Data Processing Agreement

This Data Processing Agreement, including the Appendices attached hereto (("the "**DPA**") is hereby entered into by and between:

Signatory company ("**The Customer**", "**the Data Controller**")

Meetric Nordic AB, corporate registration number 559252-4572, Kungsgatan 9, 111 21 Stockholm, Sweden ("Meetric" or",-"the Data Processor")

Each of the Data Controller and the Data Processor is referred to as a "Party" and together as the "Parties".

1. DEFINITIONS

1.1. To the extent that the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**General Data Protection Regulation**", "**GDPR**"), contains terms equivalent to those used in the Agreement, such terms shall be interpreted and applied in accordance with the GDPR.

1.2. Meetric offers a web-based platform for digital communication. Subject to the terms of the Agreement, Meetric will provide The Customer access to the platform for use of agreed services, as specified in the Agreement (below the "**Services**").

1.3. Applicable Data Protection Legislation refers to the General Data Protection Regulation (GDPR), regulations and practices relating to the General Data Protection Regulation, national supplementary legislation to the General Data Protection Regulation including the Swedish Data Protection Act, provisions, and opinions issued by supervisory authorities, including the European Data Protection Board (EDPB), and the Commission's legal acts concerning personal data.

1.4. Confidential information refers to all information related to or connected with this DPA and the processing of personal data under this DPA, as well as any other information obtained by a Party in its capacity as a Party to this DPA, regardless of the form or medium in which such information was received, or whether the information wasis provided orally or in writing. Confidential Information does not include information that: i) was already known to the Party at the time of receipt, provided the Party can substantiate this with written documentation, ii) was already publicly available at the time of entering into this DPA, or becomes publicly available during the term of this DPA, other than as a through a breach of this DPA, iii) was received from a third party, provided the Party can substantiate that the third party did not obtain the information, directly or indirectly, from the Party, iv) was created or developed independently by the Party, without reference to the Confidential Information

received from the other Party, v) was disclosed by the Party without restrictions on further dissemination, provided the Party can substantiate this with written documentation, or vi) is required to be disclosed by law, or by order from a competent authority or court, but only after notifying the affected Parties of the required disclosure.

2. AGREEMENT DOCUMENTS, PRECEDENCE AND PURPOSE

2.1. The Parties have entered into a services agreement including appendices for The Customer's use of the Meetric platform and other Services (the "**Services Agreement**"). Meetric will process personal data on behalf of The Customer in connection with the provisioning of Services under the Services Agreement. This DPA applies in relation ~~to the~~ to the Services Agreement. The clauses of this DPA are applicable to the processing of personal data in accordance with Appendix 1. Appendices~~x~~ 1-2 are attached hereto and form an integral part of the clauses in this DPA as set out below.

Appendix 1 – Personal data and processing

Appendix 2 – Security measures

Appendix 3 – List of Sub-processors

2.2. In the event of any conflict or discrepancy between the provisions of this DPA and the Services Agreement, as well as any other agreements between the Parties existing at the time these clauses are agreed upon or subsequently entered into, the provisions of this DPA shall prevail.

2.3. Meetric has, through this DPA, undertaken to process personal data on behalf of The Customer in conjunction with the Services. The Parties have agreed to regulate the scope and the details of the processing through the establishment of this DPA in accordance with article 28 GDPR (specifically Article 28.3) of the GDPR, to ensure the protection of the rights of the Data Subjects.

3. RESPONSIBILITIES AND INSTRUCTIONS

3.1. The Customer shall be responsible for ensuring that all processing of personal data is legal and is carried out in accordance with this DPA and Applicable Data Protection Legislation. The Customer shall, amongst others, be responsible for ensuring that the processing of personal data performed by Meetric on behalf of the Customer has a legal basis.

3.2. The Customer shall provide Meetric with the information and personal data that are necessary and appropriate for the Customer to be able to fulfill its obligations in accordance with this DPA and Applicable Data Protection Legislation.

3.3. The Customer shall only process the personal data that is adequate and relevant for the specifically chosen purpose of the processing and shall only grant Meetric access to the personal data that is necessary for the purpose of the processing. This obligation applies, for instance, to the volume of personal data, the duration of processing and the accessibility of the personal data.

3.4. The Customer (on behalf of Additional Controllers where relevant) is responsible for the processing of all personal data which Meetric processes on behalf of The Customer and Additional Controllers for the purpose of providing the Services.

3.5. The Customer is responsible for providing Meetric with documented instructions. Meetric shall process the personal data only on the documented instructions from The Customer. The documented instructions shall, among other things, but not exclusively, regulate the purpose of the processing, the categories of personal data to be processed, the categories of data subjects whose personal data is processed, the nature and the duration of the processing. The documented instructions are specified in Appendix 1 ("**Included Personal Data**").

3.6. Meetric undertakes to only process the Included Personal Data in accordance with the controller's written instructions as set out in this DPA, and only to the extent necessary for the performance of the Services Agreement. For the avoidance of doubt, the DPA and the Services Agreement include exhaustive instructions to Meetric as of the signing date. Meetric may alternatively terminate the DPA in such circumstances, subject to section 13.2 below.

3.7. If Meetric lacks instructions that it deems necessary to perform its tasks, Meetric shall, without undue delay, inform the Customer in writing and await the necessary instructions.

3.8. Meetric shall immediately inform The Customer if, in Meetric's opinion, an instruction infringes Applicable Data Protection Legislation.

3.9. Meetric shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Meetric is responsible for restricting access to personal data and shall therefore ensure that no more persons than necessary have access to the personal data.

3.10. Meetric shall provide reasonable assistance to The Customer in ensuring compliance with the obligations set out in Applicable Data Protection Legislation with regard to security off~~or~~ processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment and prior consultation, taking into account the nature of processing and the information available to Meetric.

3.11. Taking into account the nature of the processing, Meetric shall assist The Customer withby appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of The Customer's obligationsCustomers´ obligation to respond to requests for exercising the data subject's rights laid down in Applicable Data Protection Legislation.

3.12. The Customer is responsible for safeguarding the data subject's rights and responding to the data subject's requests for exercising its data subject's rights laid down in Chapter III GDPR, such as the right to information, access to personal data, rectification, erasure and the right to restrict the processing of personal data. If the data subject's request to exercise its data subject's rights is addressed directly to Meetric, Meetric shall inform The Customer without undue delay., upon The Customer is responsible for replying to the data subject's request, unless otherwise have agreed in writing between the Parties. Meetric furthermore undertakes to reasonably assist The Customer in fulfilling the data subject's rights.

3.13. The Customer acknowledges that the Services include functionality to enable The Customer to retrieve information and access personal data from the Services independently from Meetric, in order for The Customer to answer data subject requests and/or take other actions required pursuant to Applicable Data Protection Legislation. If and to the extent The Customer requests Meetric to assist withon a matter which The Customer could have handled itself through the Services, then Meetric is entitled to reasonable compensation for any and all such assistance or information provided.

3.14. In the event that Meetric receives a request from a governmental authority or other law enforcement entity seeking access to Included Personal Data, Meetric shall, unless legally prohibited, promptly notify The Customer within forty-eight (48) hours and provide all pertinent details regarding the request. Meetric shall cooperate with The Customer in challenging or limiting the scope of such requests where appropriate under Applicable Data Protection Legislation. The Customer retains the right to direct the response to any such request.

3.15. In the event of a request by data subjects, supervisory authorities, or any other third party, regarding the processing of the Included Personal Data, the Parties shall cooperate and exchange information to a necessary extent.

3.16. Meetric shall, when necessary and upon request, assist The Customer in fulfilling its obligations arising from the provisions of the General Data Protection Regulation regarding the performance of data protection impact assessments and prior consultations with the supervisory authority.

3.17. Meetric shall maintain a record of all categories of processing activities carried out on behalf of The Customer, containing:

- The name and contact details of the processor and of the controller on behalf of which the processor is acting, and, where applicable, of the processor's or of the controller's~~controller´s~~ representative and the Data Protection Officer,
- The categories of processing carried out on behalf of each controller,
- Where applicable, transfers of personal data to a third country or an international organization, including the identification of the third country or the international organization and documentation of suitable safeguards,
- Where possible, a general description of the technical and organizational security measures.

This record shall be in writing, including in electronic form.

4. CONFIDENTIALITY

4.1. Each Party undertakes, during the term of the agreement and thereafter, not to, without the other Party's~~Party´s~~ prior written consent, disclose or reveal to any third party personal data or information about the other Party's business that is reasonably deemed to be regarded as trade secrets, and hence "**Confidential Information**". Information which a Party has stated to be confidential is always considered ~~as~~ trade secrets.

4.2. The confidentiality requirement does not apply to information which a Party can show has been known to him in another way than in connection with the assignment or public knowledge.

4.3. The confidentiality requirement does further not apply when a Party is required by law or court order to disclose information. If a Party were to have or be required to disclose such information, that Party undertakes to immediately notify the other Party. The disclosing Party shall use its best efforts to ensure that the information disclosed in accordance with this clause is, to the greatest extent possible, treated confidentially by the recipient of the information.

4.4. The Parties undertake to use the Confidential Information solely for the purpose of fulfilling their obligations under the Services Agreement and this DPA and not for any other purpose.

4.5. Each Party is responsible for ensuring that its employees, subcontractors and subcontractors' employees are subject to confidentiality in accordance with section 5.1 above, and that such persons only have access to information to the extent that~~which~~ is necessary to perform their obligations.

5. SECURITY

5.1. Meetric guarantees that it possesses the necessary technical and organizational capacity and ability to fulfill its obligations under this DPA and the Applicable Data Protection Legislation.

5.2. Meetric shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to pseudonymisation and encryption of personal data, ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems, and regularly testing, assessing, and evaluating the effectiveness of such measures in line with GDPR Article 32.

5.3. The security measures are described in Appendix 2.

5.4. Meetric undertakes to provide The Customer with prior written notice of any intention to modify the manner in which personal data is processed or to implement other changes that could reasonably be expected to affect the security of the data subjects, the rights of the data subjects, compliance with this DPA, or Applicable Data Protection Legislation. Such notice shall be provided in writing at least thirty (30) days before the planned change and shall include a detailed description of the proposed changes as well as their potential impact on processing security, the rights of the data subjects, and compliance with this DPA and Applicable Data Protection Legislation. Meetric shall obtain the Customer's prior written consent before implementing any changes as described above. If such written consent is not provided within the agreed timeframe, the changes shall not be implemented. In the event of any disagreement regarding the proposed changes, the Parties shall promptly engage in discussions to reach a mutually acceptable solution. Until such a solution is reached, the original processing of personal data shall remain unchanged. All notifications under this Section 5.4 shall be sent by email to the Customer's designated contact person as specified in Section 15.

6. PERSONAL DATA BREACHES

6.1. In the event that Meetric suspects or becomes aware of a personal data breach, Meetric must immediately, but under no circumstances later than 24 hours after becoming aware of such suspicion or knowledge ~~has arisen~~, notify The Customer of the suspected or ascertained personal data breach. If compliance with the 24-hour timeframe is not possible due to exceptional circumstances, Meetric shall provide the Customer with a written explanation of the reasons for the delay. Meetric shall ~~and~~ otherwise provide The Customer with the necessary assistance in order to make it possible for The Customer to fulfil its obligations according to data protection legislation.

6.2. In the event of a suspected or discovered personal data breach, Meetric shall investigate the breach immediately and take appropriate measures to mitigate its potential negative effects.

6.3. The Customer shall be provided with a description of the personal data breach. Such description shall contain at least:

- a description of the type of personal data breach, including where possible the categories of and the approximate number of data subjects concerned, as well as the categories of and the approximate number of personal data items concerned,
- the name of and contact details for the Data Protection Officer or other contact points from where further information may be obtained,
- a description of the likely consequences of the personal data breach, and
- a description of the measures that have been taken or proposed by Meetric to remedy the personal data breach, including, where appropriate, measures to mitigate its potential negative effects.

If it is not possible to provide the information at the same time, the information may be provided in stages without further unnecessary delay.

6.4. A notification in accordance with the above shall contain all the information The Customer needs to fulfil its obligations towards the supervisory authority.

6.5. Meetric shall assist The Customer in ensuring that The Customer's obligations concerning personal data breaches are met, taking account of the type of processing and the information that Meetric has access to.

6.6. Meetric undertakes to document all personal data breaches, including suspected personal data breaches and the circumstances surrounding the personal data breach, its effects and the corrective measures taken and of which Meetric is aware of. Upon request, the documentation shall be provided to The Customer as soon as possible.

6.7. For the avoidance of doubt, Meetric will not be entitled to compensation for assistance related to a personal data breach caused by Meetric.

7. SUB-PROCESSORS

7.1. Meetric may engage a Sub-processor only if specific prior written authorization has been obtained from the Customer. The Parties agree that such specific prior written authorization is provided in Appendix 3. The Parties shall keep Appendix 3 updated.

7.2. If specific prior written authorization has been provided by The Customer in accordance with this DPA, as specified in an updated version of Appendix 3, Meetric shall notify The Customer in writing of any plans to engage a new Sub-Processor or replace an existing Sub-Processor. This is intended to provide The Customer with the opportunity to raise any objections to such changes. The notification shall include, at a minimum, the name of the proposed Sub-Processor, the location of the processing, and, if requested by The Customer, the type of processing to be carried out by the Sub-Processor. The notification shall be made at least fourteen (14) days in advance to ensure that The Customer is given sufficient time to raise objections before the new Sub-Processor is engaged or changes are implemented. If The Customer believes that the proposed Sub-Processor does not meet the requirements of the Applicable Data Protection Legislation and that this may materially affect or is likely to affect the privacy of the data subjects, the Customer shall have the right to raise legitimate objections. In the event of such objections, Meetric shall either modify the services provided by the relevant Sub-Processor to ensure compliance with the Applicable Data Protection Legislation or notify The Customer in writing of the reasons why the objection cannot be addressed. If Meetric is unable to address the legitimate objections of The Customer, The Customer shall have the right to terminate the DPA in accordance with the Services Agreement. If The Customer does not expressly approve or object to the engagement of the new Sub-Processor within the specified timeframe, this shall be deemed approval of the Sub-Processor. All notifications under this Section 7.2 shall be sent by email to the Customer's designated contact person as specified in Section 15. Meetric shall maintain an up-to-date list of Sub-processors, which shall be made available to the Customer upon request to dpo@meetric.com~~as approval of the Sub-Processor~~.

7.3. Meetric shall enter into data processing agreements with all its Sub-processors that will process Included personal data. Such data processing agreement shall impose the corresponding obligations to those of Meetric under this DPA on the Sub-Processor, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in accordance with the requirements of Applicable Data Protection Legislation. ~~Meetric will never store any personal data outside of EU.~~

7.4. Meetric and the Sub-processor shall agree on a third-party beneficiary clause, under which The Customer – in the event that Meetric ceases to exist in a factual or legal sense, or becomes insolvent – shall have the right to terminate the Sub-processor's data processing agreement and instruct the Sub-processor to delete or return the personal data.

7.5. Meetric shall be fully liable to The Customer for the performance of the Sub-processors' obligations according to the DPA and corresponding sections in any data processing agreements.

8. AUDIT

8.1. Customer has the right to, on its own or through an auditor, to a~~within~~ reasonable extent and with prior notice to Meetric, undertake an audit, including inspections, of Meetric. Such third-party auditor must execute a written confidentiality agreement acceptable to Meetric before conducting the audit. Subject to Section 3.5 above, Meetric will to a reasonable extent assist and permit audits by Additional Controllers and supervisory authorities. Meetric is entitled to reasonable compensation thereof.

8.2. The Customer acknowledges that Meetric may engage third party cloud providers to provide the Services. Any audit or inspection of such third-party cloud provider is subject to the policies and rules implemented by such third-party cloud provider from time to time.

8.3. To request an audit, Customer must submit a detailed audit plan to Meetric at least ten (10) business days in advance of the proposed audit. The audit plan must describe the proposed scope, duration, and start date of the audit. Meetric will review the audit plan and provide The Customer with any concerns or questions. Parties shall negotiate in good faith in agreeing on a final audit plan.

8.4. Meetric must, upon The Customer's request and to a reasonable extent, provide The Customer with available information about the processing of the Included Personal Data, in order to demonstrate compliance with its obligations under Applicable Data Protection Legislation. Meetric shall have the right to reasonable compensation therefor~~f~~.

8.5. The Customer shall document the results of the audit and delete it when it is no longer necessary for the purpose of the audit.

9. TRANSFERS TO THIRD COUNTRIES

9.1. The Parties acknowledge that the Services are designed and will be provided on the basis that all processing of Included Personal Data takes place within the EU/EEA. Meetric shall structure and maintain its technical and organisational set-up, including its choice of Sub-processors and support arrangements, so that no transfer of Included Personal Data to, or access to Included Personal Data from, a country outside the EU/EEA is required for the provision of the Services. Meetric shall not transfer or otherwise make Included Personal Data available to any recipient outside the EU/EEA, nor permit access to Included Personal Data from outside the EU/EEA, unless (i) the Customer has given its prior explicit written consent to such transfer or access, or (ii) such transfer or access is required by Union or Member State law to which Meetric is subject. Any such transfer or access pursuant to this clause shall only take place to the extent it is permitted under Applicable Data Protection Legislation, including Chapter V of the GDPR~~Meetric will not transfer the Included Personal Data outside of the EU/EEA~~.

9.2. In connection with ~~Notwithstanding~~ any ~~expectations to the contrary, if a~~ transfer pursuant~~of personal data is~~ to clause 9.1,~~take place~~ Meetric shall, before initiating such ~~prior to this~~ transfer, inform ~~obtain written consent from~~ The Customer in writing and ensure~~.~~ ~~A transfer to a third country also requires~~ that all~~Meetric, before initiating such a transfer, complies with the~~ requirements and measures set out in Chapter V of the GDPR regarding third country transfers are complied with.~~ ~~This includes, among other things, implementing appropriate safeguards such as the European Commission-approved Standard Contractual Clauses (SCC) or another valid transfer mechanism or exception under Applicable Data Protection Legislation~~other approved exceptions, including but not limited to for the performance of a contract or obtaining explicit consent from the data subject~~.

10. LIABILITY FOR DAMAGES

10.1. Meetric shall indemnify The Customer for any damage suffered by The Customer, the data subjects, or any other natural or legal person or authority as a result of Meetric's processing of personal data in violation of the documented instructions (including deficiencies in security measures) (Included Personal Data), This DPA, or Applicable Data Protection Legislation.

10.2. The Customer shall indemnify and hold Meetric harmless from~~r~~ any damages suffered by Meetric and for any claims directed against Meetric that arise from or are related to Meetric's processing of personal data in accordance with the instructions from The Customer or otherwise in accordance with this DPA. Any claims or demands may only be made in relation to personal data that needs to be processed to fulfill the Services Agreement in accordance with this DPA.

10.3. The Parties agree that if one Party is held liable under this clause, the Party that has paid compensation shall be entitled to recover from the other Party the portion of the compensation corresponding to the other Party's liability for the damage, in accordance with Article 82 of the GDPR.

10.4. Any limitation of liability in any other agreement between the Parties shall not apply in relation to processing covered by this DPA.

11. TERM AND TERMINATION

11.1. This DPA shall enter into force on the date when authorized representatives of both Parties have signed the DPA and shall remain valid for as long as the Services Agreement between the Parties is in effect ("**Term of the Agreement**").

11.2. This DPA remains in effect as long as Meetric processes included personal data on behalf of The Customer and Additional Controllers.

11.3. If the Services Agreement is terminated and a new agreement of the same kind is entered into without a new Data Processing Agreement being concluded, this DPA shall also apply to the new Services Agreement. This Agreement shall remain in effect even if the Services Agreement ceases and shall continue until Meetric and any Sub-processors engaged by Meetric have ceased processing personal Data on behalf of The Customer.

12. OBLIGATIONS AFTER THE TERMINATION OF THE AGREEMENT

12.1. Upon termination, all The Customer data shall be deleted within thirty (30) days, unless otherwise agreed upon in writing or storage of the data is required according to the law by which Meetric is governed. Upon completion of the deletion, Meetric shall provide the Customer with written certification confirming that all Included Personal Data has been securely deleted, including from all backup systems and archives, unless retention is required by applicable law. Such certification shall be provided within fourteen (14) days after the deletion is completed. If the Customer requires assistance in relation to the~~If The Customer requires assistance in relation to~~ export of data, Meetric shall be entitled to adequate compensation thereof.

12.2. If and to the extent required by Union or national law ~~that~~ Meetric shall store the Included Personal Data, Meetric has the right to do so notwithstanding what has been stated above.

13. MODIFICATIONS / AMENDMENTS

13.1. Any modifications or amendments to this DPA, including those required as a result of changes in Applicable Data Protection Legislation or regulatory guidance, shall be made in writing, agreed upon by both parties and signed by duly authorized representatives of both Parties. Upon receiving written notice of a proposed change from either party, the parties shall engage in good faith negotiations to reach a mutually acceptable amendment. Until such an amendment is executed, the existing terms of this DPA shall remain in full force and effect.

14. ASSIGNMENT

14.1. Neither Party is entitled to transfer, in whole or in part, its obligations or rights under this DPA to a third party without prior written approval from the other Party.

15. NOTICES

15.1. Notices, requests for personal data, and communications under this DPA shall be made in writing. All communications regarding data protection matters, including personal data breaches, data subject requests, and general data protection inquiries, shall be directed to the Data Protection Officer at dpo@meetric.com. Communications regarding

Sub-processor changes and security modifications shall be sent to the contact persons specified below. Notices shall be addressed to the contact persons specified below.

The Data Controller

[Company Name]

[name of contact person], [e-mail contact person]

Meetric

~~The Data Processor~~

Meetric Nordic AB

Data Protection Officer, dpo@meetric.com

Meetric has appointed a~~the above~~ dedicated Data Protection Officer as further described in Appendix 2 (Security measures). All~~responsible for overseeing our~~ data protection inquiries~~strategies, conducting regular compliance audits,~~ and notices to Meetric under this DPA shall be addressed to the Data Protection Officer at dpo@meetric.com~~managing data subject requests. The DPO also serves as our primary liaison with regulatory authorities~~.

16. GOVERNING LAW AND DISPUTES

16.1. This Agreement shall be interpreted and governed by Swedish law.

16.2. Any dispute, controversy or claim arising out of or in connection with this Agreement, or the breach, termination or invalidity thereof, shall be finally settled by arbitration in accordance with the ~~with the~~ Rules for Expedited Arbitrations of the SCC Arbitration Institute. The seat of arbitration shall be the Stockholm Chamber of Commerce Arbitration Institute. The language to be used in the arbitral proceedings shall be Swedish. This Agreement shall be governed by the substantive law of Sweden.

Appendix 1 to the DPA

Personal data and processing

The following documents constitute the documented instruction together with Appendix 2.

Definitions used in this Appendix 1 shall have the same meaning as in the DPA unless the context clearly indicates otherwise.

This Appendix 1 sets out the details concerning the Included Personal Data and processing thereof pursuant to the DPA.

The purpose of this Appendix 1 is to clarify which processing and personal data that are~~is~~ covered by the DPA, and to fulfill the requirements of the Applicable Data Protection Legislation regarding the obligation to specify the categories of a processor's processing of personal data.

The Parties confirm that this Appendix reflects the principle of data minimisation. Only the personal data specified herein may be processed, and Meetric shall not extend the scope of processing beyond what is necessary to provide the agreed Services.

1. The subject, nature, and the purpose of processing under the DPA

For communication and interaction with customers in digital salesrooms and meeting rooms in the tool Meetric. Personal data is saved for 12 months by default. This can be changed in settings.

2. Duration of the data processing

Meetric will process Personal Data solely for the period during which the Services are provided under the Services Agreement, including any additional period agreed in writing or required by applicable law. Upon termination or expiration of the Services Agreement, personal data will be returned to the Customer and/or, where technically feasible, securely deleted in accordance with Section 12.1 of this DPA (including the thirty (30) day deletion period and any applicable legal or written-agreement based retention obligations). Meetric's internal~~Meetric's~~ retention policies shall not permit retention of Personal Data beyond what is allowed under this DPA and Applicable Data Protection Legislation~~and legal obligations~~.

3. The categories of personal data

Meetric processes personal data as part of delivering its services. The specific categories of personal data, include the following, which are necessary for the provision of the Services:

Identifiers: Full name, email address, phone number, job title, company, account or user ID, device identifiers, and IP address. These identifiers are typically collected through recorded or transcribed communications, meeting participation, or system authentication within the Customer's environment.

Communication content: Voice and audio recordings, meeting and video recordings, transcripts of conversations, chat and email content, and related metadata such as meeting time, duration, participants, topics discussed, and engagement indicators. This information is processed for transcription, summarization, sentiment analysis, topic extraction, and related AI-powered insights.

Inferred and derived data: Insights generated through automated or AI-based analysis, including sentiment, behavioral patterns, and customer preferences inferred from communications. Such data remains linked to the individuals participating in the Customer's communications and is processed solely to support the Customer's use of the Services.

Integrated system data: Personal data obtained through integrations with Customer systems such as CRM, support, or marketing platforms, including contact history, deal and account information, support tickets, sales and purchase history, and website or application interaction data, to the extent these are provided or made accessible by the Customer.

Session identifiers: Session identifiers, connection data, and operational metadata generated during the use of the Services (e.g., timestamps, IPs, system events) processed only as required to provide, secure, and maintain the Customer's service environment.

Special categories of personal data (where applicable):

Given the nature of the Services (AI-powered analysis of meetings, transcriptions, and communications), the following special categories of personal data within the meaning of Article 9 GDPR may be processed:

- Health data (e.g., if disclosed during meetings, calls, or written communications)
- Biometric data (voice recordings and video recordings that may be used for identification purposes)
- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership (if disclosed during communications)

The Customer's responsibility for the legal basis:

The Customer acknowledges and confirms that:

(a) The Customer is solely responsible for ensuring that a valid legal basis exists under both Article 6 and Article 9 GDPR before providing Meetric with access to any special categories of personal data.

(b) Meetric processes special categories of personal data only on the Customer's documented instructions and for the purposes specified in this DPA.

(c) The Customer has obtained necessary explicit consents from data subjects, or established other appropriate legal grounds under Article 9.2 GDPR, prior to instructing Meetric to process such data.

(d) The Customer shall implement appropriate technical and organisational measures to ensure that data subjects are informed about the processing of special categories of personal data, including the use of AI-based analysis.

4. The categories of data subjects

The determination of which individuals' personal data is processed rests with The Customer and its authorized Users. Accordingly, Meetric processes personal data for the following categories of data subjects:

Customer Contacts: Individuals whose details are provided by The Customer, including first name, last name, address, phone number, email, and country of residence.

Meeting Participants: Individuals whose participation in video and audio meetings results in the capture of recordings and associated metadata.

5. Processing activities

In alignment with the Services Agreement, Meetric undertakes the following detailed activities concerning the Included Personal Data, which may include, but are~~is~~ not limited to:

CRM Integration: Establishing connections and enriching data between our platform and the client's Customer Relationship Management (CRM) and other internal systems.

Marketing Outreach: Engaging in targeted marketing strategies and campaigns to promote services.

Marketing Automation: Implementing and managing automated marketing processes to streamline and optimize customer outreach.

Email Management: Conducting specific email campaigns, which include~~s~~ sending, tracking, and analyzing the performance of these campaigns.

Meeting Management: Utilizing personal data during client meetings and handling any post-meeting data processing requirements.

Data Analysis: Conducting in-depth analysis and generating statistics related to client meetings, as well as evaluating the effectiveness of sales materials.

6. AI processing and use of Large Language Models

6.1. AI-powered processing activities

As part of delivering the Services, Meetric uses artificial intelligence and Large Language Models (LLMs) to perform the following processing activities on behalf of the Customer:

- Transcription of audio and video recordings
- Summarisation of conversations and meetings
- Sentiment analysis
- Topic extraction and categorisation
- Generation of automated insights and recommendations
- Other AI-powered analysis as specified in the Services Agreement

All third-party LLM providers used by Meetric are engaged as Sub-processors in accordance with Section 7 and Appendix 3 of this DPA.

6.2. EU/EEA-based processing

The Customer instructs Meetric to use only LLM providers established within the EU/EEA and to ensure that all processing of personal data by LLMs takes place exclusively on infrastructure located within the EU/EEA. No personal data shall be transferred to LLM providers located outside the EU/EEA without the Customer's prior written consent in accordance with Section 9 of this DPA.

6.3. Contractual safeguards with LLM providers

Meetric shall ensure that all third-party LLM providers are contractually bound by data processing agreements that include the following obligations:

(a) No training or model improvement: The LLM provider is prohibited from using personal data processed under this DPA to train, improve, or develop its AI models or any other models or products.

(b) No retention beyond processing: The LLM provider shall not retain personal data beyond the immediate processing session required to deliver the requested AI output, unless longer retention is explicitly agreed in writing with Meetric and notified to the Customer.

(c) Limited purpose: The LLM provider may use personal data only for the purpose of delivering the specific AI analysis requested by Meetric on behalf of the Customer, and for no other purpose.

(d) Security and confidentiality: The LLM provider shall implement appropriate technical and organisational security measures in accordance with Article 32 GDPR.

Data retention by LLM providers

Unless otherwise specified, personal data transmitted to third-party LLMs shall be processed in real-time or near-real-time sessions and shall not be retained by the LLM

provider after the processing output has been delivered to Meetric. Meetric will maintain documentation of the retention practices of each LLM provider and, upon the Customer's request, provide such information in accordance with Section 8 of this DPA.

7. Anonymisation and use of anonymised data

Instruction to anonymise

The Customer hereby authorises Meetric to anonymise personal data processed under this DPA in accordance with industry best practices and applicable data protection standards, provided that such anonymisation is conducted in a manner that ensures:

- The data subject is no longer identifiable by any means reasonably likely to be used by Meetric or any other person;
- The anonymisation is irreversible and the anonymised data cannot be re-identified;
- The anonymisation process does not reveal personal data, business secrets, confidential information, or information subject to professional secrecy.

Use of anonymised data

Once data has been effectively anonymised in accordance with this section, such data falls outside the scope of GDPR and this DPA. Meetric may use anonymised data for the following purposes without further restriction:

- Analysing and monitoring the performance, usage, and effectiveness of the Services;
- Improving, developing, and enhancing the Services and Meetric's products;
- Training, testing, and improving artificial intelligence models and algorithms;
- Conducting statistical analysis, research, and product development;
- Any other lawful business purpose that does not involve re-identification of data subjects.

Verification and accountability

Meetric shall maintain documentation of the anonymisation techniques and processes used, and shall make such documentation available to the Customer upon reasonable request for audit purposes in accordance with Section 8 of this DPA. The Customer may request Meetric to demonstrate that the anonymisation meets the requirements set out above.

Prohibition on re-identification

Meetric undertakes not to attempt to re-identify anonymised data or to combine anonymised data with other information for the purpose of identifying data subjects. Meetric shall implement appropriate technical and organisational measures to prevent unauthorised re-identification.

Appendix 2 to the DPA

Security measures

The following documents constitute the documented instruction together with Appendix 1.

Definitions used in this Appendix 1 shall have the same meaning as in the DPA unless the context clearly indicates otherwise.

At Meetric, safeguarding personal data is a top priority. Meetric's~~Our~~ security framework is designed to ensure compliance with the General Data Protection Regulation (GDPR) while maintaining the confidentiality, integrity, and availability of personal data processed in Meetric's~~our~~ EU-based cloud service. Meetric achieves~~We achieve~~ this through a layered approach that integrates robust technical controls with rigorous organis~~z~~ational policies.

1. Data Protection Officer (DPO)

Meetric has appointed a dedicated Data Protection Officer responsible for overseeing Meetric's~~our~~ data protection strategies, conducting regular compliance audits, and managing data subject requests. The DPO also serves as Meetric's~~our~~ primary liaison with regulatory authorities. For any data protection inquiries, please contact: dpo@meetric.com.

2. Data encryption

Data in Transit: Meetric secures~~We secure~~ all data transmitted over its~~our~~ networks using TLS 1.2/1.3 protocols to prevent interception and unauthorized access.

Data at Rest: Sensitive data is encrypted using AES-256. Key management practices include the use of Hardware Security Modules (HSMs), regular key rotation, and strict access controls to ensure keys are handled securely.

3. Secure development practices

Meetric maintains~~We maintain~~ a robust security posture from the earliest stages of development by integrating a comprehensive suite of security tools directly into its~~our~~ CI/CD pipelines.

Our pipelines include:

- Static Application Security Testing (SAST): Scanning Meetric's~~our~~ codebases to identify potential vulnerabilities early in the development process.
- Interactive Application Security Testing (IAST): Continuously monitoring running applications to detect vulnerabilities in real time.

- Software Composition Analysis (SCA): Analyzing third-party components to manage and mitigate risks associated with open-source software.

By embedding these automated security measures into the~~our~~ development lifecycle, Meetric~~we~~ proactively addresses potential risks and ensures that security remains a foundational element of its~~our~~ software delivery process.

4. Access control

Meetric~~The Data Processor~~ implements zero trust network access, replacing traditional VPN infrastructure. All access to internal resources requires identity verification and device posture checks through a secure client application.

Meetric enforces~~We enforce~~ role-based access control (RBAC) and implements multi-factor authentication (MFA) to ensure that only authorized personnel can access sensitive data.

Access rights are assigned based on the principle of least privilege and are reviewed periodically.

Comprehensive logging and monitoring mechanisms are in place to detect and respond to any unauthorized access attempts.

5. Data backup and recovery

Regular backups are performed daily and stored securely in geographically diverse locations to safeguard against data loss.

Meetric's~~Our~~ backup strategy is underpinned by clearly defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Meetric conducts~~We conduct~~ periodic disaster recovery drills to ensure rapid restoration of data and continuity of service in the event of an incident.

6. Network security

Meetric's~~Our~~ network infrastructure is protected by industry-leading firewalls, intrusion detection/prevention systems (IDS/IPS), and strategic network segmentation.

Meetric performs~~We perform~~ regular vulnerability assessments and penetration tests to proactively identify and mitigate potential security weaknesses.

7. Regular updates and patch management

A robust patch management process ensures that all software and systems are kept up to date.

Critical updates are tested and deployed promptly to address any vulnerabilities.

An up-to-date inventory of software and systems supports comprehensive and timely patching across the infrastructure.

8. Employee training and awareness

All employees receive regular training on data protection, security best practices, and GDPR compliance.

Training programs include periodic refresher courses and simulated phishing exercises to maintain a high level of security awareness.

Meetric assesses~~We assess~~ training outcomes continuously, ensuring that its~~our~~ team remains informed about evolving threats and compliance requirements.

9. Data Protection Impact Assessments (DPIAs)

Prior to introducing new processing activities or making significant changes, Meetric conducts~~we conduct~~ DPIAs to identify and mitigate potential risks to personal data.

DPIAs are thoroughly documented and reviewed periodically, ensuring that risk management remains an ongoing process.

10. Incident response and monitoring

Meetric maintains a comprehensive incident response plan that outlines clear procedures for detecting, containing, and mitigating security incidents.

Meetric employs~~We employ~~ a Security Information and Event Management (SIEM) system for centralized logging and real-time monitoring, enabling rapid identification and response to anomalies.

Meetric's~~By integrating these measures, we demonstrate a strong commitment to data protection and regulatory compliance. Our~~ security practices are continuously reviewed and enhanced to stay ahead of emerging threats and ensure the ongoing safety of personal data entrusted to Meetric~~us~~.

11. Security and Data Protection Policies

Device Security: Workstations shall automatically lock after 5 minutes of inactivity. Re-authentication is required to regain access.

Data Destruction: Employees must use secure erasure methods for personal data on devices, ensuring data cannot be recovered through standard recovery tools or forensic methods.

Visitor Management: All visitors must be escorted by authorized personnel at all times on the~~within~~ company premises. Visitor access logs are maintained.

12. Information Security Management System (ISMS)

Meetric is committed to achieving and maintaining ISO 27001 certification. Meetric's information security management system is designed in accordance with ISO 27001 standards, ensuring systematic risk assessment, continuous improvement, and compliance with international best practices for information security.

Appendix 3 to the DPA

Sub-processors

Below is a list of the Sub-processors engaged for the processing of personal data under this DPA.

The list shall be amended and updated each time a new Sub-processor is engaged, or a Sub-processor is replaced throughout the term of this DPA.

The Customer (The Data Controller) has approved the use of the following Sub-processors:

1. Entire Nordic AB

Organisation number: 559261-2377

Type of processing: Hosting services and infrastructure

Processing location: Uppsala, Sweden

Data residency: Sweden (EU/EEA)

DPA in place: Yes

2. Scaleway

Registration number: FR 35 433115904

Type of processing: Hosting, Storage, Transactional Emails, Databases, and general data processing

Processing location: Paris, France

Data residency: France (EU/EEA)

Description: European hosting and infrastructure provider

DPA in place: Yes

3. Google Cloud EMEA ~~Ltd. – Google Cloud EMEA~~ **Limited** Company Number: 660412

Registered office: Ireland

Type of processing: – Cloud infrastructure, data storage, databases, and AI processing services (including access to Google Gemini and other Large Language Models for transcription, summarisation, sentiment analysis, and AI-powered insights)

Processing location: EU/EEA ~~– Data is processed and stored exclusively within EU/EAA~~ regions exclusively (primary data centres: Belgium, the Netherlands, Finland)

Data residency: EU/EEA only –~~,~~ in accordance with Google's Data Processing Amendment ~~DPA~~ and data residency commitments

DPA in place: Yes (Google Cloud Data Processing Amendment)

Additional safeguards: Google Cloud is certified under ISO 27001, ISO 27017, ISO 27018, SOC 2/3, and adheres to the EU-U.S. Data Privacy Framework (though all processing for Meetric occurs exclusively within the EU/EEA)

Notification of changes: In accordance with Section 7.2 of this DPA, Meetric shall notify the Customer in writing of any planned engagement of a new Sub-processor or replacement of an existing Sub-processor, and the timing and content of such notices shall be governed solely by Section 7.2. This Appendix 3 is intended only to identify the Sub-processors approved by the Customer from time to time.

Updated list: This Appendix was last updated on 11 February 2026. An up-to-date version is available upon request to dpo@meetric.com.