Data Processing Addendum

1. This Data Processing Addendum (**DPA**) applies to the processing of Personal Data by MaxContact for any Agreements entered for MaxContact SaaS and related telecommunications services, as covered by MaxContact's Standard Terms and Conditions and executed Service Order with the Customer. The Customer shall be the party designated as such in the Service Order.

2. This Data Processing Addendum shall form part of the Agreement as defined in the Standard Terms and Conditions, and all defined terms in this DPA shall have the meaning given in the Standard Terms and Conditions unless otherwise specified in this DPA.

3. The following defined terms apply in this DPA:

Adequate Country: means any country or territory (or one or more specified sectors within that country or territory) that is recognised by the United Kingdom Government and/or European Commission (as applicable) as providing an adequate level of protection for Personal Data in accordance with Article 45 UK GDPR or Article 45 EU GDPR.

AI-Enabled Services: means Services that use artificial intelligence or machine learning to perform functions such as speech-to-text conversion, transcription, summarisation, topic or intent detection, sentiment analysis, or similar analytics.

AI Output: means model-generated outputs (e.g. data analysis, transcripts, summaries, topics, confidence scores, sentiment labels and other derived metadata) produced by the AI-Enabled Services from Customer-provided inputs.

Aggregated/Anonymised: means data that has been processed so that it does not relate to an identified or identifiable natural person and cannot reasonably be re-identified, taking into account all means reasonably likely to be used.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

Controller, processor, personal data, sub-processor, data breach shall have the meanings given in the Data Protection Legislation.

European Law: means the law and regulation of the European Union ("**EU**"), the European Economic Area ("**EEA**"), their member states, Switzerland, and the United Kingdom applicable to the Processing of Personal Data under the Agreement (including, as applicable, (i) Regulation 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 (General Data Protection Regulation) ("**EU GDPR**"); (ii) the EU GDPR as retained into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 ("**UK GDPR**"); (iii) the Swiss Federal Data Protection Act in force from 1 September 2023 and its corresponding ordinances ("**Swiss DPA**"); (iv) the EU e- Privacy Directive (Directive 2002/58/EC); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv) and any amending, updating or replacing legislation or regulation from time to time in force;

EU SCCs: means the standard contractual clauses adopted by the European Commission under Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to the EU GDPR (Modules 2 and 3, as applicable).

Inference: means the process by which a trained AI model generates AI Output from input data.

Restricted Transfer: means a transfer of Personal Data to a country outside the United Kingdom and/or European Economic Area which is not an Adequate Country.

Training/Improvement Data: means data used to develop, test or improve models, provided that any Customer Personal Data used for such purposes is Aggregated/Anonymised in accordance with this DPA.

UK Addendum: means the International Data Transfer Addendum to the EU SCCs issued under section 119A of the Data Protection Act 2018, as amended from time to time.

US Law: means the law and regulation of the United States applicable to the Processing of Personal Data under the Agreement, including (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 - 1798.199, 2022) and its implementing regulations ("**CCPA**"), (ii) the Virginia Consumer Data Protection Act, when effective, (iii) the Colorado Privacy Act and its implementing regulations, when effective, (iv) the Utah Consumer Privacy Act, when effective; and (v) Connecticut SB6, An Act Concerning Personal Data Privacy and Online Monitoring, when effective, (vi) the Texas Data Privacy and Security Act of 2023, when effective, (vii) the Tennessee Information Protection Act, when effective, (viii) the Oregon Consumer Privacy Act of 2023, when in force, (ix) the Montana Consumer Data Privacy Act of 2023, when in force, (x) the Indiana Consumer Data Protection Act of 2023, when in force, (xi) the Iowa Data Privacy Act of 2023, when in force, (xii) the Delaware Personal Data Privacy Act of 2023, when in force, (xiii) the applicable data protection laws made at federal or state level from time to time in force; and any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i) - (xiii) and any amending, updating or replacing legislation or regulation from time to time in force.

4. Both parties shall (and shall procure that any of their respective directors, officers, employees, permitted agents, licensees and contractors shall) comply with all applicable requirements of the Data Protection Legislation. This DPA is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

5. The parties acknowledge that, in respect of personal data, the Customer is the controller and MaxContact is a processor acting on behalf of the Customer. For clarity, this DPA applies to all AI-Enabled Services. Where any AI-Enabled Services are purchased under the Agreement (for example, through an applicable AI Software Addendum or Proof-of-Concept arrangement), the processing of Personal Data supporting those AI-Enabled Services is governed by this DPA he permitted processing of personal data under this DPA is as follows:

Subject Matter & Purpose	The provision of the Services as set out in the Agreement, in accordance with this DPA, including contact-centre SaaS functionality and, where purchased, AI-Enabled Services (for example, speech-to-text, transcription, summarisation, topic/intent/sentiment analytics and related model-driven features).
Nature	Personal data is processed by MaxContact through provision of the Service, including: • Collection of personal data from the Customer and its Authorised Users

	• Telecommunications administration, service management and recording of calls • Storage on MaxContact's (and its third party providers') servers • Structuring and filing in an organised database • Access, back up and retrieval of personal data • Such other processing activities as MaxContact is reasonably required to undertake in order to perform its obligations under the Agreement, in accordance with the Customer's instructions (including due to the Customer's use of the Service) • Audio ingestion and speech recognition for speech-to-text conversion and diarisation • Generation of AI Output (for example, transcripts, summaries, topics/intent, sentiment, and confidence/quality metrics) • Creation of technical logs and metadata necessary for monitoring, quality, security and troubleshooting of AI-Enabled Services
Duration	The duration of the Agreement, plus 3 months.
Types of Personal Data	• Login credentials and other personal and contact details for Authorised Users, including names, email addresses and passwords • Information relating to the data subject's work role, including job titles, unique IDs, locations, languages • Recordings of phone calls • Records of SMS, WhatsApp, and electronic communications via the Service • Such other types of Personal Data as the Customer or its Authorised Users may instruct MaxContact to process by their actions in the Software • Voice recordings and audio features relating to calls • Transcripts and conversational content derived from calls or digital channels • AI Output and associated metadata (for example, confidence scores, topics, sentiment, timestamps, and channel identifiers)
Categories of Data Subject	• Authorised Users and other employees and personnel of the Customer and/or its Affiliates • End-customers, prospective customers and other third parties whose voices or messages are captured in recorded interactions

6. Without prejudice to the generality of paragraph 1, the Customer shall:

6.1 ensure that it has all necessary and/or appropriate policies, consents (where required) and notices in place, has identified suitable lawful bases under the Data Protection Legislation or such other requirements under data protection laws in the territory of the Customer, and has taken such other measures as it is required to under the Data Protection Legislation, to enable the lawful transfer of personal data, by the Customer and its Affiliates, to MaxContact for the duration and purposes of this DPA;

6.2 ensure that all Personal Data transferred to MaxContact pursuant to this DPA is accurate and up-to-date;

6.3 not instruct MaxContact to undertake any processing activity that does not comply with the Data Protection Legislation;

6.4 not knowingly or negligently do or omit to do anything which places MaxContact in breach of its obligations under the Data Protection Legislation; and

6.5 ensure all Affiliates comply with the requirements placed on the Customer under this DPA.

7. MaxContact shall only process Personal Data in accordance with the written instructions of the Customer (including the provisions of this DPA) unless required to do so by law. Where MaxContact intends to rely on a requirement of law as the basis for processing the Personal Data, MaxContact shall promptly notify the Customer of this before performing the required processing unless the requirement of law relied upon prohibits MaxContact from so notifying the Customer.

8. MaxContact shall not engage any third party to process Personal Data on its behalf (a **Sub-Processor**), without prior specific or general written authorisation from the Customer (unless otherwise authorised under this DPA).

9. The Customer gives general authorisation for MaxContact to engage Sub-Processors and in which case the following applies:

9.1 MaxContact will maintain an up-to-date list of current Sub-processors (with service description and processing locations) and is available upon request.

9.2 MaxContact will notify the Customer of any changes to Sub-Processors made under prior general written authorisation and must allow the Customer a reasonable time to object to those changes;

9.3 MaxContact will ensure that the processing of personal data by any Sub-Processor is subject to terms substantially similar to, and no less restrictive than, the terms of this DPA; and

9.4 MaxContact shall remain fully liable, on the terms of this DPA and the Agreement, to the Customer for any acts or omissions of the Sub-Processor.

10. **Personal Data Transfers from the EEA, Switzerland and the UK:**

10.1 In connection with the Services, the Parties acknowledge that MaxContact (and its Sub-Processors) may process, outside of Switzerland, the EEA and the United Kingdom, certain Personal Data protected by European Law for which the Customer may be a Controller (or Processor on behalf of a third-party Controller, as the case may be).

10.2 For the avoidance of doubt, transfers of Personal Data from the EEA to the United Kingdom (and vice versa) do not currently require additional transfer mechanisms due to the UK's adequacy status. However, the Parties agree to implement SCCs (or another appropriate mechanism) promptly should this adequacy status be revoked. Both Parties agree that when the transfer of Personal Data protected by European Law from Customer to MaxContact is a Restricted Transfer, it shall be subject to the appropriate protections as follows:

10.3 **EEA Transfers:** in relation to Personal Data protected by the EU GDPR, the EU SCCs will apply, completed as follows:

10.3.1 Module Two (Controller to Processor) shall apply only if and when the Customer is located in the EEA and the UK is no longer subject to an adequacy decision under Article 45 of the EU GDPR. Module Three (Processor to Sub-Processor) shall apply where the Customer is a Processor on behalf of another Controller and MaxContact acts as its Sub-Processor;

10.3.2 Clause 7 (optional docking clause) applies;

10.3.3 Clause 9 Option 2 applies, and the notice for Sub-Processor changes is set out in Clause 9 of this DPA;

10.3.4 Clause 11 (optional language) does not apply;

10.3.5 Clause 17 Option 2 applies, and if the exporter's Member State does not permit third-party beneficiary rights, the law of England and Wales shall apply;

10.3.6 Clause 18(b): disputes shall be resolved before the courts of the jurisdiction governing the Agreement or, if that jurisdiction is not an EU Member State, then the courts of London, England;

10.3.7 Annex I of the EU SCCs is deemed completed with the information in Clause 5 (*table*) of this DPA; and

10.3.8 Annex II of the EU SCCs is deemed completed with the information in Clauses 11, 18 and 19 of this DPA.

10.4 **Swiss Transfers:** for Personal Data protected by the Swiss Federal Data Protection Act, the EU SCCs apply as set out above with the following adaptations:

10.4.1 the supervisory authority is the Swiss Federal Data Protection and Information Commissioner;

10.4.2 references to "Member State(s)" shall refer to Switzerland, and data subjects in Switzerland may exercise their rights there; and

10.4.3 references to "GDPR" shall mean the Swiss DPA.

10.5 **UK Transfers:** for Personal Data protected by the UK GDPR, the EU SCCs apply as set out above except that:

10.5.1 the EU SCCs are deemed amended as specified in the UK Addendum, which is deemed executed between the Customer and MaxContact;

10.5.2 any conflict between the EU SCCs and the UK Addendum shall be resolved per Sections 10 and 11 of the UK Addendum;

10.5.3 for the UK Addendum, Tables 1–3 are deemed completed using Clauses 5, 11, 18 and 19 information in this DPA; and

10.5.4 Table 4 is completed by selecting "neither party".

10.6 **General terms for EU SCCs**:

10.6.1 Customer may exercise its audit rights under the EU SCCs in accordance with Clause 17.2 and 17.3 of this DPA; and

10.6.2 MaxContact may appoint Sub-Processors as set out in Clauses 8 and 9 of this DPA, and Customer may exercise its objection rights accordingly.

10.6.3 If any provision of this DPA conflicts with the EU SCCs (or UK Addendum, as applicable), the EU SCCs / UK Addendum shall prevail to the extent of the conflict.

10.6.4 If Customer undertakes any transfer-risk assessment of the SCCs for specific destinations, MaxContact shall provide reasonable assistance where able, subject to reimbursement of reasonable costs.

10.6.5 If MaxContact later adopts an alternative transfer mechanism (for example under the EU-U.S. Data Privacy Framework, the UK Extension to that Framework, or any successor mechanism), such mechanism shall apply instead of the foregoing to the extent lawful, and the Customer shall execute any documents reasonably necessary to give effect to that change.

11. MaxContact shall put in place appropriate technical and organisational measures (having regard to the state of the art and technological development, the costs of implementation (where applicable) and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons) to:

11.1 ensure a level of security of personal data appropriate to the risk, and in particular to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, the personal data; and

11.2 enable and assist the Customer to meet its obligations to data subjects, including but not limited to:

11.2.1 rectification or erasure of personal data;

11.2.2 restriction of processing of personal data;

11.2.3 data portability; and

11.2.4 prompt response to subject access requests.

12. MaxContact shall obtain a commitment of confidentiality from anyone it allows to process the Personal Data, including but not limited to:

12.1 MaxContact's employees, agents, officers and affiliates;

12.2 agency or temporary workers; and

12.3 processors or Sub-Processors.

13. MaxContact shall assist the Customer, so far as possible and taking into account the nature of the processing under this DPA and the information available to MaxContact, in meeting the Customer's obligations under the Data Protection Legislation, including but not limited to:

13.1 the obligation to keep personal data secure;

13.2 the obligation to notify personal data breaches to the supervisory authority;

13.3 the obligation to advise data subjects where there has been a personal data breach;

13.4 the obligation to carry out data protection impact assessments;

13.5 the obligation to consult with the supervisory authority where a data protection impact assessment indicates an unmitigated high risk to the processing activities under this DPA; and

13.6 Where a data subject request relates to audio or to AI Output derived from audio or messages, MaxContact will, taking into account the nature of the processing and the information available to it, reasonably assist the Customer to identify relevant records (for example, by call ID, time window, channel, or other available metadata) and to provide intelligible descriptions of the categories of AI Output generated (for example, transcript, summary, sentiment, topic labels), in each case to the extent such information is available via the Services and subject to the Customer's configuration and retention settings.

14. **Automated decision-making. MaxContact** does not use the AI-Enabled Services to take decisions solely by automated means that produce legal or similarly significant effects on individuals on behalf of the Customer. If the Customer configures workflows that could amount to automated decision-making engaging Article 22 UK GDPR / EU GDPR, the parties will agree in advance the required safeguards (including human review, appropriate transparency, and rights to obtain human intervention) before such workflows are enabled.

15. **Service improvement and anonymisation**. MaxContact may use Aggregated / Anonymised data derived from the Customer's use of the Services to maintain, improve and develop the Services (including AI-Enabled Services). MaxContact will not use Customer Personal Data in a form that identifies the Customer or any data subject for model training or improvement, and will not attempt to re-identify Aggregated / Anonymised data.

16. **AI data retention and deletion.** For AI-Enabled Services, audio files, transcripts and AI Output follow the retention periods configured by the Customer in the Services (or, if not configured, MaxContact's standard product retention). Backups follow platform backup cycles and are overwritten on a rolling basis. Upon termination of the Agreement or upon written request, MaxContact will securely delete or return AI-related Customer Personal Data and confirm completion, subject to standard backup overwrites and any legal holds.

17. MaxContact shall:

    17.1 maintain a record of its processing activities in accordance with the requirements of the Data Protection Legislation and retain all other information required to demonstrate that MaxContact has met its obligations under the Data Protection Legislation and under this DPA;

    17.2 submit and contribute to reasonable audits and inspections carried out by the Customer or a third-party appointed by the Customer to carry out such audits or inspections (provided that such audits shall occur no more frequently than once in each calendar year). The Customer shall endeavour to provide reasonable written notice of the date of inspections or audits;

    17.3 on reasonable request, provide high-level descriptions of AI-Enabled Service data flows, the roles of relevant Sub-Processors and the safeguards applied, to assist the Customer's accountability obligations (for example, records of processing, DPIAs and transfer assessments);

    17.4 inform the Customer immediately if MaxContact believes or suspects that it has been given an instruction that does not comply with the Data Protection Legislation; and

    17.5 notify the Customer immediately if MaxContact becomes aware of or reasonably suspects a personal data breach.

18. MaxContact shall ensure it has implemented an ISMS (Information Security Management System) to ensure that the Customers Data is protected. This ISMS is ISO 27001 accredited and externally audited by BSI, the certificate number is IS 695173.

19. **Additional controls for AI-Enabled Services.**

19.1 In addition to MaxContact's ISO 27001-aligned Information Security Management System described above, the following controls apply to AI-Enabled Services where relevant and appropriate to risk:

19.1.1 tenant isolation and access controls on audio, transcripts and AI Output;

19.1.2 encryption in transit and at rest;

19.1.3 role-based access control, least-privilege principles and multi-factor authentication for users with access to AI-related datasets;

19.1.4 monitoring of AI model pipelines, including logging of prompts or inputs (where applicable), outputs and administrator actions for security and quality assurance;

19.1.5 regular vulnerability testing of AI service components and of any third-party model endpoints;

19.1.6 safeguards against prompt or command injection and other misuse of AI model endpoints;

19.1.7 documented procedures for redaction or anonymisation of datasets used for testing or service improvement; and

19.1.8 periodic review of model performance to assess accuracy, drift and fairness in proportion to the risk and nature of use.

20. Each party (the **first party**) shall indemnify the other party (to the fullest extent permitted by law), but subject to any limits on liability set out in the Agreement, against any claim, loss, damage, expense or fine incurred by the other party arising under or in connection with the Data Protection Legislation and caused by any action or omission of the first party or its Affiliates (or its directors, officers, employees, permitted agents, licensees and contractors) unless such action or omission is specifically requested by the other party.