Data Processing Agreement

Last updated: 15 April 2025

This Data Processing Agreement, including its Appendices ("**DPA**") forms part of the MSA or other written or electronic agreement between Sana and Subscriber for the purchase of online services (including associated Sana offline or mobile components) from Sana (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "**Agreement**") to reflect the following parties' agreement with regard to the Processing of Personal Data:

1. **Sana** (as defined in the Agreement); and
2. **Subscriber** (as defined in the Agreement);

The above parties are hereinafter each referred to as a "**Party**" and jointly as the "**Parties**."

1 BACKGROUND

1.1 This DPA shall be deemed to be part of the Agreement between the Parties.

1.2 To the extent Subscriber uses the Services to Process Personal Data, Subscriber must ensure that necessary consents have been obtained or another legal basis for the Processing of such Personal Data apply, and Subscriber represents to us that Subscriber is Processing such Personal Data in accordance with applicable law.

1.3 Parties understand and agree that Subscriber will use the Services provided by Sana for the Subscriber and its Affiliates, if applicable, and that the Personal Data that is being processed can therefore belong to any of the Affiliates as defined below. As between the Parties, Subscriber will act as a Controller on behalf of all its Affiliates for the term of this Agreement. If Subscriber acts as a Processor on behalf of its Affiliates and is required to retain such Processor role when using the Services, the Parties have agreed that Module 3 of the SCC with specific terms in Appendix C of this DPA shall apply. If any deviations are necessary due to mandatory legal requirements applicable on one of the Affiliates, Subscriber will provide instructions to Sana.

1.4 This DPA regulates Subscriber's rights and obligations in its capacity as Controller (as defined below) as well as Sana' rights and obligations in its capacity as Processor (as defined below) when Sana Processes Personal Data on behalf of Subscriber under the Agreement. If applicable, this DPA also regulates Subscriber's rights and obligations in its capacity as data processor on behalf of its Affiliates only to the extent related to the provision of the Services under the Agreement and Sana's rights and obligations in its capacity as sub-processor when Sana Processes Personal Data on behalf of Subscriber in its Processor capacity under the Agreement.

2 DEFINITIONS

Concepts, terms, and expressions in this DPA shall be interpreted in accordance with applicable data protection laws ("**Applicable Data Protection Laws**").

"**Adequacy Decision**" means a decision determining that a country, territory or sector within a country ensures an adequate level of protection for Personal Data under the EU GDPR or UK GDPR as applicable to the Personal Data Processing activity, which remains valid for the duration of the Agreement;

"**Affiliate**" shall have the meaning assigned to it in the MSA;

"**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement and this DPA including, but not limited to, the EU GDPR; the UK GDPR; and the UK Data Protection Act 2018; and US Data Protection Laws (defined herein);

"**Authorized Affiliates**" means any of Subscriber's Affiliate(s) which is permitted to use the Services pursuant to the Agreement between Subscriber and Sana, but has not signed its own Service Order Form with Sana;

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data;

"**Data Subject**" shall have the same meaning as if read in the context of the EU GDPR. For clarity, Data Subjects include "Consumers," as that term is defined by the CCPA or in other applicable law, as the case may be;

"**EU GDPR**" means the General Data Protection Regulation (EU) 2016/679;

"**EU Standard Contractual Clauses**" means: (i) the standard contractual clauses adopted by the European Commission on 4th June 2021 for the transfer of Personal Data to third countries pursuant to the GDPR and where (a) "MODULE TWO: Transfer controller to processor" therein is selected and applies where relevant; and/or "MODULE THREE: Transfer processor to processor" therein is selected and applies where relevant; or (ii) such other standard contractual clauses that are approved by the European Commission for Controller to Processor or Processor to Sub-Processor, as applicable, transfers of Personal Data to a third country which has not received an Adequacy Decision (and are subsequently incorporated into this DPA);

"**Personal Data**" shall have the same meaning as if read in the context of the EU GDPR, except where the UK GDPR applies to the Personal Data Processing activity, in which case the interpretation of the term under the UK GDPR shall apply. Personal Data includes "personal data", "personally identifiable information", and "personal information" as such terms are defined in Applicable Data Protection Laws;

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

"**Process**" / "**Processing**" / "**Processed**" shall have the same meaning as if read in the context of the EU GDPR, except where the UK GDPR applies to the Personal Data Processing activity, in which case the interpretation of the term under the UK GDPR shall apply;

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "**Service Provider**" as that term is defined by the US Data Protection Laws;

"**Restricted Transfer**" means a transfer of Personal Data to a country, a territory or specified sector within a country that: (i) is not subject to an Adequacy Decision; or (ii) is not subject to any derogations that would permit the transfer of the Personal Data to the country, territory or sector in accordance with the EU GDPR or UK GDPR (as applicable to the Personal Data transfer);

"**Sell**" or "**Sale**" of Personal Data means the transfer, sale, renting, releasing, disclosing, or making available of Personal Data to a third party in exchange for money or other valuable consideration;

"**Security Measures**" means the technical and organizational measures implemented by Sana to protect the confidentiality, integrity, availability, and resilience of Personal Data processed under this Agreement. These measures include, but are not limited to: encryption of data at rest and in transit, access controls and authentication mechanisms, regular vulnerability assessments, incident response procedures, and physical security safeguards at processing facilities. The Security Measures are further detailed in Appendix B to this Agreement and are designed to ensure a level of security appropriate to the risks associated with the processing of Personal Data, as required by Applicable Data Protection Laws, including Article 32 of the GDPR;

"**Services**" shall have the meaning given to it in the MSA;

"**Subscriber**" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Service Order Forms. For the purposes of this DPA only, and except where indicated otherwise, the term "Subscriber" shall include Subscriber and its Authorized Affiliates;

"**Subscriber Data**" means what is defined in the Agreement as "Subscriber Data" provided that such data is electronic data and information submitted by or for Subscriber to the Services. This DPA does not apply to External Content or Non-Sana Services as defined in the Agreement or, if not defined in the Agreement, as defined in the MSA;

"**Sub-processor**" means any person or entity engaged by the Processor to Process Personal Data on behalf of the Controller in connection with the provision of the Services;

"**Supervisory Authority**" means an independent public authority which is established pursuant to Article 51 of the EU GDPR, except where the UK GDPR applies to the Personal Data Processing activity, in which case the interpretation of the term under the UK GDPR shall apply;

"**UK Approved Addendum**" means the template addendum issued by the UK's Information Commissioner's Office and laid before the UK Parliament in accordance with section 119A of the UK Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of the Mandatory Clauses from time to time. Where the template addendum referred to in this definition, it means the document entitled: International Data Transfer Addendum to the EU Commission Standard Contractual, version B1.0, in force 21 March 2022;

"**UK GDPR**" means the EU GDPR as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and 2020 respectively and any legislation in force in the United Kingdom from time to time that subsequently amends or replaces the UK GDPR;

"**US Data Protection Laws**" means the standard which the Processor shall apply to Customer Personal Data sourced from residents in the United States. These laws include the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., and any implementing regulations ("**CCPA**"), as amended and appended by the California Privacy Rights Act of 2020 ("**CPRA**"). Where data from residents of other states are Processed or held by the Processor, the Processor shall read the requirements of those states into any references to CCPA; such laws to include, but not be limited to: Virginia's Consumer Data Protection Act ("**CDPA**"), the Colorado Privacy Act ("**CPA**"), the Personal Information Protection Act and the Biometric Information Act

("**BIPA**") of Illinois, as well as other laws that may be passed by the states relating to Personal Data.

With respect to Personal Data not subject to the EU GDPR or the UK GDPR, the definitions defined in this Section shall be interpreted in accordance with Applicable Data Protection Laws, to the extent that such definitions are incompatible, and such interpretations are necessary to comply with Applicable Data Protection Laws.

3 LIST OF APPENDICES

The following appendices shall form part of the DPA:

- Specification of data processing — Appendix A
- Security measures — Appendix B
- Information required for the EU Standard Contractual Clauses — Appendix C
- Information required for the UK Approved Addendum — Appendix D

4 PROCESSING OF PERSONAL DATA

4.1 Sana undertakes to process Personal Data for the limited and specified business purpose set forth in this DPA and in Appendix A and in accordance with Subscriber's written instructions, unless otherwise required by Applicable Data Protection Laws to which Sana is subject, in such a case, Sana shall inform the Subscriber of that legal requirement before Processing, unless Applicable Data Protection Laws prohibits such information to be shared with SubscriberThe Subscriber's instructions to Sana regarding the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, and the rights and obligations of both Parties are set forth in this DPA and in Appendix A. For the avoidance of doubt, the Subscriber does not permit any Sale of Personal Data under any circumstances and Parties acknowledge and agree that Subscriber has not Sold (as such term is defined herein and by the CCPA) Personal Data to Sana;

4.2 Sana shall also take steps to ensure that any natural person acting under the authority of Sana who has access to Subscriber Personal Data shall only Process the Subscriber Personal Data on the documented instructions of the Subscriber.

4.3 Processing Requirements, as Processor and a Service Provider, Sana agrees to:

4.3.1 Comply with all Applicable Data Protection Laws and promptly inform Subscriber in writing if it cannot comply with the requirements of this DPA or Applicable Data Protection Laws;

4.3.2 Grant Subscriber the right to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data upon notification of noncompliance with the requirements of this DPA or Applicable Data Protection Laws;

4.3.3 Inform Subscriber promptly (i) if, in Sana' opinion, an instruction from Subscriber violates Applicable Data Protection Laws; (ii) if Sana is unable to follow Subscriber's instructions for the Processing of Personal Data.

4.3.4 To the extent that Sana receives de-identified data derived from Personal Data subject to the CCPA from Subscriber, Sana shall (i) adopt reasonable measures to prevent such deidentified data from being used to infer information about, or otherwise being linked

to, a particular natural person or household; (ii) publicly commit to process data only in a de-identified fashion and not attempt to re-identify data; and (iii) before sharing de-identified data with any other party, including sub-processors, contractually obligate any such recipients to comply with the requirements of this provision;

4.3.5 For the purposes of US Data Protections Laws, the Processors acts as a Service Provider to which the Controller is disclosing Personal Data. Where acting as a Service Provider, Sana shall not (i) Sell, retain, use, disclose, or otherwise process Personal Data except as necessary for the business purposes specified in the Agreement or this DPA; (ii) retain, use, disclose, or otherwise process Personal Data in any manner outside of the direct business relationship between Sana and Subscriber; or (iii) combine any Personal Data with Personal Data that Sana receives from or on behalf of any other third party or collects from Sana' own interactions with individuals, provided that Sana may so combine Personal Data for a purpose permitted under the US Data Protection Laws if directed to do so by Subscriber or as otherwise permitted by the US Data Protection Laws.

4.3.6 Sana shall, without undue delay, inform Subscriber of any communication with the Supervisory Authority, other competent authority or third party that relates to or can be of interest for Sana's Processing of Personal Data under this DPA, and Sana will provide reasonable assistance to Subscriber if Subscriber receives a request from such authority or is subject to a regulatory investigation;

4.3.7 Sana shall assist Subscriber, through appropriate technical and organizational measures, with Subscriber's compliance obligations to implement reasonable security procedures and practices appropriate to the nature of the Personal Data.

5 OBLIGATIONS OF SUBSCRIBER

5.1 Subscriber represents, warrants, and covenants that it has and shall maintain throughout the term all necessary rights, consents, and authorizations to provide the Personal Data to Sana and to authorize Sana to use, disclose, retain and otherwise process that Personal Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to Sana. For the avoidance of doubt, Subscriber's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Subscriber shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Subscriber acquired Personal Data.

5.2 Subscriber specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Applicable Data Protection Laws.

5.3 Subscriber shall comply with all Applicable Data Protection Laws. Subscriber shall, in its use of the Services, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Sana as Processor (including where the Subscriber is a Processor, by ensuring that the ultimate Controller does so).

5.4 Without limitation to the foregoing, Subscriber represents, warrants, and covenants that it shall only transfer Personal Data to Sana using secure, reasonable, and appropriate mechanisms.

5.5 Subscriber shall not provide Personal Data to Sana except through agreed mechanisms. For example, Subscriber shall not include Personal Data other than technical contact information, or in technical support tickets, transmit Personal Data to Sana by email.

5.6 Subscriber shall not take any action that would (i) render the provision of Personal Data to Sana a "Sale" or a "share" under the US Data Protection Laws; or (ii) render Sana not a "Service Provider" under the US Data Protection Laws.

6 DISCLOSURE OF PERSONAL DATA

6.1 Sana undertakes not to, with the exception of sub-processors that have been approved by Subscriber in accordance with Section 7 below, without Subscriber's prior written consent, disclose or otherwise make Personal Data processed under this DPA available to any third party, unless otherwise provided by applicable Swedish or European law, judicial, or administrative decision.

6.2 If competent authorities or any other third parties request information from Sana regarding the processing of Personal Data covered by this DPA, Sana shall refer such requests to Subscriber to the extent permissible under applicable law. Sana may not in any way act on behalf of or as a representative of Subscriber and may not, without prior instructions from Subscriber, transfer or in any other way disclose Personal Data or any other information relating to the processing of Personal Data to any third party to the extent permissible under applicable law. In the event that Sana, according to Applicable Data Protection Laws or other applicable Swedish or European laws and regulations, is required to disclose Personal Data processed under this DPA, Sana shall immediately inform Subscriber thereof, unless otherwise legally prohibited, and request confidentiality in conjunction with the disclosure of requested information. To the extent Sana is prohibited by law from providing such aforementioned notification, Sana shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Sana to communicate as much information as possible, as soon as possible.

6.3 With regards to requests for Personal Data from Supervisory Authorities or other government authorities, Sana requires an official, signed document issued pursuant to local law and rules. Sana's compliance team will review government demands for Subscriber Data and use lawful efforts to ensure the requests are legally binding, reject those that are not legally binding and only provide the Subscriber Data specified in the legal order.

6.4 For the purposes of clarification to this Section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the applicable laws.

6.5 In the case that Sana receives an order from any third party for compelled disclosure of any Personal Data that has been transferred under the EU Standard Contractual Clauses, Sana will, (i) where possible, redirect the third party to request Personal Data directly from Subscriber and provide a copy of the demand unless legally prohibited from doing so; and (ii) use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable Member State law.

6.6 Sana will not provide any third party: (a) direct, indirect, blanket or unfettered access to any Personal Data; (b) platform encryption keys used to secure Personal Data or the

ability to break such encryption; or (c) access to Personal Data if Sana is aware that the data is to be used for purposes other than those stated in the third party's request.

7 SUB-PROCESSORS

7.1 Sana may engage sub-processors within and outside the EU/EEA and may transfer and in other ways process Personal Data outside the EU/EEA. Sana shall ensure that sub-processors are bound by written agreements which impose on them data processing obligations no less protective than the obligations under this DPA in respect of data protection, to the extent applicable to the nature of the Services provided by such Sub-processor.

7.2 The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed under Sana Sub-processors. Subscriber hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data and the Purchased Services.

7.3 The List of Sana Sub-processors contains a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, and if Subscriber subscribes, Sana shall provide notification of any change of or new Sub-processor(s).

7.4 Subscriber may object to the Processing of Subscriber's Personal Data, based on grounds regarding a new Sub-processor's ability to comply with Applicable Data Protection Laws if the change places the location of the processing outside of the EU / EEA, by providing a written objection to legal@sanalabs.com within thirty (30) business days following Sana' notification to Subscriber. Sana shall upon request provide Subscriber with all information that Subscriber may reasonably request to assess the proposed Sub-processor's ability to comply with Applicable Data Protection Laws. If Subscriber continues to object to the use of the new Sub-processor after having conducted the aforementioned assessment, Sana will use reasonable efforts to make available to Subscriber a change in the Services or recommend a commercially reasonable change to Subscriber's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Subscriber. If Sana is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Subscriber may terminate the applicable Service Order Form(s) with respect only to those Services which cannot be provided by Sana without the use of the objected-to new Sub-processor by providing written notice to Sana. Sana will refund Subscriber any prepaid fees covering the remainder of the term of such Service Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Subscriber.

7.5 Sana shall ensure that all Sub-processors comply with the obligations imposed on Sana under this DPA. For the avoidance of doubt, Sana shall be liable for the acts and omissions of its Sub-processors to the same extent Sana would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

8 THIRD COUNTRY TRANSFERS

8.1 If Restricted Transfers of Personal Data will be undertaken in connection with the Agreement, the Parties agree that the EU Standard Contractual Clauses shall be deemed as incorporated into this DPA and shall apply to such Restricted Transfers without further need for reference, incorporation or attachment and that by signing of the Agreement,, the Controller and the Processor are deemed to have executed the following transfer mechanisms:

8.1.1 EU Standard Contractual Clauses Module Two (which means EU Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor), where Subscriber and/or its Authorized Affiliate is a Controller and a data exporter, subject to the additional terms in Appendix C.

8.1.2 EU Standard Contractual Clauses Module Three (which means EU Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor), where Subscriber and/or its Authorized Affiliate is a Processor acting on behalf of a data controller and a data exporter, subject to the additional terms in Appendix C.

8.2 The Subscriber hereby authorizes Sana to enter into such EU Standard Contractual Clauses with sub-processors on behalf of Subscriber.

8.3 Sana shall closely follow the development regarding Restricted Transfers of Personal Data and, to the extent possible, implement any evolved requirements related to the transfer of Personal Data to a sub-processor, including the adoption of additional security measures and the conducting of all required risk assessments of privacy laws in the jurisdiction where the sub-processor is located, to ensure that the Services and the use of the Services are compliant with Applicable Data Protection Laws.

8.4 Sana agrees that it, at the time of concluding this DPA, has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which Personal Data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from Subscriber and its obligations under the EU Standard Contractual Clauses. In the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the EU Standard Contractual Clauses, Sana agrees to notify the change to Subscriber as soon as it is aware, in which case Subscriber is entitled to suspend the transfer of data and / or terminate the Agreement.

9 INFORMATION SECURITY AND CONFIDENTIALITY

9.1 Sana shall protect the Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed. The Personal Data shall also be protected against all other forms of unlawful processing.

9.2 Sana shall assist Subscriber and fulfill its legal obligations regarding information security under Applicable Data Protection Laws. Sana shall thereby take appropriate technical and organizational measures to maintain an adequate level of security for the protection of Personal Data, as set forth in Appendix B and the Policies. Sana regularly monitors compliance with Security Measures. Sana shall be obliged to ensure that only

such staff and other representatives of Sana that directly require access to Personal Data in order to fulfill Sana' obligations in accordance with this DPA have access to such information. Sana shall ensure that all persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that all persons authorized to process Personal Data have had sufficient and necessary training covering awareness of GDPR and data processing agreements.

10 DATA SUBJECT RIGHTS

10.1 Sana shall, to the extent legally permitted, promptly notify Subscriber of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "**Data Subject Request**".

10.2 Sana may not respond to a Data Subject Request by itself and Sana may not in any way act on behalf of or as a representative of Subscriber, except that Subscriber authorizes Sana to redirect the Data Subject Request as necessary to allow Subscriber to respond directly. Sana shall refer any Data Subject Requests to Subscriber to the extent permissible under applicable law.

10.3 Sana shall, insofar as it is possible and taking into account the nature of the processing, through technical and organizational measures assist Subscriber in responding to Data Subject Requests as laid down in Applicable Data Protection Laws, as applicable.

10.4 If Sana receives a Data Subject Request, it will:

(a) Inform the Data Subject that it is not the Controller of the information,
(b) Request that the Data Subject sends its request to the Controller, and
(c) forward the original request to Subscriber without undue delay.

10.5 To the extent Subscriber, in its use of the Services, does not have the ability to address a Data Subject Request, Sana shall upon Subscriber's request provide commercially reasonable efforts to assist Subscriber in responding to such Data Subject Request, to the extent Sana is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws. To the extent legally permitted, Subscriber shall be responsible for any costs arising from Sana's provision of such assistance.

11 DATA BREACH NOTIFICATIONS

11.1 The Processor shall notify the Controller without undue delay after becoming aware of, and in any event within 48 hours of discovering, any Personal Data Breach. Such notification shall as a minimum include the following:

(i) a description of the nature of the Personal Data Breach, including: a description of the Personal Data Breach; an explanation of how it occurred; the date and time of the Personal Data Breach; the date and time the Processor became aware of the Personal Data Breach; a description of how the Processor became aware of the Personal Data Breach; the type(s) of Personal Data affected by the Personal Data Breach; and the categories and approximate number of Data Subjects that have been impacted by the Personal Data Breach;

(ii) a description of the likely consequences of the Personal Data Breach including damage to reputation, the risk of harm, financial loss and/or prejudice to a criminal investigation; and

(iii) the measures taken or proposed by the Processor to address the Personal Data Breach, including, where appropriate, to mitigate its possible adverse effects.

11.2 If for any reason the Processor is unable to provide any of the information referred to in Clause 11.1 within the required timescale, the Processor shall provide a written explanation to the Controller and use reasonable endeavours to provide all such information as soon as possible and in any event within 48 hours. Notwithstanding the foregoing and for the avoidance of doubt, even where all information listed in Clause 11.1 is not available to the Processor, the Processor shall notify and provide such information that is available to the Controller within a 48 hour time period.

11.3 In the event of a Personal Data Breach, the Processor will take all steps necessary to secure and protect Subscriber Personal Data in order to limit the effects and impacts of any Personal Data Breach, and to reasonably assist the Controller in meeting the Controller's obligations under applicable law, including in relation to any notification to supervisory authorities and communications to Data Subjects regarding the Personal Data Breach as may be required under Applicable Data Protection Laws. In addition, the Processor shall reasonably cooperate with Controller's investigation into the Personal Data Breach and carry out its own investigation in accordance with Controller's instructions.

12 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATIONS

Sana shall, taking into account the nature of the Processing and the information available to Sana, assist Subscriber in fulfilling Subscriber's obligation to, when applicable, carry out data protection impact assessments and prior consultations with the Supervisory Authority.

13 AUDIT RIGHTS

13.1 The Subscriber shall be entitled to take measures necessary, including On-Site Audits (as defined below), to verify that Sana is able to comply with its obligations under this DPA.

13.2 Sana undertakes to make available to Subscriber all information and other assistance necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits conducted by Subscriber or another auditor mandated by Subscriber, provided that the individuals performing the audits enter into confidentiality agreements or are bound by statutory obligations of confidentiality.

13.3 Subscriber may request an on-site inspection of Sana's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by Subscriber either itself or through a third party auditor, who is a third-party independent contractor that is not a competitor of Sana, selected by Subscriber when:

(a) the information available pursuant to 13.2 is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Appendices;
(b) Subscriber has received a notice from Sana of a Data Breach; or
(c) such an audit is required by Applicable Data Protection Laws or by Subscriber's competent Supervisory Authority.

Any On-Site Audits will be limited to Subscriber Data Processing and storage facilities operated by Sana or any of Sana's Affiliates.

13.4 An On-Site Audit shall be conducted by Subscriber or its third-party auditor:

(a) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Subscriber;

(b) up to one time per year with at least three weeks' advance written notice. If an emergency justifies a shorter notice period, Sana will use good faith efforts to accommodate the On-Site Audit request; and

(c) during Sana's normal business hours, under reasonable duration and shall not unreasonably interfere with Sana's day-to-day operations.

13.5 Before any On-Site Audit commences, Subscriber and Sana shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Subscriber shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Sana. Sana shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Sana subscribers' information.

13.6 Subscriber must promptly provide Sana with information regarding any non-compliance discovered during the course of an On-Site Audit.

13.7 Sana shall immediately inform Subscriber if, in its opinion, an instruction provided to Sana when Subscriber exercises its rights under this Section 13, infringes Applicable Data Protection Laws.

14 AUTHORIZED AFFILIATES

14.1 The parties acknowledge and agree that, by executing the Agreement, Subscriber enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Sana and each such Authorized Affiliate subject to the provisions of the Agreement and this section 14 and section 17.

14.2 Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is a party only to this DPA. However, Subscriber shall ensure that all access to and use of the Services and Content by Authorized Affiliates comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Subscriber.

14.3 The Subscriber that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Sana under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

14.4 Where an Authorized Affiliate becomes a party to this DPA with Sana, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

14.4.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Sana directly by itself, the parties agree that (i) solely the Subscriber that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Subscriber that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in section 14.4.2, below).

14.4.2 The parties agree that the Subscriber that is the contracting party to the Agreement shall, when carrying out an On-Site Audits, pursuant to section 13, of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any substantial disruption to Sana and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

15 TERM OF AGREEMENT

The Processor will only Process Subscriber's Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and will remain in full force and effect until the later of the following: (a) the expiration or termination of the Agreement; and (b) the Processor and its Sub-processors (if any) no longer retain any Personal Data of the Subscriber in their possession or control.

16 MEASURES UPON COMPLETION OF PROCESSING OF PERSONAL DATA

16.1 The Processor shall, at the choice of the Controller, upon receipt of a written request within 30 days of the end the provision of the Services relating to Processing, securely delete or return all Personal Data to Controller. The Processor shall in any event delete all copies of Personal Data in its systems within 3 months of the effective date of termination of the Agreement unless Applicable Data Protection Laws require storage of Personal Data after termination.

16.2 If return or destruction is impracticable or incidentally prohibited by a valid legal order, Sana shall take measures to inform Subscriber and block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by applicable law) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control and, where any authorized sub-processor continues to possess Personal Data, require the authorized sub-processor to take the same measures that would be required of Sana.

16.3 Upon request by Subscriber, Sana shall provide a written notice of the measures taken regarding the Personal Data upon completion of the processing as set out in Section 14.1 above.

16.4 Archival Copies: If Sana is required by law to retain archival copies of Subscriber data for tax or similar regulatory purposes, Sana shall (i) not use the archived information for any other purpose; and (ii) remain bound by its obligations under this agreement, including, but not limited to, its obligations to protect the information using appropriate safeguards and to notify Subscriber of any Security Incident involving the information.

16.5 Deletion Standard: All Subscriber data deleted by Sana will be securely deleted using an industry-accepted practice designed to prevent data from being recovered using standard disk and file recovery utilities (e.g., secure overwriting, degaussing of magnetic media in an electromagnetic flux field of 5000+ GER, shredding, or mechanical disintegration). With respect to Subscriber data encrypted in compliance with this DPA, Sana may delete data by permanently and securely deleting all copies of the encryption keys.

17 LIABILITY

17.1 Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Sana, whether in contract, tort or under any other theory of liability, shall be subject to the limitations set out in art. 82 of EU GDPR.

17.2 Notwithstanding the aforementioned, Sana's liability towards the Subscriber under this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the limitations of liability set out in the MSA as the *Liability Super Cap*.

17.3 For the avoidance of doubt, Sana's and its Affiliates' total liability for all claims from Subscriber and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Subscriber and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Subscriber and/or to any Authorized Affiliate that is a contractual party to any such DPA.

18 GOVERNING LAW AND SETTLEMENT OF DISPUTES

18.1 This DPA shall be governed by and construed in accordance with Swedish law, without regard to the conflict of law rules.

18.2 To the extent that any provisions contained in this DPA or the Agreement conflict with the EU Standard Contractual Clauses, the provisions of the EU Standard Contractual Clauses shall prevail.

18.3 Any dispute, controversy, or claim arising out of or in connection with this DPA, or the breach, termination, or invalidity thereof, shall be finally settled in accordance with the dispute resolution provision set out in the Agreement.

_____

APPENDIX A.1 - SPECIFICATION OF DATA PROCESSING FOR SANA LEARN

1 Instructions

1.1 Short description of the service and the purposes of the processing

The purpose of processing is Sana's provision of Services to the Subscriber under the Agreement. Sana shall only process Personal Data as required to provide the Services in accordance with the Agreement.

1.2 Categories of Personal Data

- User:
  - Name
  - Email
  - Username
  - Password
  - Alphanumeric identifier
  - Profile picture
  - Custom attributes from Subscriber's pre-approved integrations
- Content:
  - In-meeting content: video, audio, images, chat, text, recordings, transcriptions, interactive card responses, files
  - Self-paced content: video, audio, images, chat, text, interactive card responses, files
  - Search queries: end-user's submitted queries
  - Third-party content: Content from Subscriber's pre-approved integrations
- Performance:
  - Time
  - Completion data
  - Progress
  - Course and path assignments
  - Favorites
- Device:
  - IP-address
  - City and country
  - Device type
  - MAC address
- Activity:
  - Event logs (e.g., action taken, event type, event location, timestamp, client UUID, user ID, and channel ID)
  - Cookies
  - Session information (e.g., frequency, average and actual duration, quantity, quality, network activity, and network connectivity)
  - Session facilitator/participant ID
- Support:
  - Troubleshooting subject
  - Problem description
  - Post-session feedback (score of 1-5 and free text)

- User-supplied attachments (e.g., recordings, transcripts or screenshots, text, post-session feedback)

1.3 Categories of data subjects

Sana will process Personal Data regarding Subscriber's end-users of the Services, which includes the following categories of data subjects:

- Natural persons who are authorized to administer and use the Services:
  - Subscriber's employees
  - Subscriber's third-parties, such as contractors, consultants, advisors
  - Subscriber's customers

1.4 Processing operations

Sana will collect, store, organize, and analyze the Personal Data for the purpose indicated above, as included in the Agreement and in accordance with instructions of Subscriber.

1.5 Location of processing operations

Sweden and as specified in Sana Sub-processors.

APPENDIX A.2 – SPECIFICATION OF DATA PROCESSING FOR SANA AGENTS

1 Instructions

1.1 Short description of the Services and the purposes of the processing

The Services include:

1. Sana Agents, i.e. web-based solutions for:

- Editing content,
- search and answer,
- generative responses,
- semantic search and source tagging,
- document upload and storage,
- user access controls and permissions,
- meeting transcription and,
- search and usage analytics.

2. Support services.

Sana shall process Personal Data on behalf of the Subscriber for the purpose of providing the Support Services.

1.2 Categories of Personal Data

- **User:** Your name, email, username, password, alphanumeric identifiers, profile picture, and other attributes that are provided when using the Services. Such personal data might also be collected from third-party systems per the Subscriber's Instruction.
- **Content:** Video, text, audio, and image files; end-user's search queries; third-party content from Subscriber's or Guest's pre-approved integrations.
- **Usage (Support purposes):** Data about activity on and use of our Services, such as app launches within our Services, including page history, search history, product interaction, crash data, performance and other diagnostic data, and other Usage data.
- **Device (Support purposes):** IP address, city and country, device type, MAC address.
- **Other Information You Provide to Us for Support Services:** Details such as the content of your communications with Sana, including interactions with customer support and contacts through social media channels.

1.3 Categories of data subjects

Sana will process Personal Data regarding the Subscriber's end-users of the Services, which includes the following categories of data subjects:

Natural persons who are authorized to administer and use the Services:

- Subscriber's employees
- Subscriber's third parties, such as contractors, consultants, advisors

- Subscriber's customers

1.4 Processing operations

Sana will collect, store, organize, and analyze the Personal Data for the purpose indicated above, as included in the Agreement and in accordance with instructions of the Subscriber.

1.5 Location of processing operations

Sweden and as specified in Sana Sub-processors.

APPENDIX B - SECURITY MEASURES

Our obligations to Subscriber are to ensure a continuous high quality delivery of our services, built on the highest level of security and resilience. We use the latest technology to make sure our infrastructure is reliable, and Subscriber data is protected.

This document describes the technical and organizational security measures and controls implemented by Sana to protect Personal Data and ensure the ongoing confidentiality, integrity and availability of Sana' products and services.

More details on the security measures and controls by Sana to secure Subscriber data are available in the Sana Labs Trust Center.

Sana reserves the right to revise these technical and organizational measures at any time, without notice unless required under applicable laws, so long as any such revisions will not materially reduce or weaken the protection provided for Personal Data that Sana processes in providing its products and services.

Sub-processors

Sana engages carefully vetted sub-processors for specific purposes to enhance Sana Services provided to Subscribers. For a list of sub-processors, please see Sana Sub-processors.

Business continuity management

Data backup is one of the pillars of Sana' IT continuity plan. Trained personnel manage and follow up on the automated backup execution to ensure the integrity, confidentiality, and accuracy of the backup data. Backups are taken daily. Personal Data is kept in backups for the first 30 days of the backup time, after which all Personal Data is removed from the backup, and the original backup is securely deleted. .

Another pillar is the streamlined IT incident response and disaster recovery processes that are carried out in case a serious incident occurs.

Sana continually works on keeping processes updated, measured and improved. The continuity plan is tested in tabletop and live exercises annually and based on regular risk assessments.

Sana has a high degree of IT digitization with all internal services and tools being digitally accessible using Google Accounts' SAML-based Federated SSO. As a result, most employees can continue to work from other locations even if Sana' offices are closed or not accessible due to an extreme event.

Supplier relationship management

Sana ensures that industry-standard security requirements are met by external suppliers during the procurement process. A contract with a chosen supplier addresses the demands on the supplier's IT environment,information security measures, security certifications in place. The supplier shall present and account for their technology, routines, and processes as well as IT,information security policies and continuous improvement of their practices. Non-disclosure agreements and other relevant regulatory agreements are signed by the supplier before the service is taken into service. Sana conducts regular supplier reviews, control of suppliers' access rights and other aspects of the agreement with the supplier. Suppliers agree to carry out assignments in accordance with the provisions specified in applicable laws and regulations in the country where the assignments are performed.

Information security management

Sana uses an Information Security Management System (ISMS) certified under ISO/IEC 27001:2022 as the basis for all company security routines, procedures and policies.. The ISO/IEC 27001:2022 standard provides guidelines and general principles for planning, implementing, maintaining, and continuously improving information security in the organization.

For technical security implementation and uniform coverage of systems in scope, Sana has implemented a set of technical controls and procedures that has been SOC 2 Type 2 certified.

System access control

Measures that prevent unauthorized persons from accessing IT systems:

- When provisioning access, Sana adheres to the principle of least privilege and role-based access control — meaning our employees are only authorized to access data that they reasonably must handle in order to fulfill their job responsibilities.
- Sana enforces multi-factor authentication for access to systems with highly confidential data, including our production environment which handlesPersonal Data.

Physical access control

Measures to prevent physical access of unauthorized persons to IT systems that handle Personal Data:

- Sana partners with industry-leading data center and cloud infrastructure providers. Access to all data centers is strictly controlled. All data centers are equipped with 24x7x365 surveillance and biometric access control systems. Additionally, all providers are ISO27001, ISO27017, ISO27018, SOC2 Type II, PCI DSS, and CSA STAR certified.
- Data centers are equipped with at least N+1 redundancy for power, networking, and cooling infrastructure.
- Sana replicates data across four separate, physically independent, and highly secure locations, ensuring high availability, and protection from local failures such as power outages and fires.

Measures to prevent physical access of unauthorized persons to physical office locations:

- Sana ensures that only authorized persons can access physical office locations through comprehensive physical and identity access management consisting of redundant key-card access points, video surveillance, and 24/7 identity management.
- Sana ensures effective and timely onboarding and offboarding of employees, contractors, and third parties, including the provision of relevant security trainings for said personnel and immediate return and / or destruction of sensitive documents and access cards upon termination.

Data access control in Sana products

Measures to ensure that persons authorized to use Sana products have access only to the Personal Data pursuant to their access rights:

- For local users, Sana utilizes programmatic enforcement of strong passwords that meet industry-standard complexity requirements..

- Recovery of lost passwords is done by requesting a signed link to the user's email account so that no passwords are sent in plain text over email, chat, phone, or any other communication method.
- Sana ensures passwords for local users are hashed (and salted) securely and stored in a secure database.
- For single sign-on users, authentication is performed using SAML 2.0 protocol - by contacting the Identity Provider service. This approach ensures that Sana does not store user passwords, and relies on a single enterprise identity.
- Sana uses a variety of best-in-breed tools for vulnerability scanning, logging, monitoring, malicious activity detection.
- Sana utilizes firewalls to segregate unwanted traffic from entering the network, and create separation between the network zones. A dedicated network segment DMZ for internet-facing infrastructure is used to further protect internal systems protecting sensitive data and limit any lateral movement from resources in this zone in case of a security event.

Data transmission control in Sana products

Measures to ensure that Personal Data cannot be read, copied, altered, or deleted by unauthorized persons during electronic transmission or during transport or storage of data, and that those areas can be controlled and identified where transmission of Personal Data is to be done via data transmission systems:

- Subscriber data at rest is encrypted with AES-256, and data in transit is encrypted with TLS 1.2+.
- Encryption keys (for data in rest and data in transit) are stored securely within the EU-located digital infrastructure.
- We also sign the data to ensure its integrity when feasible;

Entry control

Measures to ensure that it can be subsequently reviewed and determined if and from whom Personal Data was entered, altered, or deleted in the IT system:

- Access to production systems is audited and accounted for at all times.
- Logs are centrally stored and indexed. Critical logs, such as security logs, are retained for at least 2 months. Logs can be traced back to unique identities with timestamps to investigate nonconformities or security events.

Availability control

Measures to ensure that Personal Data are protected against accidental destruction or loss:

- Sana saves a full backup copy of production data daily to ensure rapid recovery in the event of a large-scale disaster. Incremental/point-in-time recovery is available for all primary databases. Backups are encrypted-in-transit and at rest using strong encryption.
- Sana' patch management process ensures that production systems are patched at least once every month. Monitoring, alerting, and routine vulnerability scanning occurs to ensure that all product infrastructure is patched consistently.

- When necessary, Sana patches infrastructure in an expedited manner in response to the disclosure of critical vulnerabilities to ensure system uptime is preserved.
- Customer environments are logically separated at all times. Subscribers are not able to access accounts other than those given authorization credentials.

Separation control

Measures to ensure that Personal Data collected for different purposes can be processed separately:

- Sana employs different data processing systems for different purposes. These systems are architecturally (logical and physically) separated. All systems require valid authorization to be accessed.
- To ensure against the unintentional amalgamation of data, Sana separates development, testing, staging, and production environments.

Risk management

Sana conducts the following risk management activities: :

- Periodic reviews and assessments of risks; monitoring and maintaining compliance with Sana' policies and procedures.
- Periodic, effective reporting of information security conditions and compliance to senior internal management.
- Periodic security risk management training, including but not limited to data protection for all employees, including an initial onboarding training for new employees to review and ensure compliance with up-to-date security risk management procedures and policies.
- central IT policy covering guidelines for Internet usage.

Operations security

Sana has implemented numerous controls and protections to ensure that the Services, independent of Subscriber Data, will not transmit Malicious Code.

Measures to ensure the appropriate operations security safeguarding against malicious code include but are not limited to:

- Sana has different systems and methods to protect the IT infrastructure against malicious code, including antivirus scanners, spam filters, timely security updates, and personnel security training.
- Sana uses active monitoring to ensure that antivirus scanners and spam filters are active and updated.
- Sana IT automatically installs the latest security updates on systems and applications to minimize the risk for exploitation of vulnerabilities.
- Sana, as part of basic training, ensures all employees and contractors take periodic training covering the identification of malicious code, common exploits and malware.

Measures to ensure that the appropriate operations security safeguarding email in place include but are not limited to:

- Sana utilizes world-leading email security services to protect all inbound and outbound emails from malware.

- Sana leverages email spam filtering services to guard against spam, virus, and phishing attacks.
- Employees of Sana are instructed to notify security staff about any emails that reached their inbox and are suspected to be infected or harmful. If confirmed, the email sender is blocked and quarantined. The initial verification and assessment of whether an email is malicious or not is automated and based on the rules but rather based on the competency of each Sana employee — educated on a periodic basis to identify harmful emails.

Security regarding personnel

Sana ensures that personnel complies with the laws and regulations of their employment country, and that they l abide by the relevant terms and conditions of supplier and customer agreements:

- Sana' personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Sana conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
- Personnel is required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Sana' confidentiality and privacy policies.
- Personnel is provided with security training. Sana' personnel will not process customer data without authorization.

Retention of Personal Data

Unless otherwise agreed between the During the term of the DPA, the Personal Data processed by Sana will be subject to the retention requirements of the Services and as per this Appendix B and the Agreement with Subscriber. After the termination or expiration of the DPA, Section 15 of the DPA shall apply.

Appendix C - Information required for the EU Standard Contractual Clauses

Module Two

For the purposes of EU Standard Contractual Clauses Module 2, the Parties agree the following:

Clause reference	Option selected
Clause 7 – Docking clause (optional)	The optional docking clause is not selected.
Clause 8.1(a)- Instructions	This DPA and the Agreement are Subscriber's complete and final documented instructions at the time of signature of the Agreement to Sana for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Subscriber to Process Personal Data are set out in section 4.1 of this DPA and include onward transfers to a third party located outside EU / EEA for the purpose of the performance of the Services.
Clause 8.5 and 16(d) - Certification of Deletion	The Parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the EU Standard Contractual Clauses shall be provided by Sana to Subscriber only upon Subscriber's written request.
Clause 8.9 - Audits of SCCs	The Parties agree that the audits described in clause 8.9 of the EU Standard Contractual Clauses shall be carried out in accordance with the audit provisions as agreed in the Agreement.
Clause 9(a) – Use of sub-processors	Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Processor has Controller's general authorization to engage Sub-processors in accordance with section 8 of this DPA. Processor shall make available to Controller the current list of Sub-processors in accordance with section 8 of this DPA. Pursuant to clause 9(a), Controller acknowledges and expressly agrees that Processor may engage new Sub-processors as described in sections 8 of this DPA. Processor shall inform Controller of any changes to Sub-processors following the procedure provided for in section 8 of this DPA.
Clause 11 – Redress (optional)	This optional redress clause is not selected.

Clause 13 - Supervision	Clause 13 shall apply as follows: ● If Subscriber is established in an EU Member State, the Supervisory Authority with responsibility for ensuring compliance by Subscriber with EU GDPR as regards the data transfer shall act as competent Supervisory Authority. ● If Subscriber is not established in an EU Member State, but falls within the territorial scope of application of EU GDPR in accordance with art. 3.2 and has appointed a representative pursuant to art. 27.1, the Supervisory Authority of the Member State in which the representative within the meaning of art. 27.1 is established shall act as competent Supervisory Authority. ● If Subscriber is not established in an EU Member State, but falls within the territorial scope of application of EU GDPR in accordance with art. 3.2 without however having to appoint a representative pursuant to art. 27.1, the Swedish Authority for Privacy Protection ("IMY") shall act as competent Supervisory Authority. ● If Subscriber is in the United Kingdom or falls within the territorial scope of application of the UK GDPR, the Information Commissioner's Office ("ICO") shall act as competent Supervisory Authority. ● If Subscriber is established in Switzerland or falls within the territorial scope of application of the data protection laws and regulations of Switzerland ("Swiss Data Protection Laws and Regulations"), the Swiss Federal Data Protection and Information Commissioner shall act as competent Supervisory Authority insofar as the relevant data transfer is governed by Swiss data protection laws and regulations.
Clause 15(1)(a) - Notification	For the purposes of clause 15(1)(a), Sana shall notify Subscriber (only) and not the Data Subject(s) in case of government access requests. Subscriber shall be solely responsible for promptly notifying the Data Subject as necessary.
Clause 17 - Governing law	Option 1 is selected. The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by a EU Member State law, the EU Standard Contractual 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 Sweden.

Clause 18 – Choice of forum and jurisdiction	The courts under clause 18 shall be those designated in the venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the Parties agree that the courts of Sweden shall have exclusive jurisdiction to resolve any dispute arising from the EU Standard Contractual Clauses.
Appendix	The Appendix shall be completed as follows: ● The contents of the list of parties in the MSA shall form Annex I.A to the EU Standard Contractual Clauses. ● The contents of Appendix A of this DPA shall form Annex I.B to the EU Standard Contractual Clauses. ● The contents of this table section "Clause 13 - Supervision" shall form Annex I.C to the EU Standard Contractual Clauses. ● The contents of Appendix B shall form Annex II to the EU Standard Contractual Clauses. ● The contents of this table section "Clause 9(a) - Subprocessors" and section 8 of this DPA shall form Annex III to the EU Standard Contractual Clauses.

Additional Terms for EU Standard Contractual Clauses Module 3

For the purposes of SCC Module 3 (only), the Parties agree the following:

Clause reference	**Option selected**
Clause 8.1(a)	Subscriber hereby informs Sana that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Subscriber warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Sana for the appointment of Subprocessors in accordance with this DPA, have been authorized by the relevant Controller. Subscriber shall be solely responsible for forwarding any notifications received from Sana to the relevant Controller where appropriate.
Clause 8.6(c) and (d),	Sana shall provide notification of a personal data breach concerning Personal Data Processed by Sana to Subscriber.
Clause 8.9	All enquiries from the relevant Controller shall be provided to Sana by Subscriber. If Sana receives an enquiry directly from a Controller, it shall forward the enquiry to Subscriber and

	Subscriber shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.
Clause 10	Subject to section 9 of this DPA, Sana shall notify Subscriber about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Subscriber shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

Appendix D - Information required for the UK Approved Addendum

In accordance with section 17 of the UK Approved Addendum, the Parties agree that the format and content of the tables in Part 1 of the UK Approved Addendum shall be amended and replaced with the table below.

Table reference in UK Approved Addendum	Section	Information to complete the table
Table 1: Parties	Start date	Is the Effective Date of the Agreement between the Parties.
Table 1: Parties	Parties' details	Name and address of the parties can be found at the "Parties" section on the first page of the MSA.
Table 2: Addendum EU SCCs	Addendum EU Standard Contractual Clauses	The Parties select the following option: "*EU Standard Contractual Clauses, including the Appendix Information and with only the following modules, clauses or optional provisions of the EU Standard Contractual Clauses brought into effect for the purposes of this Addendum*". The terms used in the paragraph above have the same meaning as in the UK Approved Addendum and details of the "Appendix Information", "clauses" and "optional provisions" are set out in Appendix C to this DPA.
Table 3: Appendix Information	Annex 1A – List of parties	Name, address and contact person's name, position and contact details can be found on the first page of the MSA and the Service Order Form. Activities relevant to the data transferred under these clauses and the role (controller/processor) can be found in Appendix A to this DPA. Signature and date can be found in the signatory page of the Service Order Form.
Table 3: Appendix Information	Annex 1B – Description of transfer	This information can be found in Appendix A to this DPA. To the extent applicable, the descriptions of safeguards applied to special categories of Personal Data can be found in the security measures referenced for satisfying the completion of Annex II of the EU standard contractual clauses (see below).

Table 3: Appendix Information	Annex II – Technical and organisational measures including technical and organisational measures to ensure the security of the data	The descriptions of technical and organisational measures applied to Personal Data is set-out in Appendix B, pursuant to section 9.2 of this DPA.
Table 3: Appendix Information	Annex III: List of Sub processors	See Sana Sub-processors.
Table 4: Ending this Addendum	Ending this Addendum when the UK Approved Addendum Changes	For the purposes of Table 4 of Part One of the UK Approved Addendum, neither Party may end the UK Approved Addendum when it changes.