
COMPLIANCE

Data Processing Agreement

For personal data. Explains how Safespring handles data on the customer's behalf, which instructions apply, and which sub-processors may be involved.

Version	1.0
ID	65d031118b1a
Prepared by	Safespring
Approver	Safespring
Date	2026-03-23
Classification	Public

This Data Processing Agreement (the “DPA”) between the Customer (below, the “Controller”) and Safespring AB (559075-0245) (below, the “Processor”) constitutes a part of the Agreement, under which the Processor will process personal data on behalf of the Controller when supplying the Service. The Controller is the data controller in relation to the processing of the Personal Data. The Processor is data processor.

This DPA applies only to Safespring’s processing of Personal Data on behalf of the Customer in its capacity as a data processor. Where and to the extent Safespring processes personal data in its capacity as a data controller (including for example for account administration, billing, marketing, security and compliance), such processing is not subject to this DPA and is instead governed by applicable data protection law and included in Safespring’s privacy policy as updated from time to time or as otherwise communicated by Safespring.

1. Documents

1.1 This DPA consists of this main document and Appendix 1, Instructions and Sub-Processors.

2. Definitions and interpretation

2.1 In this DPA, capitalized terms shall have the meanings set out below or if not defined herein, the meanings set forth in Applicable Legislation or the Agreement.

Applicable Legislation means

1. the GDPR and
2. any applicable supplementary legislation to the GDPR.

GDPR means Regulation (EU) 2016/679 of the European Parliament and the Council as amended, supplemented and/or varied from time to time.

Personal Data means the personal data (as defined in Applicable Legislation), specified in Appendix 1 hereto.

3. Instructions

3.1 The Processor shall process the Personal Data in accordance with Article 28(3) and the Controller’s written instructions set forth in Appendix 1.

3.2 The Processor may not process the Personal Data for any other purposes or in any other way than as instructed by the Controller from time to time. The Parties shall update Appendix 1 in the event of new or amended instructions.

3.3 Notwithstanding the above, the Processor may undertake reasonable day-to-day actions with the Personal Data without having received specific written instructions from the Controller, provided that the Processor acts for and within the scope of the purposes stated in Appendix 1.

3.4 In the event that the Processor considers that any instruction violates Applicable Legislation, the Processor shall refrain from acting on such instructions and shall promptly notify the Controller and await amended instructions.

4. The controller's obligation to process data lawfully

4.1 The Controller shall ensure that a legal ground recognized under Applicable Legislation applies for processing of the Personal Data. The Controller shall further meet all other obligations of a controller under Applicable Legislation.

4.2 The Controller's instructions for the processing of the Personal Data shall comply with Applicable Legislation. The Controller shall have sole responsibility for the accuracy, quality, and legality of the Personal Data and the means by which it acquired the Personal Data.

5. Security measures

5.1 The Processor shall maintain appropriate technical and organisational measures in accordance with Article 32 of the GDPR to ensure that the Personal Data is protected against destruction, modification and proliferation. The Processor shall further ensure that Personal Data is protected against unauthorized access and that access events are logged and traceable.

5.2 The Processor shall ensure

1. that only authorized employees have access to the Personal Data,
2. that the authorized employees process the Personal Data only in accordance with this DPA and the Controller's instructions and
3. that each authorized employee is bound by a confidentiality undertaking towards the Processor in relation to the Personal Data.

5.3 The Processor shall notify the Controller without undue delay and, where feasible, within 48 hours after becoming aware of a personal data breach. Such notification shall, where possible, at least contain the information described in Article 33.3 of the GDPR.

5.4 The Processor shall maintain an information security management system aligned with ISO 27001 or an equivalent standard.

6. The processor's obligations to assist

6.1 The Processor shall assist the Controller with the fulfilment of the Controller's obligation to ensure that the data subjects may exercise their rights under Applicable Legislation by ensuring appropriate technical and organizational measures. The Processor shall without undue delay and taking into account the nature of the processing further assist the Controller in relation to the Controller's obligations under Articles 32-36 of the GDPR.

7. Sub-processors

7.1 The Processor may engage third parties to process the Personal Data or any part thereof on its behalf ("Sub-Processor"). Where the Processor intends to engage a new Sub-Processor, the Controller must be informed thereof in writing. The new Sub-Processor may process the Personal Data if the Controller has not objected in writing 30 days after such information was provided. The absence of Controller's objections will be deemed as the Controller's acceptance of the change of Sub-Processor. Sub-Processors are listed in Appendix 1, which shall be updated in the event of changes to the Sub-Processors.

7.2 The Processor shall enter into a written agreement with every Sub-Processor, in which each Sub-Processor undertakes obligations at least reflecting those undertaken by the Processor under this DPA. The Processor is responsible towards the Controller for its Sub-Processors' acts and omissions as for its own.

7.3 In the event the Controller objects to a new Sub-Processor in accordance with Section 7.1, the Processor shall use reasonable efforts to offer an alternative or suggest a commercial reasonable change in the Service or the Controller's configuration to prevent processing of Personal Data by the objected Sub-Processor. If no practical or commercially reasonable solution is possible according to the Processor, the Processor shall notify the Controller accordingly and, the Controller may terminate the relevant agreement, solely in respect of the affected Service, by giving written notice no later than forty-five (45) days following receipt of such notification, failing which the Controller shall be deemed to have accepted the use of the relevant Sub-Processor.

who may terminate the relevant agreement with respect for any affected Service by giving 45 days' written notice after receiving this information.

8. Transfers to third countries

8.1 The Parties acknowledge that, as of the effective date of the DPA, the Processor does not transfer Personal Data outside the EU/EEA, and does not engage Sub-Processors to process Personal Data outside the EU/EEA, in connection with the Services. If, during the term of the Agreement, the Processor intends to introduce any transfer of Personal Data outside the EU/EEA, the Processor shall (i) inform the Controller in advance in accordance with this DPA, and (ii) ensure that such transfer is carried out in accordance with Applicable Legislation,

including by implementing appropriate safeguards (such as an applicable adequacy decision or Standard Contractual Clauses) and, where required, supplementary measures.

9. Audit

9.1 Upon the Controller's request, the Processor will provide to the Controller information necessary to demonstrate the Processor's compliance with its obligations under Applicable Legislation and this DPA.

9.2 If the Controller, despite receiving the information set out in Section 9.1 above, has a legitimate reason to suspect that the Processor does not fulfill its obligations under Applicable Legislation and this DPA, the Controller shall be entitled on 30 days' written notice to carry out an audit of the Processor's processing of the Personal Data and information relevant in that respect. Such audit shall be performed by an independent auditor agreed between the parties. Audits shall be limited to once per year and shall not disrupt the Processor's operations. The Processor shall assist the Controller and disclose any information necessary in order for the Controller to carry out such audit. The Controller shall carry the costs for such audit.

9.3 If a data protection authority carries out an audit of the Processor which may involve the processing of Personal Data, the Processor shall promptly notify the Controller thereof.

10. Costs

10.1 The Processor shall be entitled to remuneration for any time spent to comply with Section 6 in accordance with the Services Fee for Professional Services as set out in the Service Order or otherwise as stated in the Processor's general price list for consultancy services. The Controller shall further bear all costs incurred by the Processor due to any altered or additional instructions issued by the Controller regarding the processing of the Personal Data.

11. Limitation of liability

11.1 The Processor's liability arising out of or related to this DPA is subject to the provisions on limitation of liability stated in the Agreement.

12. Confidentiality

12.1 The Processor undertakes not to disclose or provide any Personal Data, or any information related to the Personal Data, to any third party. For the avoidance of doubt, any Sub-Processor shall not be considered a third party for the purposes of this Section 12. This

confidentiality obligation will continue to apply also after the termination of this DPA without limitation in time.

12.2 Notwithstanding Section 12.1 above, the Processor may disclose such information if the Processor is obliged hereto by law, judgement by court or by decision by a competent authority. When such obligation arises, the Processor shall promptly notify the Controller in writing before disclosure, unless restricted from doing so under Applicable Legislation.

12.3 The Processor shall make available a contact point for data protection and security matters.

Contact: gdpr@safespring.com

13. Return and deletion of data

13.1 The Controller shall upon termination of the Agreement or this DPA instruct the Processor in writing whether or not to transfer the Personal Data to the Controller (such transfer to be made in a common machine-readable format). The Processor will erase the Personal Data from its systems no earlier than 30 days and no later than 40 days after the effective date of termination of the Agreement. The Processor shall confirm deletion in writing upon request.

14. Term

14.1 This DPA shall, notwithstanding the term of the Agreement, enter into effect when the Processor commences to process Personal Data on behalf of the Controller and shall terminate when the Processor has erased the Personal Data in accordance with Section 13 above.