies, Gibraltar acts as Customer's service provider, contractor or processor in relation to Customer Personal Data. Customer discloses Customer Personal Data to Gibraltar only for these limited and specified business purposes: hosting and storing log data; authenticating users; analysing and displaying data; delivering notifications; customer support; security monitoring; and maintaining and improving the Service as described in Clause 3.4. Gibraltar will:

(a) not sell or share Customer Personal Data (as "sell" and "share" are defined in the CCPA);

(b) not retain, use or disclose Customer Personal Data for any purpose other than those business purposes (including any commercial purpose) or outside the direct business relationship with Customer, except as the CCPA permits a service provider to do;

(c) not combine Customer Personal Data with personal data it receives from or on behalf of others, or that it collects from its own interactions with consumers, except as the CCPA permits;

(d) comply with the US State Privacy Laws that apply to it, and provide the same level of privacy protection they require;

(e) notify Customer if it determines that it can no longer meet its obligations under them;

(f) allow Customer, on notice, to take reasonable and appropriate steps to ensure that Gibraltar uses Customer Personal Data consistently with Customer's obligations, and to stop and remediate unauthorised use (the steps include those in Clause 9);

(g) assist Customer with consumer requests as set out in Clause 8; and

(h) bind its Sub-processors by written contract to obligations consistent with this Clause 14.

14.2 Gibraltar certifies that it understands and will comply with the restrictions in this Clause 14.

15. Liability

15.1 Single aggregate cap. Each party's total liability arising out of or relating to this DPA, the EU SCCs and the UK Addendum (as between the parties) and the Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is subject to the limitations and exclusions of liability in the Agreement. All such liability counts toward, and is limited by, the single aggregate limitation of liability in the Agreement. This DPA does not create any separate, additional or increased limit.

15.2 Excluded losses. The exclusions of indirect, incidental, special, consequential and punitive damages, and of lost profits, revenue, goodwill and data (to the extent the Agreement excludes them), in the Agreement apply to liability under this DPA.

15.3 Fallback cap. If the Agreement does not set a monetary limit on a party's liability, that party's total aggregate liability arising out of or relating to this DPA and the Agreement will not exceed the fees paid or payable by Customer for the Service in the 12 months preceding the event giving rise to the claim. Where no fees were paid or payable in that period, including for free and trial subscriptions, that limit is zero (US$0), so that neither party has any such liability to the maximum extent permitted by law. In each case Clause 15.4 applies.

15.4 Mandatory carve-outs. Nothing in this DPA or the Agreement limits or excludes (a) the rights of data subjects, or either party's liability to data subjects, under the EU SCCs (including Clause 12), the UK Addendum or Applicable Data Protection Law, or (b) any liability that cannot lawfully be limited or excluded.

16. Term and general provisions

16.1 This DPA stays in force for as long as Gibraltar processes Customer Personal Data on Customer's behalf. Following termination of the Agreement, the obligations of this DPA continue to apply to any Customer Personal Data retained by Gibraltar until that data is deleted or otherwise lawfully ceases to be Customer Personal Data. This does not oblige Gibraltar to continue providing the Service.

16.2 Except as stated in Clause 12 (the EU SCCs are governed by the law and courts chosen in Clause 12.2, the UK Addendum by the laws of England and Wales, and the Swiss provisions as set out in Clause 12.4), this

DPA is governed by the laws of the State of Maryland, United States. Disputes under this DPA are subject to the exclusive jurisdiction of the state and federal courts located in Maryland, United States.

16.3 Gibraltar may update this DPA (a) to reflect changes in Applicable Data Protection Law or guidance from supervisory authorities, (b) under Clause 12.6, or (c) in any other way that does not materially reduce the protection of Customer Personal Data. Gibraltar will notify Customer of any material update at least 30 days before it takes effect, unless the law requires an earlier change. Any other amendment requires the written agreement of both parties.

16.4 If any provision of this DPA is invalid or unenforceable, the rest of the DPA remains in effect, and the provision will be modified to the minimum extent necessary to make it valid while keeping its intent.

16.5 Notices under this DPA may be given by email: to Gibraltar at support@onloupe.com, and to Customer at the email address of the Customer Contact.

16.6 Acceptance and signed copies. This DPA forms part of the Agreement and is accepted by Customer when it accepts the Agreement, including electronically. It is binding on both parties, including as to the EU SCCs and the UK Addendum incorporated in Clause 12, without any signature. A Customer that wants a signed copy may request one from support@onloupe.com. Gibraltar will provide a copy pre-signed by Gibraltar for Customer to countersign, and electronic signatures are valid. A signed copy does not change the terms of this DPA. Except for updates expressly permitted by Clauses 5.2, 6, 12.6 and 16.3, any amendment requires the written agreement of both parties in a document expressly amending this DPA.

Signatures

Signature is optional; see Clause 16.6.

Gibraltar Software, Inc.	**Customer**
Signature: _____	Legal entity name: _____
Name: Kendall Miller	Address: _____
Title: Chief Executive Officer	Name: _____
Date: _____	Title: _____
	Signature: _____
	Date: _____

Annex I: Parties and description of processing

A. List of parties

	Data exporter	Data importer
Name	Customer, as identified in the Agreement or in a signed copy of this DPA	Gibraltar Software, Inc.
Address	As stated in the Customer's account or in a signed copy of this DPA	4 Valleywood Court, Timonium, MD 21093, United States
Contact	The Customer Contact, or the signatory of a signed copy of this DPA	Kendall Miller, Chief Executive Officer; support@onloupe.com
Activities relevant to the transfer	Use of the Loupe Service to collect, store and analyse application logs and telemetry	Provision of the Loupe Service and related support
Role	Controller (Module Two) or processor (Module Three)	Processor (Module Two) or sub-processor (Module Three)
Signature and date	By acceptance of the Agreement, or signature of this DPA	By acceptance of the Agreement, or signature of this DPA

B. Description of processing / transfer

Categories of data subjects	End users of Customer's software whose activity, identifiers or devices appear in logs. Customer's employees and contractors who run software instrumented with Loupe. Customer's authorised users of the Service. Individuals named in Support Data (paying customers only).
Categories of personal data	Application log sessions and telemetry: user names and account identifiers, machine and host names, IP addresses, operating-system, environment and process details, timestamps, exception and stack-trace content, and any other data that Customer's developers choose to log. Loupe user account data, held on hub.gibraltarsoftware.com: the full name and email address of the user, as provided by them. Usage metadata from the Loupe web application (Clause 3.4), linked to a Loupe user identifier. Support Data: contact details, ticket content and attached logs.
Sensitive data	None intended (see Clause 3.5). Applied safeguards: the measures in Annex II, including encryption in transit and at rest and restricted, MFA-protected administrative access.
Frequency of transfer	Continuous, for as long as Customer's installations submit sessions and Customer uses the Service.
Nature of processing	Receiving, storing, indexing, analysing, displaying, sending notifications about, supporting, backing up and deleting log data. Product analytics from usage metadata and anonymised aggregate totals only, never from log content (Clause 3.4).
Purpose of processing	To provide, support, secure and improve the Loupe Service under the Agreement.
Retention	Customer-configured retention during the term; a 30-day window after termination in which Customer may request a bulk export; deletion within 30 days after that; backups gone within 35 days; everything in the Service deleted within 95 days (Clause 13.2). Support Data is kept for 3 years after the ticket is closed, then deleted, or earlier on Customer's request, and usage metadata is kept for 24 months, or deleted earlier on Customer's request, including after termination (Clause 13.3). Monitoring and diagnostic logs that Gibraltar keeps to operate the Service expire within 90 days (Annex II), within the 95-day limit.
Transfers to Sub-processors	As set out in Annex III, for the purposes and durations stated there.

C. Competent supervisory authority

EU transfers: the supervisory authority determined in accordance with Clause 13 of the EU SCCs. UK transfers: the Information Commissioner's Office. Swiss transfers: the FDPIC.

Annex II: Technical and organisational measures

Area	Measures
Hosting and infrastructure	The Service is hosted on Microsoft Azure: US instance and hub.gibraltarsoftware.com in Azure US East 2, and EU instance in Azure West Europe. It uses Azure SQL Database and Azure Service Bus. Physical and environmental security is provided by Microsoft under its data protection terms. Each customer's data is stored in its own dedicated Azure SQL database.
Encryption in transit	Connections to the Service, including session submission from Loupe agents and web and API access, are encrypted using TLS 1.2 or higher.
Encryption at rest	Customer Personal Data is encrypted at rest using Azure SQL Transparent Data Encryption and Azure disk and storage encryption, with Microsoft-managed keys.
Administrative access control	Production administrative access is restricted to a limited number of authorised personnel, currently two (the Chief Executive Officer and one senior engineer), all located in the United States. Administrative accounts are protected by multi-factor authentication.
Customer-side controls	The following controls are available to Customer: (a) individual named user accounts, with no shared logins; (b) Customer administrators add, remove and manage their own users; (c) per-repository and per-application agent keys, which Customer can rotate; (d) customer-configurable redaction rules in the Loupe agent, which are applied before data is sent to the Service; (e) the Loupe agent's anonymous mode, which Customer can enable to stop the agent collecting personal data it would otherwise record automatically (it does not remove personal data that Customer's applications deliberately log); (f) Customer-set data retention periods; and (g) self-service export and deletion of some individual items of data through the Service. Bulk export and bulk deletion are provided by Gibraltar on request to support@onloupe.com (Clauses 8.2 and 13.2).
Personnel	Background checks are carried out on personnel with access to Customer Personal Data. Personnel are bound by confidentiality obligations (Clause 4) and complete annual security awareness training.
Incident response	Gibraltar maintains an incident response plan covering detection, containment, investigation, remediation and notification. Personal Data Breaches are notified under Clause 7 (within 48 hours).
Backup and resilience	The Service uses Azure SQL Database automated backups, and restores are tested periodically. Backups are kept for no more than 35 days (Clause 13). Backups of the EU instance are stored only in Azure regions within the EU.
Patching	Servers receive automatic Windows updates.
Monitoring and logging	Azure Monitor, Log Analytics and Application Insights provide monitoring and alerting. Their logs and telemetry are retained for up to 90 days.
Assurance	Microsoft Azure's certifications and reports cover the infrastructure layer of the Service.
Sub-processors	Sub-processors are bound by written data-protection terms under Clause 6 (see Annex III).
Assistance to Customer	Data subject requests, and bulk export and deletion, are handled on request under Clauses 8.2 and 13.2.

Annex III: Sub-processors

List current as of the date this version of the DPA was published. The current list is maintained at https://onloupe.com/about/loupe-service-subprocessors/. Gibraltar's own service providers for its commercial relationship with Customer (for example, its payment provider) are not Sub-processors (Clause 2.2).

Sub-processor	Purpose and data	Location	Transfer safeguard / terms
Microsoft Corporation (Microsoft Azure)	Cloud hosting (compute, Azure SQL Database, Azure Service Bus, storage and networking) for us.onloupe.com and hub.gibraltarsoftware.com (Loupe user accounts for all customers)	United States: Azure US East 2 (Virginia)	Microsoft Products and Services Data Protection Addendum https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
Microsoft Corporation (Microsoft Azure)	Cloud hosting for the EU instance (europe.onloupe.com), including its backups	EU: Azure West Europe (Netherlands); backups stored in the EU	As above
Twilio Inc. (SendGrid)	Email delivery for notifications and alerts, which may contain log excerpts	United States	EU SCCs (and UK and Swiss equivalents) in the Twilio Data Protection Addendum https://www.twilio.com/en-us/legal/data-protection-addendum
Freshworks Inc. (Freshdesk)	Customer support ticketing for paying customers: Support Data, including any attached logs, retained for 3 years after the ticket is closed (see Clauses 11.4 and 13.3)	United States	EU SCCs in the Freshworks data protection terms, and/or Freshworks' EU-U.S. DPF certification (including the UK Extension and Swiss-U.S. DPF) https://www.freshworks.com/freshdesk/gdpr/
PostHog, Inc.	Product analytics of usage metadata from the Loupe web application (features used, pages viewed and timestamps, linked to a Loupe user identifier); never log content (Clause 3.4). Retained for 24 months, or deleted earlier on Customer's request (Clause 13.3)	United States (PostHog US Cloud)	EU SCCs (Module 2), UK Addendum and Swiss adaptations in the PostHog DPA, and PostHog's EU-U.S. DPF certification (including the UK Extension and Swiss-U.S. DPF) https://posthog.com/dpa