Data Processing Agreement

Last updated: April 9, 2024

This DATA PROCESSING AGREEMENT ("**DPA**") is entered into on this day between:

1. **Sana** (as defined in the Agreement), and
2. **Subscriber** (as defined in the Agreement);
3. Sana and Subscriber are hereinafter each referred to as a "**Party**" and jointly as the "**Parties**."
4. For the purposes of this DPA, Subscriber shall also mean Subscriber Affiliates that are acting as a data controller when using Sana's Services.

1 BACKGROUND

1.1 The Parties have entered into an agreement under which Sana grants the Subscriber a limited subscription to use Sana's Services (the "**Agreement**").

1.2 This DPA shall be deemed to be part of the Agreement between the Parties. In case of any discrepancies between the Agreement and this DPA, this DPA shall prevail.

1.3 If the Parties agree that a Subscriber group company ("**Affiliate**") that is listed in the Subscription Service Order Form, should be eligible to use the Services, Subscriber confirms that is authorized to enter into relevant data processing agreements with Sana on such Affiliates' behalf. If any deviations are necessary due to mandatory legal requirements applicable to an Affiliate, Subscriber undertakes to ensure that such issues are raised in advance (prior to any processing on behalf of such Affiliate takes place) in writing to Sana.

1.4 This DPA regulates the Subscriber's rights and obligations in its capacity as *data controller* as well as Sana's rights and obligations in its capacity as *data processor* when Sana processes Personal Data on behalf of the Subscriber under the Agreement.

1.5 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 Standard Contractual Clauses.

2 DEFINITIONS

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

2.2 Personal data ("**Personal Data**") is limited to any information relating to an identified or identifiable natural person that Sana processes on behalf of and under the authority of the Subscriber to provide the Services under this Agreement.

2.3 The term Applicable Data Protection Laws shall for the purpose of this DPA, and at any time during the term of this DPA, mean any nationally or internationally binding data protection laws, case law, and regulations, applicable within the European Union (the "**EU**"), the European Economic Area ("**EEA**"), including the EU General Data Protection Regulation ("**GDPR**"), Cal. Civ. Code §§ 1798.100 et seq., as amended, including by the California

Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("**CCPA**"), and applicable subordinate legislation and regulations implementing those laws.

3 LIST OF APPENDICES

The following appendices shall form part of the DPA:

Specification of data processing	*Appendix A*
Pre-approved sub-processors	*Appendix B*
Security measures	*Appendix C*

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 the Subscriber's written instructions, unless otherwise required by Applicable Data Protection Laws to which Sana is subject. The 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.

4.2 Processing Requirements: As data processor and a service provider, Sana agrees to:

4.2.1 Comply with all Applicable Data Protection Laws, and where the CCPA applies, in a manner that provides no less than the level of privacy protection required by the CCPA;

4.2.2 Promptly inform you in writing if it cannot comply with the requirements of this DPA or Applicable Data Protection Laws;

4.2.3 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;

4.2.4 Cooperate with reasonable audits conducted by Subscriber, and at Subscriber's request, make information available to demonstrate Sana's compliance with Applicable Data Protection Laws;

4.2.5 Not provide Subscriber with remuneration in exchange for Personal Data from Subscriber. The parties acknowledge and agree that Subscriber has not "sold" (as such term is defined by the CCPA) Personal Data to Sana;

4.2.6 Not "sell" (as such term is defined by the CCPA) or "share" (as such term is defined by the CCPA) Personal Data;

4.2.7 Inform Subscriber promptly if, in Sana's opinion, an instruction from Subscriber violates applicable Data Protection Laws;

4.2.8 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;

4.2.9 Where the Personal Data is subject to the CCPA, not (i) 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's own interactions with individuals, provided that Sana may so combine Personal Data for a purpose permitted under the CCPA if directed to do so by Subscriber or as otherwise permitted by the CCPA. In the event that contrary to the parties' understanding, Sana is considered a contractor under CCPA, Sana certifies that it understands the restrictions in this section 4.2.10 and will comply with such terms, and will permit Subscriber, subject to Sana's agreement, to monitor Sana's compliance with this DPA, including through manual reviews, automated scans, regular assessments, audits, and technical and operational testing at least once per year;

4.2.10 Sana shall, to the extent permitted by applicable law, without undue delay, inform the Subscriber of any communication with the Data Protection 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;

4.2.11 Sana shall assist the 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.

5.2 Subscriber shall comply with all Applicable Data Protection Laws.

5.3 Subscriber shall reasonably cooperate with Sana to assist Sana in performing any of its obligations regarding any requests from Subscriber's data subjects, including, without limitation by maintaining a record of which "user ID" or similar numbers that are related to which data subjects in order to facilitate individual rights requests.

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 take any action that would (i) render the provision of Personal Data to Sana a "sale" or a "share" under the CCPA; or (ii) render Sana not a "service provider" under the CCPA.

6 DISCLOSURE OF PERSONAL DATA

6.1 Unless the Parties have agreed otherwise, Sana undertakes to only use sub-processors that have been approved by the Subscriber in accordance with Clause 6 below.

6.2 If data subjects, 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 the Subscriber to the extent permissible under applicable law. Sana may not in any way act on behalf of or as a representative of the Subscriber and may not, without prior instructions from the 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. If 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 the Subscriber thereof and request confidentiality in conjunction with the disclosure of requested information.

6.3 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 laws of the relevant jurisdiction:

- 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 Standard Contractual Clauses, Sana will, where possible, redirect the third party to request data directly from the Subscriber and provide a copy of the demand unless legally prohibited from doing so.
- 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 Standard Contractual Clauses, use all lawful efforts to challenge the order for disclosure based on 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.

6.4 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 AND THIRD COUNTRY TRANSFERS

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. For data transfers outside the EU/EEA, Sana ensures that certain appropriate safeguards are put in place and that sub-processors are bound by written agreements which impose on them the same data processing obligations as the obligations under this DPA with respect to data protection. Appendix B contains a complete list of its sub-processors that from the date of entry into force of this DPA have been pre-approved by the Subscriber.

7.2 Sana shall inform the Subscriber of any new sub-processors and give the Subscriber the opportunity to object to such changes. Such objections by the Subscriber shall be based on grounds regarding the new sub-processor's ability to comply with Applicable Data Protection

Laws and be made in writing within thirty (30) days from receipt of the information. Sana shall upon request provide the Subscriber with all information that the Subscriber may reasonably request to assess the proposed sub-processor's ability to comply with Applicable Data Protection Laws. If Sana, despite the Subscriber's objection, wishes to engage the proposed sub-processor, the Subscriber is entitled to terminate the Agreement at no extra cost.

7.3 If Personal Data is transferred to, or made available from, outside EU/EEA, Sana shall ensure that the transfer is subject to an appropriate safeguard under Applicable Data Protection Laws, using Standard Contractual Clauses adopted by the European Commission or an adequacy decision from the European Commission.

7.4 Sana shall closely follow the development regarding the transfer of Personal Data outside the EU/EEA 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 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 INFORMATION SECURITY AND CONFIDENTIALITY

8.1 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. 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.

8.2 Sana shall be obliged to ensure that only such staff and other representatives of Sana that directly require access to Personal Data to fulfill Sana's 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.

9 DATA SUBJECT RIGHTS

Sana shall, insofar as it is possible and considering the nature of the processing, through technical and organizational measures assist the Subscriber in responding to requests for exercising the data subject's rights as laid down in Chapter III of the GDPR and in the CCPA, as applicable. If Sana receives a Data Subject Rights request, it will:

- Inform the data subject that it is not the controller that should receive the request,
- Request that the data subject sends its request to the data controller,
- and forward the original request to the Subscriber without undue delay.

10 DATA BREACH NOTIFICATIONS

10.1 Sana shall without undue delay inform the Subscriber after becoming aware of any Personal Data breach.

10.2 Sana shall assist the Subscriber with any information reasonably required to fulfill the Subscriber's data breach notification requirements under Applicable Data Protection Laws.

11 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATIONS

Sana shall, considering the nature of the processing and the information available to Sana, assist the Subscriber in fulfilling the Subscriber's obligation to, when applicable, carry out data protection impact assessments and prior consultations with the Data Protection Authority.

12 AUDIT RIGHTS

12.1 The Subscriber shall be entitled to take measures necessary, including site visits, to verify that Sana is able to comply with its obligations under this DPA.

12.2 Sana undertakes to make available to the 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, including on-site inspections, conducted by the Subscriber or another auditor mandated by the Subscriber, provided that the individuals performing the audits enter into confidentiality agreements or are bound by statutory obligations of confidentiality.

12.3 Sana shall immediately inform the Subscriber if, in its opinion, an instruction provided to Sana when the Subscriber exercises its rights under this Clause 12, infringes Applicable Data Protection Laws.

13 TERM OF AGREEMENT

THE PROVISIONS OF THIS DPA SHALL APPLY AS LONG AS SANA PROCESSES PERSONAL DATA FOR WHICH THE SUBSCRIBER IS DATA CONTROLLER.

14 MEASURES UPON COMPLETION OF PROCESSING OF PERSONAL DATA

14.1 Before the expiration of this DPA, Sana shall, at the choice of the Subscriber, securely delete or return all Personal Data to the Subscriber without undue delay, unless Applicable Data Protection Laws require Sana to store the Personal Data.

14.2 If return or destruction is impracticable or incidentally prohibited by a valid legal order, Sana shall take measures to inform the 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.

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

14.4 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.

14.5 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.

15 AMENDMENTS

15.1 Any substantial amendments to this DPA shall, to be valid, be communicated to Subscriber in writing and Subscriber shall be given the opportunity to object to the proposed amendments. An objection shall be made in writing within thirty (30) days from receipt of the proposed amendments. If Sana, despite the Subscriber's objection, wishes to continue with the proposed amendments, the Subscriber is entitled to terminate the Agreement at no extra cost.

15.2 Notwithstanding Section 15.1 above, the Subscriber is entitled to make updates to its written instructions regarding the processing set out in Appendix A to the extent required by Applicable Data Protection Laws.

16 COMPENSATION

Sana shall be entitled to reasonable remuneration for any additional costs that arise due to Subscriber having made amendments to its written instructions regarding the processing.

17 LIABILITY

The liability provisions and limitations as it relates to personal data in the EU shall be in accordance with Article 82 of GDPR. All other liability provisions and limitations thereof set out in the Agreement shall apply to this DPA. To the greatest extent permitted by applicable laws, this shall mean that the aggregate liability per Section 7 in the Terms of Use shall apply for all Subscribers and Affiliates. Such maximum amount shall thus not be expanded on the basis that Affiliates use the Services and/or accede to this DPA.

18 GOVERNING LAW AND SETTLEMENT OF DISPUTES

18.1 As far as Applicable Data Protection Laws do not require otherwise, this DPA shall be governed by and construed in accordance with Swedish law.

18.2 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

Specification of data processing

1 INSTRUCTIONS

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

The Services include:

1. Sana AI, 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, access level and system role, 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, browser type, operating system, 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 Appendix B.

Appendix B

Pre-approved Sub-processors

For each sub-processor that we use, we apply the principles of least privilege. This means that each third party system shall only have access to the minimum data required to fulfill its purpose.

Sub-processor	Purpose	Data categories processed	Location and legal basis of processing	Legal entity
Anthropic	Search and model infra	Content (Search queries)	USA; SCC	Anthropic PBC, 548 Market Street, PMB 90375, San Francisco, CA 94104, United States
Azure	Search infra	Content (Search queries)	EEA/EU; EU-U.S. DPF, Swiss-U.S. DPF, UK Ext. to the EU-U.S. DP	Microsoft Ireland Operations, Ltd. One Microsoft Place, Dublin 18, D18 P521, Ireland
Gladia	Meeting transcriptions and recordings	User, Content	EEA/EU; GDPR	38 rue de la Tremblaie 35510 Cesson-Sévigné, France
Google Cloud	Hosting infra	User, Content, Performance, Device, Activity	EEA/EU; EU-U.S. Data Privacy Framework	Google Ireland Limited, Gordon House Barrow Street Dublin 4 Ireland VAT number: IE 6388047V
Intercom	Support	Support	EEA/EU; EU-U.S. DPF, Swiss-U.S. DPF, UK Ext. to the EU-U.S. DPF	Intercom R&D Unltd. Co, Stephen Court, 18-21 St., Dublin 2, Ireland
OpenAI	Search and model infra	Content (Search queries)	USA; SCC	OpenAI LP, 3180 18th St, San Francisco, CA 94110, USA
Recall	Meeting transcriptions and recordings	User, Content	USA; SCC	Hyperdoc Inc., 2261 Market Street #4339, San Francisco, CA
SendGrid	Transactional emailing	User, Content	USA; EU-U.S. Data Privacy Framework	Twilio Ireland Limited, 3 Dublin Landings, North Wall Quay, Dublin 1, Ireland
Vespa	Search infra	User, Content, Performance, Device, Activity	EEA/EU; GDPR	Vespa.AI AS, Prinsensgate 49, 7011 Trondheim, Norway

Appendix C

Security Measures

Our obligations to the 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. Just as we put hard work into our product, we also put the same energy and enthusiasm into our security practices.

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's products and services. More details on the measures we implement are available upon request. Sana reserves the right to revise these technical and organizational measures at any time, without notice, 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.

Description of our services

Sana provides teams with web-based solutions for editing, search and answer, generative responses, document storage, and meeting transcriptions.

Sub-processors

Sana engages carefully vetted sub-processors for specific purposes to enhance our services for our Subscribers. For a list of sub-processors, please see Appendix B for pre-approved Sub-processors.

Business continuity management

Data backup is one of the pillars of Sana's IT continuity plan. Trained personnel manage and follow up on 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 scrubbed from the backup, and the scrubbed backup is stored indefinitely.

Another pillar is the IT and management processes and routines that are carried out when a serious incident occurs. Sana continually works on keeping processes and routines updated. The continuity plan is tested at intervals based on regular risk assessments.

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

Supplier relationship management

Sana ensures that identified 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 and information security measures. The supplier shall present and account for their technology, routines, and processes as well as IT and information security policies. Non-disclosure agreements and other relevant regulatory agreements are signed by the supplier before the service is taken into service. Sana conducts regular 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 as the basis for all security measures. The ISO/IEC 27001 standard provides guidelines and general principles for planning, implementing, maintaining, and improving information security in an organization.

System access control

Measures that prevent unauthorized persons from using IT systems and processes:

- When provisioning access, Sana adheres to the principle of least privilege and role-based permissions — meaning our employees are only authorized to access data that they reasonably must handle to fulfill their job responsibilities.
- Sana utilizes multi-factor authentication for access to systems with highly confidential data, including our production environment which houses Personal 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 GCP 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 immediate onboarding and offboarding of employees, contractors, and third parties, including the security training of said personnel and immediate return and / or destruction of sensitive documents and access cards upon termination.

Data access control

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

- Sana utilizes the zxcvbn-estimator to validate passwords and only ensures strong passwords are used by users.
- Recovery of lost passwords is done by requesting a signed link to the user's email account — no passwords are sent in plain text over email, chat, phone, or any other communication method.
- Sana ensures passwords are hashed (and salted) securely using scrypt and stored in PostgreSQL, and upon Subscriber request, requires single sign-on (SSO) powered by SAML 2.0, for secure user authentication.
- Sana uses best-practice tools for vulnerability scanning, malicious activity detection, and blocks suspicious behavior automatically.
- Sana utilizes firewalls to segregate unwanted traffic from entering the network. A DMZ is utilized using firewalls to further protect internal systems protecting sensitive data.

Transmission access control

Measures to ensure that Personal Data cannot be read, copied, altered, or deleted by unauthorized persons during electronic transmission or during transport or storage on data media 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-128 and AES-256, and data in transit is encrypted with TLS 1.2.
- Sana is alerted to encryption issues through periodic risk assessments and third-party penetration tests. Sana performs third-party penetration tests on an annual basis, or as needed due to changes in the business.
- Sana attests that the key for the encryption (for data in rest and data in transit) is kept within the EU.
- We also sign the data to ensure its integrity; An IT security diagram can be found in Appendix C.1: IT Security diagram.

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:

- Systems are monitored for security events to ensure quick resolution.
- 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 individual unique usernames 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's patch management process ensures that 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.
- Subscriber environments are always logically separated. 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

Measures to ensure that the appropriate risk management and security risk management in place include but are not limited to:

- Sana conducts periodic reviews and assessments of risks, monitoring and maintaining compliance with Sana's policies and procedures.
- Sana ensures periodic, effective reporting of information security conditions and compliance to senior internal management.
- Sana hosts 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.
- Sana maintains a central IT policy covering guidelines for Internet usage.

Operations security

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

- Sana has different systems and methods to protect the IT infrastructure against malicious code, including various antivirus scanners, spam filters, security updates, and training.
- Sana uses active monitoring to ensure that antivirus scanners and spam filters are active and updated.
- Sana actively 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 take periodic training covering the identification of malicious code.

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

- Sana utilizes Google's world-class email security to protect all inbound and outbound emails from malware.
- Sana leverages Google's email spam filtering services to guard against spam, virus, and phishing attacks.
- Employees of Sana immediately notify staff of email identified as infected or harmful and ensure that the email sender is blocked and quarantined. The 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

Measures to ensure that Sana's personnel comply with the laws and regulations of the country, and ensuring that personnel abides by the relevant terms and conditions of supplier and customer agreements:

- Sana's 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's confidentiality and privacy policies. Personnel is provided with security training. Sana's personnel will not process customer data without authorization.

Retention of Personal Data

During the term of the DPA, the Personal Data processed by Sana will be subject to the retention requirements instructed from time to time by the Subscriber. After the termination or expiration of the DPA, Section 13 of the DPA shall apply.

Appendix C.1: IT Security diagram