

**Functional Software, Inc.**

**Data Processing Addendum**

*(Custom clauses on Revision September 2021)*

Legal Name of Customer Entity:	<b>PagoPA S.p.A.</b>
--------------------------------	----------------------

This Data Processing Addendum (this “DPA”) is entered into and effective as of the last date of signature below by and between Functional Software, Inc. d/b/a Sentry (“Sentry”, “we”, or “us”) and the party named above (“Customer”, or “you”).

You have entered into one or more agreements with us (each, as amended from time to time, an “Agreement”) governing the provision of our real-time error tracking, crash reporting, application monitoring, and visibility service more fully described at [www.sentry.io](http://www.sentry.io) (the “Service”). This DPA will amend the terms of the Agreement to reflect the parties’ rights and responsibilities with respect to the processing and security of Customer Data (as defined below) under the Agreement. If you are accepting this DPA in your capacity as an employee, consultant or agent of Customer, you represent that you are an employee, consultant or agent of Customer, and that you have the authority to bind Customer to this DPA.

Any capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

**1. Definitions.** The following definitions apply to this DPA:

“Customer Data” means data you submit to, store on, or send to us via the Service.

“Data Incident” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data on systems that are managed and controlled by Sentry. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security, integrity, availability and/or confidentiality of Personal Data, including, without limitation, pings, port scans, or unsuccessful login attempts.

“Data Privacy Framework” means the set of rules set out by or otherwise stemming from the European Commission’s adequacy decision for the EU-U.S. of July 10, 2023, including the EU-U.S. DPF Principles, the Supplemental Principles, Annex I of the Principles and the list published at [dataprivacyframework.gov](http://dataprivacyframework.gov)

“Europe” means, for the purposes of this DPA, the member states of the European Economic Area, Switzerland and the United Kingdom.

“GDPR” 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 personal data and on the free movement of such data, and repealing Directive 95/46/EC.

“Notification Email Address” means the email address(es) set out in the last page of this DPA. Each party is solely responsible for ensuring that its own Notification Email Address is current and valid at all times.

“Personal Data” means any personal data or personal information (as those terms are defined by European Data Protection Legislation) contained within Customer Data.

“Privacy Laws” means the GDPR and any applicable data protection laws and regulations enacted in the EEA, Switzerland and the United Kingdom, including but not limited to the GDPR, the Italian Privacy Code (D. Lgs. 196/2003), as well as the orders, determinations, decisions, recommendations and guidelines of the EDPB/WP29, supervisory authorities and competent courts.

“Standard Contractual Clauses” or “SCCs” means (a) where the GDPR applies, the standard contractual clauses as approved by the European Commission pursuant to its decision 2021/914 of 4 June 2021 (“EU SCCs”); and (ii) where the UK GDPR applies, the standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR (“UK SCCs”).

“Subprocessor” means a third party that we use to process Customer Data in order to provide parts of the Service and/or related technical support. For the avoidance of doubt, the term Subprocessor shall not include Sentry employees or individual contractors.

“Term” means the term of the Agreement.

The terms “personal data”, “special categories of personal data”, “data subject”, “process”, “processing”, “controller”, “processor” and “supervisory authority” have the meanings given in Privacy Laws.

## **2. Data Processing.**

### **2.1 Roles and Regulatory Compliance; Authorization.**

2.1.1 *Scope of this DPA.* This DPA applies where and only to the extent Sentry processes Personal Data as a processor for the purposes of Privacy Laws.

2.1.2 *Roles and Responsibilities.* The parties acknowledge and agree as follows: (i) that Sentry will process the Personal Data as described in Annex I; (ii) that for the purposes of Privacy Laws, Sentry is a processor of Personal Data and Customer is the controller (or a processor acting on behalf of a third party controller); (iii) Sentry shall not retain, use or disclose Personal Data for any purpose other than the purposes described in this DPA, shall not “sell” Personal Data, and shall not use or further process Personal Data, even in a de-identified and aggregated form, for Sentry’ own business purposes, including but not limited to analytics, benchmarking, reporting, developing new products and services, and training and developing machine learning algorithms ; and (iv) that each of us will comply with our obligations under Privacy Laws with respect to the processing of Personal Data.

2.1.3 *Authorization by Third Party Controller.* If you are a processor of Personal Data acting on behalf of a third party controller: (i) you warrant to us that your instructions and actions with respect to that Personal Data, including your appointment of Sentry as another processor, have been authorized by the relevant controller; and (ii) you will serve as our sole point of contact and where we would otherwise be required (including for the purposes of the Standard Contractual Clauses) to provide information, assistance or cooperation to or seek authorization from any such third party controllers, we may provide such information, assistance or cooperation to or seek such authorization from you.

### **2.2 Customer responsibilities.**

2.2.1 *Customer Authorization.* Sentry shall process Personal Data in accordance with Customer’s documented lawful instructions. By entering into this DPA, you hereby authorize and instruct us to process Personal Data: (i) to provide the Service, and related technical support; (ii) as otherwise permitted or required by your use of the Service and/or your requests for technical support; (iii) as otherwise permitted or required by the Agreement, including this DPA; and (iv) as further documented in any other written instructions that are agreed by the parties. We will not process Personal Data for any other purpose, unless required to do so by applicable law or regulation. The parties agree that the Agreement (including this DPA), and your use of the Service in accordance with the Agreement, set out your complete and final processing instructions and any processing outside the scope of these instructions (if any) shall require prior written agreement between the parties. Customer shall ensure its instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate Privacy Laws. Notwithstanding the foregoing, if you are a processor of Personal Data acting on behalf of a third party controller then where legally required we are entitled to follow the instructions of such third party controllers with respect to their Personal Data.

2.2.2 *Prohibition on Sensitive Data.* You will not submit, store, or send any sensitive data or special categories of personal data (collectively, “Sensitive Data”) to us for processing, and you will not permit nor authorize any of your employees, agents, contractors, or data subjects to submit, store, or send any Sensitive Data to us for processing. You acknowledge that we do not request or require Sensitive Data as part of providing the Service to you, that we do not

wish to receive or store Sensitive Data, and that our obligations in this DPA will not apply with respect to Sensitive Data.

### **3. Deletion.**

3.1 Deletion During Term. We will enable you to delete Personal Data during the Term in a manner that is consistent with the functionality of the Service. If you use the Service to delete any Personal Data in a manner that would prevent you from recovering Personal Data at a future time, you agree that this will constitute an instruction to us to delete Personal Data from our systems in accordance with our standard processes and applicable law. We will comply with this instruction as soon as reasonably practicable, but in all events in accordance with applicable law.

3.2 Deletion upon termination. In any case of termination of the Agreement (including this DPA) , we will securely destroy any Personal Data in our possession or control. This requirement will not apply to the extent that we are required by applicable law to retain some or all of the Personal Data, in which event we will isolate and protect the Personal Data from further processing and delete in accordance with Sentry's deletion practices, except to the extent required by law. Sections 4.7 and 11.3 of the MSA will apply.

### **4. Data Security.**

4.1 Security Measures. We will implement and maintain appropriate technical and organizational measures to protect Personal Data against Data Incidents and to preserve the security, integrity and confidentiality of Personal Data, as described in Annex II (collectively, the "Security Measures"). Sentry shall ensure that any person who is authorized by Sentry to process Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). Customer acknowledges that Security Measures are subject to technical progress and development and that accordingly we may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service.

4.2 Data Incidents. Upon becoming aware of a Data Incident, we will notify you within 48 (forty-eight) hours and in any case without undue delay, and will take reasonable steps to minimize harm and secure Personal Data. Any notifications that we send you pursuant to this Section 4.2 will be sent to your Notification Email Address and will describe, to the extent possible and/or known to Sentry, the details of the Data Incident, the steps we have taken to mitigate the potential risks, and any suggestions we have for you to minimize the impact of the Data Incident. We will not assess the contents of any Personal Data in order to identify information that may be subject to specific legal requirements. You are solely responsible for complying with any incident notification laws that may apply to you, and to fulfilling any third-party notification obligations related to any Data Incident(s). Our notification of or response to a Data Incident under this Section will not constitute an acknowledgement of fault or liability with respect to the Data Incident.

4.3 Your Security Responsibilities. You agree that, without prejudice to our obligations under Sections 4.1 or 4.2: (i) you are solely responsible for your use of the Service, including making appropriate use of the Service to ensure a level of security appropriate to the risk in relation to Customer Data, securing any account authentication credentials, systems, and devices you use to use the Service. You understand and agree that we have no obligation to protect Customer Data that you elect to store or transfer outside of our or our Subprocessors' systems (e.g., offline or on-premise storage). You are solely responsible for evaluating whether the Service and our commitments under this Section 4 meet your needs, including with respect to your compliance with any of your security obligations under Privacy Laws, as applicable.

#### **4.4 Audit Rights.**

4.4.1 Audit Reports. You acknowledge that Sentry is regularly audited against various information security standards by independent third-party auditors and internal auditors, respectively. Upon request, we shall supply (on a confidential basis) a summary copy of our audit report(s), so that you can verify our compliance with the audit standards against which it has been assessed, and this DPA. Further, we will provide written responses (on a confidential basis) to all reasonable requests for information necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year, except if required by a competent data protection authority.

4.4.2 *Independent Audits.* While it is the parties' intention to rely ordinarily on the provision of the above audit report(s) to verify our compliance with this DPA, we will allow an internationally-recognized independent auditor that you select to conduct audits to verify our compliance with our obligations under this DPA. You must send any requests for audits under this Section 4.4.2 to legal@sentry.io. Following our receipt of your request, the parties will discuss and agree in advance on the reasonable start date, scope, duration, and security and confidentiality controls applicable to the audit. You will be responsible for any costs associated with the audit. You agree not to exercise your audit rights under this Section 4.4.2 more than once in any twelve (12) calendar month period, except (i) if and when required by a competent data protection authority; or (ii) an audit is necessary due to a Data Incident. You agree that (to the extent applicable), you shall exercise any audit rights under Privacy Laws and the Standard Contractual Clauses by instructing us to comply with the measures described in this Section 4.4.

## 5. **Data Subject Rights; Data Export.**

5.1 Access; Rectification; Restricted Processing; Portability. You acknowledge that the Service may, depending on the functionality of the Service, enable you to: (i) access the Customer Data; (ii) rectify inaccurate Customer Data; (iii) restrict the processing of Customer Data; (iv) delete Customer Data; and (v) export Customer Data.

5.2 Cooperation; Data Subjects' Rights. To the extent that you cannot access the relevant Personal Data within the Service, we will provide you, with all reasonable and timely assistance to enable you to respond to: (i) requests from data subjects who wish to exercise any of their rights under applicable Privacy Laws; and (ii) any other correspondence, enquiry or complaint received from a data subject, supervisory authority or other third party in connection with the processing of the Customer Data. In the event that any such request, correspondence, enquiry or complaint is made directly to us, we will promptly inform you of it, and provide you with as much detail as reasonably possible, before responding. Sentry reserves the right to reimbursement from Customer for the reasonable cost of any expenditures incurred in connection with such assistance, provided that such expenditures are agreed in writing beforehand between the parties.

## 6. **Data Transfers.**

6.1 Data Storage and Processing Facilities. You agree that we may, subject to Section 6.2, store and process Customer Data in the United States and any other country in which we or our Subprocessors maintain data processing operations, solely as strictly necessary to provide the Service and related support to Customer. Sentry shall ensure that such transfers are made in compliance with applicable Privacy Laws and this DPA.

6.2 Transfers of Data out of Europe. If the storage and/or processing of Personal Data as described in Section 6.1 involves a transfer of Personal Data to Sentry outside of Europe (collectively, "**Transferred Personal Data**"), then (i) the Standard Contractual Clauses shall be incorporated into and form a part of this DPA in accordance with Section 6.3; and (ii) for so long as Sentry is enrolled in the Data Privacy Framework we shall process Transferred Personal Data in compliance with the EU-U.S. DPF Principles. With respect to Transferred Personal Data, you agree that if we adopt an alternative data transfer mechanism (including any new version of, or successor to, the Standard Contractual Clauses or Data Privacy Framework adopted pursuant to applicable Privacy Laws) for Transferred Personal Data not described in this DPA ("**Alternative Transfer Solution**"), the Alternative Transfer Solution shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Solution complies with applicable Privacy Laws and extends to the territories to which Transferred Personal Data is transferred), and if we request that you take any action (including, without limitation, execution of documents) reasonably required to give full effect to that solution, you will promptly do so.

6.3 Standard Contractual Clauses. For the purposes of the Standard Contractual Clauses, the parties agree that (i) Sentry is the "data importer" and you are the "data exporter"; (ii) the EU SCCs shall be incorporated in the form attached hereto and the UK SCCs shall be incorporated by reference; (iii) the Annexes or Appendices of the EU SCCs and UK SCCs (as applicable) shall be populated with the information from Annexes I, II and III of this DPA; and (iv) the EU SCCs shall be governed by the laws of the Republic of Ireland and the UK SCCs shall be governed by the laws of England and Wales. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA), the Standard Contractual Clauses shall prevail to the extent of such conflict. In particular, nothing in the DPA shall exclude the rights of third-party beneficiaries granted under the Standard Contractual Clauses. You agree that in the event we cannot ensure compliance with the Standard

Contractual Clauses, we will inform you promptly and you will provide us with a reasonable period of time to cure any non-compliance. You will reasonably cooperate with us to agree what additional safeguards or measures, if any, may be reasonably required to cure the non-compliance and will only be entitled to suspend the transfer of Personal Data and/or terminate the affected parts of the Service if we have not or cannot cure the non-compliance before the end of the cure period.

## **7. Subprocessors.**

7.1 Consent to Engagement. You authorize us to engage third parties as Subprocessors. Whenever we engage a Subprocessor, we will enter into a contract with that Subprocessor which imposes data protection terms that require the Subprocessor to protect Personal Data to an equivalent standard required under this DPA, and we shall remain responsible for the Subprocessor's compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause us to breach any of our obligations under this DPA.

7.2 List of Subprocessors. A list of our current Subprocessors is set out in Annex III. We may update the list of Subprocessors upon thirty (30) days' prior written notice to you, during which period you will have the opportunity to object as described in Section 7.3 below. Sentry will make it available to Customer upon request any information on Personal Data processed, location of processing activities, data retention and security measures adopted by, including the name, address, and role of each Subprocessor, along with any other information as necessary to allow Customer to assess their adequacy with regard to the level of protection of Personal Data required by this DPA.

7.3 Objections; Sole Remedy. During the thirty (30) day period beginning on the date we notify you of any new or replacement Subprocessor, you have the right to object to the appointment of that Subprocessor on reasonable grounds that the Subprocessor does not or cannot comply with the requirements set forth in this DPA or Privacy Laws (each, an "**Objection**"). If we do not remedy or provide a reasonable workaround for your Objection within a reasonable time, you may, as your sole remedy and our sole liability for your Objection, terminate the Agreement for your convenience, and without further liability to either party. We will not owe you a refund of any fees you have paid in the event you decide to terminate the Agreement pursuant to this Section.

7.4 Disclosure of Subprocessor agreements. You agree that by complying with this Section 7, we fulfil our obligations under Clause 9(a) and (b) of the Standard Contractual Clauses. You further acknowledge that, for the purposes of Clause 9(c) of the Standard Contractual Clauses, we may be restricted from disclosing Subprocessor agreements to you (or the relevant third party controller) due to confidentiality restrictions. Notwithstanding this, we shall use reasonable efforts to require Subprocessors to permit us to disclose Subprocessor agreements to you and, in any event, will provide (upon request and on a confidential basis) all information we reasonably can in connection with such Subprocessor agreement. Pursuant to this Section, we will notify and you have the opportunity to object to any material downgrade of the level of data protection provided by our Subprocessors.

**8. Additional Information.** You acknowledge that we are required under Privacy Laws (i) to collect and maintain records of certain information, including, among other things, the name and contact detail of each processor and/or controller on whose behalf we are acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (ii) to make such information available to the supervisory authorities. Accordingly, to the extent that Privacy Laws apply to the processing of Personal Data, you will, when requested, provide this additional information to us, and ensure that the information is kept accurate and up-to-date.

## **9. Impact Assessments.**

9.1 We will provide you with reasonable and timely assistance as you may require in order to conduct a data protection impact assessment and, if necessary, consult with the relevant data protection authority.

9.2 Prior to the execution of this DPA, the parties conducted the transfer impact assessment provided by Clause 14 of the SCCs and concluded that the laws and practices of the third country of destination, along with the safeguards put in place by Sentry, do not in practice prevent the parties from fulfilling their obligations under the SCCs with regard to transfers of personal data outside of the EU, and are compatible with the commitments required by Article 46 of the GDPR regarding the transfer tools. As long as processing of Personal Data by Sentry while providing the Service implies a transfer of such Personal Data, as authorized by Customer in accordance with this DPA, the parties agree to maintain and update the Transfer Impact Assessment.

10. **Miscellaneous.** With the exception of the third-party beneficiary rights granted (where applicable) under the Standard Contractual Clauses, there are no third-party beneficiaries to this DPA. Except as expressly provided herein, nothing in this DPA will be deemed to waive or modify any of the provisions of the Agreement, which otherwise remains in full force and effect. Specifically, nothing in this DPA will affect any of the terms of the Agreement relating to Sentry's limitations of liability, which will remain in full force and effect. Notwithstanding the foregoing, in no event shall either party exclude or limit its liability with respect to any data subject's rights under Privacy Laws or the Standard Contractual Clauses. If you have entered into more than one Agreement with us, this DPA will amend each of the Agreements separately. In the event of a conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA will control. This DPA amends and supersedes any prior data processing addendum or similar agreement regarding its subject matter.

11. **Change in Privacy Laws.** Notwithstanding anything to the contrary in the Agreement (including this DPA), in the event of a change in Privacy Laws affecting this DPA or the lawfulness of any processing activities under this DPA, we reserve the right to make any amendments to this DPA as are reasonably necessary to ensure continued compliance.

IN WITNESS WHEREOF, the parties cause this DPA to be signed by their duly authorized representatives as set out below.

**FUNCTIONAL SOFTWARE, INC. DBA SENTRY**  
Signature: DocuSigned by:  
Justin Elrod  
8558512A59964A3...  
Name: Justin Elrod  
Title: Director of Sales  
Date: 3/11/2024

**CUSTOMER**  
Signature: DocuSigned by:  
Marta Colonna  
8B440B8E74024A8...  
Name: Marta Colonna  
Title: Chief Legal & Compliance Officer  
Date: 3/11/2024

Notification Email Address: [REDACTED]

Notification Email Address: [REDACTED]



## Standard Contractual Clauses

### MODULE TWO: Transfer Controller to Processor MODULE THREE: Transfer Processor to Processor

#### SECTION I

##### *Clause 1*

##### ***Purpose and scope***

- a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 personal data and on the free movement of such data (General Data Protection Regulation)<sup>1</sup> for the transfer of personal data to a third country.
- b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- c) have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- d) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- e) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### *Clause 2*

##### ***Effect and invariability of the Clauses***

- a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

##### *Clause 3*

##### ***Third-party beneficiaries***

- a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
  - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 - Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Clause 18(a) and (b).
- b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

##### *Clause 4*

---

1

***Interpretation***

- a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, 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.
- c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5***

***Hierarchy***

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

***Clause 6***

***Description of the transfers***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7 - Optional***

***Docking clause***

- a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II - OBLIGATIONS OF THE PARTIES**

***Clause 8***

***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**MODULE TWO: Transfer Controller to Processor**

**8.1 Instructions**

- a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data



is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

- a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.
- d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer 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 (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>2</sup> (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

---

2

- a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.
- d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### **MODULE THREE: Transfer processor to processor**

#### **8.1 Instructions**

- a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

#### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

- a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to

encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.
- d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

#### **8.7 Sensitive data**

Where the transfer 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 (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

#### **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>3</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### **8.9 Documentation and compliance**

- a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
- b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

---

3

- f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*  
***Use of sub-processors***

**MODULE TWO: Transfer Controller to Processor**

- a) **OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**MODULE THREE: Transfer processor to processor**

- a) **OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*  
***Data subject rights***

**MODULE TWO: Transfer Controller to Processor**

- a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

**MODULE THREE: Transfer processor to processor**

- a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

*Clause 11*  
**Redress**

- a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*  
**Liability**

- a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

- e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*  
***Supervision***

- a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY  
PUBLIC AUTHORITIES**

*Clause 14*  
***Local laws and practices affecting compliance with the Clauses***

- a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>4</sup>;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

**MODULE TWO: Transfer Controller to Processor**

- e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract,

insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

### **MODULE THREE: Transfer processor to processor**

- e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.
- f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 15*

#### *Obligations of the data importer in case of access by public authorities*

### **15.1 Notification**

- a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

*(module three: The data exporter shall forward the notification to the controller.)*

- b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc.). *(module three: The data exporter shall forward the information to the controller.)*
- d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent suspensory authority on request.
- e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### **15.2 Review of legality and data minimisation**

- a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. *(module three: The data exporter shall make the assessment available to the controller.)*

- c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV - FINAL PROVISIONS**

##### *Clause 16*

##### ***Non-compliance with the Clauses and termination***

- a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority (*module three* – and the controller of) such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

##### *Clause 17*

##### ***Governing law***

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Italy.

##### *Clause 18*

##### ***Choice of forum and jurisdiction***

- a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b) The Parties agree that those shall be the courts of the Republic of Ireland.
- c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d) The Parties agree to submit themselves to the jurisdiction of such courts.



## Annex I

### **A. List of Parties**

#### ***Data exporter(s):***

Name: Customer (as defined in the DPA)

Address: Customer's address (as specified in the Agreement)

Contact person's name, position and contact details: Customer's contact details (as specified in the DPA)

Role (controller/processor): Controller/processor

#### ***Data importer(s):***

Name: Functional Software, Inc. d/b/a Sentry

Address: 45 Fremont Street, 8th Floor, San Francisco, CA 94105

Contact person's name, position and contact details: Virginia Badenhope, General Counsel, legal@sentry.io

Role (controller/processor): Processor

### **B. Data Processing Description**

Subject Matter: Sentry's provision of the Service to Customer, and related technical support.

Purpose of the Processing: Sentry will process personal data submitted to, stored on, or sent via the Service for the purpose of providing the Service and related technical support in accordance with this DPA.

Categories of Data Subjects: The personal data transferred concern the following categories of data subjects:

- End users of the Service
- Individuals whose personal data is supplied by end users of the Service.

Categories of Personal Data: The personal data transferred concern the following categories of data:


- Direct identifying information (e.g. name, email address, telephone)
- Indirect identifying information (e.g. job title, gender, date of birth)
- Device identification data and traffic data (e.g. IP addresses, MAC addresses, web logs, browser agents)
- Any personal data supplied by end users of the Service

Sensitive Data: The personal data transferred to Sentry through the Service is determined and controlled by Customer. As such, Customer controls the content of the personal data transferred to Sentry and is solely responsible for ensuring the legality of the categories of data it may choose to transfer to Sentry. The DPA includes an express prohibition on the transfer of special categories of personal data to Sentry.

Frequency of the Transfer: Continuous

Nature of the Processing: Sentry will perform the following basic processing activities: processing to provide the Service in accordance with the Agreement; processing to perform any steps necessary for the performance of the Agreement; and processing to comply with other reasonable instructions provided by Customer (e.g. via email) that are consistent with the terms of the Agreement.

Period for which the personal data will be retained: Throughout the Term of the Agreement plus the period from expiry of the Term until deletion of Personal Data by Sentry in accordance with the Agreement.



**C. Competent Supervisory Authority**

The Irish Data Protection Commissioner.

## Annex II

### Security Measures

Technical and Organizational Measures	Relevant Section(s) of Sentry’s Security Policy (see below)
Measures of pseudonymization and encryption of personal data	<ul style="list-style-type: none"> <li>● Data Flow – Data into System</li> <li>● Data Flow – Data through System</li> <li>● Data Security and Privacy – Data Encryption</li> <li>● Data Security and Privacy – PII Scrubbing</li> </ul>
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<ul style="list-style-type: none"> <li>● Infrastructure and Network Security – Physical Access Control</li> <li>● Infrastructure and Network Security – Logical Access Control</li> <li>● Application Security – Two-Factor Authentication</li> <li>● Application Security – Single Sign-On</li> <li>● Application Security – SAML 2.0</li> <li>● Application Security – REST API Authentication (API Key)</li> <li>● Application Security – Audit Controls</li> </ul>
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	<ul style="list-style-type: none"> <li>● Infrastructure and Network Security – Intrusion Detection and Prevention</li> <li>● Business Continuity and Disaster Recovery</li> <li>● Corporate Security – Contingency Planning</li> <li>● Corporate Security – Vulnerability Disclosure</li> </ul>
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	<ul style="list-style-type: none"> <li>● Infrastructure and Network Security – Penetration Testing</li> <li>● Infrastructure and Network Security – Third-Party Audit</li> <li>● Corporate Security – Risk Management</li> <li>● Corporate Security – Security Policies</li> </ul>
Measures for user identification and authorization	<ul style="list-style-type: none"> <li>● Infrastructure and Network Security – Logical Access Control</li> <li>● Application Security – Two-Factor Authentication</li> <li>● Application Security – Single Sign-On</li> <li>● Application Security – SAML 2.0</li> <li>● Application Security – REST API Authentication (API Key)</li> <li>● Application Security – Audit Controls</li> </ul>
Measures for the protection of data during transmission	<ul style="list-style-type: none"> <li>● Data Flow – Data Through System</li> </ul>
Measures for the protection of data during storage	<ul style="list-style-type: none"> <li>● Data Security and Privacy – Data Encryption</li> </ul>
Measures for ensuring physical security of locations at which personal data are processed	<ul style="list-style-type: none"> <li>● Infrastructure and Network Security – Physical Access Control</li> </ul>
Measures for ensuring events logging	<ul style="list-style-type: none"> <li>● Application Security – Audit Controls</li> </ul>
Measures for ensuring system configuration, including default configuration	<ul style="list-style-type: none"> <li>● Application Security – Secure Application Development (Application Development Lifecycle)</li> <li>● Corporate Security – Risk Management</li> <li>● Corporate Security – Security Policies</li> </ul>
Measures for internal IT and IT security governance and management	<ul style="list-style-type: none"> <li>● Security and Compliance</li> <li>● Infrastructure and Network Security – Third-Party Audit</li> <li>● Corporate Security – Risk Management</li> </ul>
Measures for certification/assurance of processes and products	<ul style="list-style-type: none"> <li>● Infrastructure and Network Security – Third-Party Audit</li> <li>● Corporate Security – Risk Management</li> </ul>

Technical and Organizational Measures	Relevant Section(s) of Sentry’s Security Policy (see below)
Measures for ensuring data minimization	<ul style="list-style-type: none"> <li>● Data Security and Privacy – Data Retention</li> <li>● Data Security and Privacy – Data Removal</li> </ul>
Measures for ensuring data quality	<ul style="list-style-type: none"> <li>● Data Flow – Data Through System</li> <li>● Data Security and Privacy – Data Encryption</li> <li>● Application Security – Audit Controls</li> <li>● Sentry maintains an online form to allow data subjects to request a copy of their personal data, make changes to their personal data or request deletion of their personal data</li> </ul>
Measures for ensuring limited data retention	<ul style="list-style-type: none"> <li>● Data Security and Privacy – Data Retention</li> <li>● Data Security and Privacy – Data Removal</li> </ul>
Measures for ensuring accountability	<ul style="list-style-type: none"> <li>● Corporate Security – Risk Management</li> <li>● Corporate Security – Security Policies</li> </ul>
Measures for allowing data portability and ensuring erasure	<ul style="list-style-type: none"> <li>● Sentry maintains an online form to allow data subjects to request a copy of their personal data, make changes to their personal data or request deletion of their personal data</li> </ul>
Measures and assurances regarding U.S. government surveillance (“Additional Safeguards”)	<ul style="list-style-type: none"> <li>● Sentry uses encryption both in transit and at rest.</li> <li>● As of the date of this DPA, Sentry has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.</li> <li>● No court has found Sentry to be the type of entity eligible to receive process issued under FISA Section 702: (i) an “electronic communication service provider” within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.</li> <li>● Sentry shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific “targeted selector” (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).</li> <li>● Sentry has not built – and undertakes not to build, for the duration of the Agreement and for the services provided to Customer - any backdoors or other methods into its Service to allow third parties to circumvent its security measures to gain access to Customer Data.</li> <li>● Sentry shall use all available legal mechanisms to challenge any demands for data access through national security process that Sentry receives, as well as any non-disclosure provisions attached thereto.</li> <li>● Sentry shall take no action pursuant to U.S. Executive Order 12333.</li> <li>● Sentry publishes a transparency report indicating the types of binding legal demands for the personal data it has received, including national security</li> </ul>

Technical and Organizational Measures	Relevant Section(s) of Sentry's Security Policy (see below)
	<p>orders and directives, which shall encompass any process issued under FISA Section 702.</p> <ul style="list-style-type: none"> <li>● Sentry will notify Customer if Sentry can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.</li> </ul>

## Sentry Security Policy

### **Security & Compliance**

Security and compliance are top priorities for Sentry because they are fundamental to your experience with the product. Sentry is committed to securing your application's data, eliminating systems vulnerability, and ensuring continuity of access.

Sentry uses a variety of industry-standard technologies and services to secure your data from unauthorized access, disclosure, use, and loss. All Sentry employees undergo background checks before employment and are trained on security practices during company onboarding and on an annual basis.

Security is directed by Sentry's Chief Technology Officer and maintained by Sentry's Security & Operations team.

### **Infrastructure and Network Security**

#### **Physical Access Control**

Sentry is hosted on Google Cloud Platform. Google data centers feature a layered security model, including extensive safeguards such as:

- Custom-designed electronic access cards
- Alarms
- Vehicle access barriers
- Perimeter fencing
- Metal detectors
- Biometrics

According to the Google Security Whitepaper: "The data center floor features laser beam intrusion detection. Data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are reviewed in case an incident occurs. Data centers are also routinely patrolled by professional security guards who have undergone rigorous background checks and training."

Sentry employees do not have physical access to Google data centers, servers, network equipment, or storage.

#### **Logical Access Control**

Sentry is the assigned administrator of its infrastructure on Google Cloud Platform, and only designated authorized Sentry operations team members have access to configure the infrastructure on an as-needed basis behind a two-factor authenticated virtual private network. Specific private keys are required for individual servers, and keys are stored in a secure and encrypted location.

#### **Penetration Testing**

Sentry undergoes annual penetration testing conducted by an independent, third-party agency. For testing, Sentry provides the agency with an isolated clone of sentry.io and a high-level diagram of application architecture. No customer data is exposed to the agency through penetration testing.

Information about any security vulnerabilities successfully exploited through penetration testing is used to set mitigation and remediation priorities. A summary of penetration test findings is available upon request to enterprise customers.

### **Third-Party Audit**

Google Cloud Platform undergoes various third-party independent audits regularly and can provide verification of compliance controls for its data centers, infrastructure, and operations. This includes, but is not limited to, SSAE 16-compliant SOC 2 certification and ISO 27001 certification. Sentry undergoes regular third-party independent audits on a regular basis and can provide its SOC-2 report upon request.

### **Intrusion Detection and Prevention**

Unusual network patterns or suspicious behavior are among Sentry's most significant concerns for infrastructure hosting and management. Sentry and Google Cloud Platform's intrusion detection and prevention systems (IDS/IPS) rely on both signature-based security and algorithm-based security to identify traffic patterns that are similar to known attack methods.

IDS/IPS involves tightly controlling the size and make-up of the attack surface, employing intelligent detection controls at data entry points, and developing and deploying technologies that automatically remedy dangerous situations, as well as preventing known threats from accessing the system in the first place.

Sentry does not provide direct access to security event forensics but does provide access to the engineering and customer support teams during and after any unscheduled downtime.

### **Business Continuity and Disaster Recovery**

#### **High Availability**

Every part of the Sentry service uses properly-provisioned, redundant servers (e.g., multiple load balancers, web servers, replica databases) in the case of failure. As part of regular maintenance, servers are taken out of operation without impacting availability.

#### **Business Continuity**

Sentry keeps hourly encrypted backups of data in multiple regions on Google Cloud Platform. While never expected, in the case of production data loss (i.e., primary data stores lost), we will restore organizational data from these backups.

#### **Disaster Recovery**

In the event of a region-wide outage, Sentry will bring up a duplicate environment in a different Google Cloud Platform region. The Sentry operations team has extensive experience performing full region migrations.

### **Data Flow**

#### **Data into System**

SDKs securely send events, containing information on errors and exceptions, to the Sentry server, which processes and stores the events. Audit data of processing and storing is transmitted to our in-house logging infrastructure through encrypted connections.

We believe SDKs should provide some mechanism for proactively scrubbing data, ideally through an extensible interface that the user can customize. Sentry provides documentation outlining SDK configuration to filter out bits of data for security and privacy purposes, but that otherwise delivers the rest of the event data intact. Scrubbing the following values is recommended:

- Values where the keyname matches password, passwd, or secret
- Values that match the regular expression of `r'^(?:\d[ -]*?){13,16}\$'` (credit card-like)
- Session cookies
- Authentication header (HTTP)

#### **Data through System**

Data is sent securely to Sentry via TLS to an HTTPS endpoint. All data is AES-256bit encrypted, both in transit and at rest. Sentry aggregates events along with contextual data related to the user's environment, preceding events, and the release and deployment changeset. Events data is also enriched with artifacts like source maps or symbols uploaded by the user or sourced externally.

Sentry's latest SSL Labs Report can be found [here](#).

### **Data out of System**

Once the event is processed, it can then be accessed via Sentry's user interface and REST APIs. Sentry integrates with a variety of third-party tools so developers can combine error data from Sentry with data from other systems, manage workflows efficiently, and be alerted of errors through notification and chat tools, in addition to email and SMS. Therefore, Sentry's high standards for security and compliance also extend to its partner network.

### **Data Security and Privacy**

#### **Data Encryption**

All data in Sentry servers is encrypted at rest. Google Cloud Platform stores and manages data cryptography keys in its redundant and globally distributed Key Management Service. So, if an intruder were ever able to access any of the physical storage devices, the Sentry data contained therein would still be impossible to decrypt without the keys, rendering the information a useless jumble of random characters.

Encryption at rest also enables continuity measures like backup and infrastructure management without compromising data security and privacy.

Sentry exclusively sends data over HTTPS transport layer security (TLS) encrypted connections for additional security as data transits to and from the application.

#### **Data Retention**

Sentry retains event data for 90 days by default, regardless of plan. We remove individual events after 90 days, and we remove aggregate issues after 90 days of inactivity. All event data and most metadata is eradicated from the service and from the server without additional archiving in order to prevent the threat of intrusion.

#### **Data Removal**

All customer data stored on Sentry servers is eradicated upon a customer's termination of service and deletion of account after a 24-hour waiting period to prevent accidental cancellation. Data can also be deleted upon request and via Sentry's REST API and UI.

Users have the ability to remove individual events via bulk delete of all events within an issue and can permanently remove data related to a given tag.

#### **PII Scrubbing**

We recommend that users do not send any personally identifiable information (PII) to Sentry. To mitigate accidents and other security risks, Sentry offers server-side filtering as a default setting. The Data Scrubber option in Sentry's settings ensures PII doesn't get sent to or stored on Sentry's servers, automatically removing values that appear to be sensitive information.

Additionally, users can specify values to be scrubbed in the Project Settings. IP Address storage can also be disabled. The latter is particularly important if you're concerned about PII and using Sentry's Browser JavaScript SDK.

### **Application Security**

#### **Two-Factor Authentication**

In addition to password login, two-factor authentication (2FA) provides an added layer of security to Sentry via a time-based one-time password algorithm (TOTP). We encourage 2FA as an important step towards securing data access from intruders. Sentry users can deploy universal second-factor devices like YubiKeys (which can also be used to confirm the sudo prompt), TOTP apps like Google Authenticator, or SMS as second factors. This also applies to sign-in with an SSO provider.

Sentry's organization list also displays who has 2FA enabled so users can vet their own organization's security.

#### **Single Sign-On**

Sentry's single sign-on (SSO) implementation prioritizes security. We aggressively monitor linked accounts and disable them with any reasonable sign that the account's access has been revoked. SSO also improves user experience by streamlining login and improving access from trusted domains. Sentry currently offers SSO via Google Apps for

Work and GitHub Organizations.

## **SAML 2.0**

To facilitate user authentication through the web browser and improve identity management, Sentry offers assertion markup language (SAML)-based SSO as a standard feature to customers on its Enterprise plan. SAML 2.0 enhances user-based security and streamlines signup and login from trusted portals to enhance user experience, access management, and auditability.

Sentry integrates with SAML 2.0 providers including OneLogin, Auth0, and Okta (as well as enhanced member administration and management on the Medium and Large plans via an integration with Rippling).

## **REST API Authentication (API Key)**

Sentry's REST API uses an auth token for authentication. Authentication tokens are passed using the auth header and are used to authenticate a user account with the API.

We strongly recommend using organization-wide authentication tokens.

## **Email Security**

The Sentry service includes email notifications and reports. Sender policy framework (SPF) is a system to prevent email address spoofing and minimize inbound spam. We have SPF records set through Dyn, our domain name service (DNS), and domain-based message authentication, reporting, and conformance (DMARC) set up for monitoring reports to prevent the possibility of phishing scams. Sentry users can see the TXT records on [dmarc.getsentry.com](https://dmarc.getsentry.com) and [md.getsentry.com](https://md.getsentry.com):

```
\$ dig \_dmarc.getsentry.com TXT +short
```

```
"v=DMARC1; p=none; pct=100; rua=mailto:re+tlipc5xia1x@dmarc.postmarkapp.com; sp=none; aspf=r;"
```

```
\$ dig md.getsentry.com TXT +short
```

```
"v=spf1 ip4:167.89.86.73 ip4:167.89.84.14 ip4:167.89.84.75 -all"
```

## **Audit Controls**

We know user administration is central to security and management, and auditing user logs is often the first step in both an emergency response plan and policy compliance requirements. All Sentry customers get admin controls governing identity, access, and usage to keep your data safe, secure, and centrally managed.

Membership within Sentry is handled at the organization level. The system is designed so each user has a singular account that can be reused across multiple organizations (even those using SSO). Each Sentry user should have their own account and can choose their own personal preferences and notifications settings. Access to organizations is dictated by role:

- Billing
- Member
- Admin
- Manager
- Organization Owner

For any organization on a Sentry plan, the project administration portal is the hub for seeing and managing users and usage. The member list includes the username, email, status, added date, teams, and role for each user. The admin or owner can revoke access by project, team, or org and change the user role. Additionally, the admin can request login and password history and revoke passwords and active sessions for any user via request to Sentry Support.

In the audit log, all of the actions by user and event within the Sentry UI (e.g., `member.invite`, `project.create`) are listed chronologically by time and IP address so you'll always have a view into your organization's most recent history.

## **Secure Application Development (Application Development Lifecycle)**



Sentry practices continuous delivery, which means all code changes are committed, tested, shipped, and iterated on in a rapid sequence. A continuous delivery methodology, complemented by pull request, continuous integration (CI), and automated error tracking, significantly decreases the likelihood of a security issue and improves the response time to and the effective eradication of bugs and vulnerabilities. Release notes and details for Sentry and its SDKs can be found on their respective GitHub release pages (e.g., Sentry releases and raven-js releases).

### **Corporate Security**

#### **Malware Protection**

At Sentry, we believe that good security practices start with our own team, so we go out of our way to protect against internal threats and local vulnerabilities. All company-provided workstations run FleetSmith for inventory management, which enables and enforces full-disk encryption, screen lock, and other security features.

#### **Risk Management**

Sentry follows the risk management procedures outlined in NIST SP 800-30, which include nine steps for risk assessment and seven steps for risk mitigation.

All Sentry product changes must go through code review, CI, and build pipeline to reach production servers. Only designated employees on Sentry's operations team have secure shell (SSH) access to production servers.

We perform testing and risk management on all systems and applications on a regular and ongoing basis. New methods are developed, reviewed, and deployed to production via pull request and internal review. New risk management practices are documented and shared via staff presentations on lessons learned and best practices.

Sentry performs risk assessments throughout the product lifecycle per the standards outlined in HIPAA Security Rule, 45 CFR 164.308:

- Before the integration of new system technologies and before changes are made to Sentry physical safeguards
- While making changes to Sentry physical equipment and facilities that introduce new, untested configurations
- Periodically as part of technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting security

#### **Contingency Planning**

The Sentry operations team includes service continuity and threat remediation among its top priorities. We keep a contingency plan in case of unforeseen events, including risk management, disaster recovery, and customer communication sub-plans that are tested and updated on an ongoing basis and thoroughly reviewed for gaps and changes at least annually.

#### **Security Policies**

Sentry maintains an internal wiki of security policies, which is updated on an ongoing basis and reviewed annually for gaps. An overview of specific security policies is available to Sentry enterprise customers upon request:

- Information Security
- Risk Management
- Security Incident Response
- Vulnerability Management
- Policy Management and Maintenance
- Data Request
- Change Management
- System Access

#### **Background Checks**

Sentry conducts background checks for all new hires, including verification on the following:

- Identity verification

- Global watchlist check
- National criminal records check
- County criminal records check
- (U.S. only) Sex offender registry check

### **Security Training**

All new employees receive onboarding and systems training, including environment and permissions setup, formal software development training (if pertinent), security policies review, company policies review, and corporate values and ethics training.

All engineers review security policies as part of onboarding and are encouraged to review and contribute to policies via internal documentation. Any change to policy affecting the product is communicated as a pull request, such that all engineers can review and contribute before internal publication. Major updates are communicated via email to all Sentry employees.

### **Disclosure Policy**

Sentry follows the incident handling and response process recommended by SANS, which includes identifying, containing, eradicating, recovering from, communicating, and documenting security events. Sentry notifies customers of any data breaches as soon as possible via email and phone call, followed by multiple periodic updates throughout each day addressing progress and impact. Sentry Enterprise plans include a dedicated customer success manager who holds responsibility for customer communication, as well as regular check-ins and escalations.

Sentry maintains a live report of operational uptime and issues on our status page. Anyone can subscribe to updates via email from the status page. Any known incidents are reported there, as well as on our Twitter feed.

### **Vulnerability Disclosure**

Anyone can report a vulnerability or security concern with a Sentry product by contacting [security@sentry.io](mailto:security@sentry.io) and including a proof of concept, a list of tools used (including versions), and the output of the tools. We take all disclosures very seriously, and once we receive a disclosure we rapidly verify each vulnerability before taking the necessary steps to fix it. Once verified, we periodically send status updates as problems are fixed.

To encrypt sensitive information that is sent to us, our PGP key can be found on keyservers with the fingerprint:

774A FA98 315A 9600 41C7 C17B F08D DBE4 DB76 8FBC


### **Other Resources**

#### **Compliance Certifications**

Sentry has obtained the following compliance certifications:

- SOC2 Type I
- SOC2 Type II
- HIPAA Attestation

Contact us for a copy of any report(s) you're interested in reading (It'll be less infuriating than your social feed.) If you already use Sentry, you can access the report via your Sentry account.



[Page left intentionally blank]

**Annex III**

**List of Subprocessors**

**Third Party**

<b>Name (full legal name)</b>	<b>Address:</b>	<b>Description of processing and purpose</b>	<b>Processing location</b>	<b>Data</b>	<b>Retention</b>
Amazon Web Services	410 Terry Avenue North - Seattle, WA 98109	Cloud infrastructure services	United States*	Customer Data	As set forth in the DPA
Google Cloud Platform	1600 Amphitheatre Parkway - Mountain View, CA 94043	Cloud infrastructure services	United States*	Customer Data	As set forth in the DPA
SendGrid	889 Winslow St. - Redwood City, CA 94063	Email delivery services	United States*	Email addresses	As set forth in the DPA

\* as of the effective date (last date of signature by and between Sentry and Customer). It is understood between the parties that Sentry intends to launch additional data regions that Customer may configure. Data residency options for Customer Data will be therefore under the control of Customer based on Customer's configuration of the Service and such choice will supersede the information contained herein.

**Affiliates**

<b>Name (full legal name)</b>	<b>Address:</b>	<b>Description of processing and purpose:</b>	<b>Processing location</b>	<b>Data</b>	<b>Retention</b>
Functional Software GmbH	Rothschildplatz 3 Top 3.02.AB 1020 Vienna Austria	Provides parts of the Service and related technical support	Austria	Customer Data	As set forth in the DPA
Sentry Software Canada Inc.	129 Spadina Ave, 7th Floor Toronto, ON M5V 2L3 Canada	Provides parts of the Service and related technical support	Canada	Customer Data	As set forth in the DPA

Sentry Software Netherlands B.V.	Schiphol Boulevard 359 WTC Schiphol Airport, D-Tower 11th floor 1118BJ Schiphol Netherlands	Provides parts of the Service and related technical support	Netherlands	Customer Data	As set forth in the DPA
-------------------------------------	---	---	-------------	---------------	-------------------------