PERSONAL DATA PROCESSING AGREEMENT

Customer

and

Destiny Sweden AB

1 PARTIES

The Parties to this Data Processing Agreement ("Agreement") are:

1.1 **Data Controller:** [Full Legal Name], Reg. No. [●], with registered address at [●], and designated contact email [●], hereinafter referred to as the "Data Controller."

1.2 **Data Processor:** Destiny Sweden AB, Reg. No. 556377-2317, Lumaparksvägen 11, 120 31 Stockholm, Sweden, contact email: dpo@dstny.se, hereinafter referred to as the "Data Processor."

Each individually a "Party" and collectively the "Parties."

1.3 **Roles:**
The Data Controller determines the purposes and means of processing Personal Data, while the Data Processor processes Personal Data on behalf of The Data Controller in accordance with GDPR and this Agreement.

2 INITIAL PROVISIONS

2.1 GDPR Basis

The Parties have entered into a Main Agreement and related contractual documents concerning the provision of telecommunication products, services and, where applicable, operator services (the "Main Agreement"), under which the Data Processor may process Personal Data on behalf of The Data Controller. This Data Processing Agreement (the "Agreement") is concluded to ensure compliance with Article 28 of the General Data Protection Regulation (EU) 2016/679 ("GDPR") and applicable Swedish and EU data protection laws, establishing adequate safeguards for the protection of Personal Data and the rights and freedoms of Data Subjects.

2.2 Documented Instructions

For the purposes of Article 28(3)(a) GDPR, the Controller instructs the Processor to process Personal Data in accordance with the Main Agreement and this Data Processing Agreement, including all applicable Appendices, which together constitute the Controller's complete and documented instructions to the Processor.

Without limiting the foregoing, the Controller expressly authorizes the Processor to process Personal Data as necessary to provide the Services and to perform related activities such as support and maintenance, service monitoring, security logging and incident prevention, billing and accounting, compliance with legal obligations, and the improvement and protection of the Services, in each case in accordance with this Agreement and applicable Data Protection Law.

2.3 Purpose of the Agreement

The purpose of this Agreement is to ensure adequate safeguards for the protection of Personal Data and the rights and freedoms of Data Subjects.

2.4 Regulatory Changes and EDPB Guidance

The Parties agree to comply with future amendments to applicable data protection legislation and EDPB guidelines, implementing necessary changes without undue delay.

2.5 Transfer Mechanisms

Standard Contractual Clauses (SCC) and other transfer mechanisms under Chapter V GDPR shall apply where relevant.

3 DEFINITIONS

The following terms, used in this Agreement, have the following meanings:

3.1 "Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject") as defined in GDPR Article 4(1).

3.2 "Processing" means any operation performed on Personal Data, whether automated or not, as defined in GDPR Article 4(2).

3.3 "Personal Data Legislation" means GDPR (EU 2016/679), Swedish data protection law, and any applicable EU or Member State regulations.

3.4 "Third Country" means any country outside the EEA.

3.5 "Supervisory Authority" means an independent public authority established under GDPR Article 51.

3.6 "Personal Data Breach" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Undefined terms shall have the meaning given under GDPR and related guidance.

4 OBLIGATIONS OF THE DATA CONTROLLER

4.1 Lawful Instructions

The Data Controller shall provide the Data Processor with documented instructions for the processing of Personal Data, as set out in Appendix A and any subsequent written amendments. The Data Controller warrants that such instructions comply with applicable Personal Data Legislation.

4.2 Legal Basis and Transparency

The Data Controller is responsible for ensuring that all Personal Data provided to the Data Processor is collected and processed lawfully, including having a valid legal basis under GDPR. The Data Controller shall inform Data Subjects of the processing in accordance with Articles 13 and 14 GDPR.

4.3 Data Accuracy and Minimization

The Data Controller shall ensure that Personal Data shared with the Data Processor is accurate, up to date, and limited to what is necessary for the purposes described in the Main Agreement and this Agreement.

4.4 Cooperation and Communication

The Data Controller shall promptly inform the Data Processor of any changes to processing instructions, categories of Personal Data, or other relevant circumstances that may affect the Data Processor's obligations under this Agreement.

4.5 Data Subject Rights

The Data Controller shall handle requests from Data Subjects to exercise their rights under GDPR. The Data Processor shall assist as described in Clause 4.4, but ultimate responsibility for responding to such requests rests with The Data Controller.

4.6 Records and Impact Assessments

The Data Controller shall maintain records of processing activities and, where required, conduct Data Protection Impact Assessments and prior consultations with supervisory authorities.

4.7 Cooperation in Audits

The Data Controller shall cooperate with the Data Processor in relation to audits by providing, without undue delay, all information, decisions, and instructions reasonably required to enable the Data Processor to comply with its obligations under this Agreement and applicable Data Protection Law.

4.8 Audit and Supervisory Authority Access

The Data Processor shall provide The Data Controller and, upon request, the competent supervisory authority with access to all information necessary to demonstrate compliance with this Agreement and applicable Personal Data Legislation. The Data Processor shall also allow supervisory authorities access to its facilities and systems upon presentation of appropriate identification, as required by law.

5 OBLIGATIONS OF THE DATA PROCESSOR

5.1 Processing Instructions

a) The Data Processor shall process Personal Data only on documented instructions from The Data Controller, including with respect to transfers to third countries or international organizations, unless required by Union or Member State law. In such cases, the Data Processor shall inform The Data Controller of the legal requirement prior to processing, unless prohibited by law.
b) The Data Processor shall immediately notify The Data Controller if, in its

opinion, an instruction infringes applicable Personal Data Legislation and shall suspend the relevant processing until the matter is resolved or a supervisory authority confirms lawfulness.

5.2 Security Measures

a) The Data Processor shall implement and maintain appropriate technical and organizational measures as described in Appendix C to ensure a level of security appropriate to the risk, including measures for confidentiality, integrity, availability, and resilience of processing systems.
b) The Data Processor shall review and update these measures regularly to reflect technological developments, regulatory changes, and industry best practice.

5.3 AI Regulatory Compliance

Where the Services include AI-based, automated or machine-learning-supported functionalities, the Data Processor shall implement appropriate technical and organizational measures designed to support compliance with applicable legislation governing artificial intelligence systems, including, where applicable, the EU Artificial Intelligence Act, to the extent such legislation applies to the Data Processor's role.

The allocation of responsibilities between the Parties in relation to such AI-supported functionalities is further clarified in Appendix D.

5.4 Confidentiality and Authorized Personnel

a) The Data Processor shall ensure that persons authorized to process Personal Data have committed to confidentiality or are subject to statutory obligations of confidentiality.
b) Confidentiality obligations regarding Personal Data shall remain in effect for as long as the Data Processor processes such data, regardless of termination.
c) All customer data, including customer content (such as call recordings, voicemail, call logs, and messages), is treated as confidential. Personal Data remains confidential until returned or securely deleted in accordance with Clause 7.

5.5 Use of Personal Data

The Data Processor shall process Personal Data only on documented instructions from The Data Controller and solely for the purposes of providing, administering, maintaining, supporting, securing and protecting the Services provided under the Main Agreement.

The Data Processor shall not use Personal Data processed on behalf of The Data Controller for its own independent purposes, including product development, analytics or model training, unless such processing:

a) is based on The Data Controller's documented instructions
b) is required by applicable law or
c) concerns data that has been irreversibly anonymized so that it no longer constitutes Personal Data.

Processing carried out by the Data Processor in its capacity as an independent controller shall take place only where such processing falls outside the scope of this Agreement and is governed by the Data Processor's applicable privacy notice.

5.6 Assistance to The Data Controller

The Data Processor shall assist The Data Controller in fulfilling obligations under applicable Personal Data Legislation, including:

a) Responding to Data Subject rights requests.
b) Conducting Data Protection Impact Assessments and prior consultations with supervisory authorities.
c) Managing Personal Data Breaches.

5.7 Assistance with Data Subject Rights

The Data Processor shall assist The Data Controller in fulfilling its obligations to respond to requests from Data Subjects under Articles 12–22 GDPR, including:

a) Access to Personal Data.
b) Rectification of inaccurate data.
c) Erasure of Personal Data.
d) Restriction of processing.
e) Data portability.
f) Objection to processing.
g) Objection to automated decision-making, including profiling.
h) Such assistance shall be provided without undue delay, to the extent reasonably possible, and in accordance with The Data Controller's documented instructions.

5.8 Sub-Processors and Transfers

a) The Data Processor shall engage sub-processors only in accordance with the authorization framework and conditions set out in Clause 6 (Sub-Processing) and shall ensure that all sub-processors are subject to written obligations that are no less protective than those set out in this Agreement.
b) Transfers of Personal Data outside the EEA shall be carried out only in accordance with Clause 8 (Data Transfers) and subject to appropriate safeguards in compliance with Chapter V GDPR.

5.9 Records and Audit

a) The Data Processor shall maintain records of processing activities and make them available to The Data Controller upon request.
b) The Data Controller may audit the Data Processor's compliance with this Agreement and applicable law upon reasonable notice. Audits shall be conducted in a manner that minimizes disruption and protects confidentiality.

5.10 Demonstration of Compliance and Audits

The Data Processor shall make available to The Data Controller all information

reasonably necessary to demonstrate compliance with this Agreement and applicable Personal Data Legislation.

Audits and inspections shall be conducted in a risk-based, proportionate and non-duplicative manner and, where reasonably possible, shall be satisfied through existing audit reports, certifications, written responses and remote review procedures.

On-site inspections of facilities or systems shall take place only where:

a) required by applicable law or by a competent supervisory authority;

b) reasonably necessary due to substantiated compliance concerns that cannot reasonably be addressed through alternative means; and

c) conducted subject to appropriate confidentiality, security and access procedures.

Nothing in this Clause limits the powers of a competent supervisory authority under applicable law.

5.11 Audit Costs

Each Party shall bear its own costs in relation to audits and inspections carried out under this Agreement. The Data Controller shall bear all costs associated with audits initiated by The Data Controller, including costs of any third-party auditors appointed by The Data Controller. The Data Processor shall bear its own internal costs related to supporting such audits. Where an audit reveals a material non-compliance with this Agreement or applicable Personal Data Legislation attributable to the Data Processor, the Parties may agree that reasonable audit costs shall be borne by the Data Processor.

6 SUB-PROCESSING

6.1 Authorization and List of Sub-Processors

a) The Data Controller grants general authorization for the use of sub-processors, provided that the Data Processor maintains an up-to-date list of approved sub-processors at the following URL: https://www.dstny.se/om/gdpr/sub-processors
b) The Data Processor shall ensure that the list of sub-processors is reviewed and updated at least once per year and whenever a new sub-processor is engaged or an existing one is removed. The updated list shall always remain accessible, and the Data Processor shall maintain and publish a change log indicating the date and nature of each update for full transparency.

6.2 Notification and Right to Object

a) The Data Processor shall notify The Data Controller of any intended changes to the list of authorized sub-processors, including the addition or replacement of sub-processors, in accordance with the procedure set out in Appendix B.2.
b) The Data Controller may object to such changes within the objection period specified in Appendix B.2, provided that the objection is based on reasonable and documented data protection grounds relating to the proposed sub-processor.

6.3 Equivalent Obligations

The Data Processor shall ensure that each sub-processor is bound by written obligations equivalent to those set out in this Agreement, including confidentiality, security measures, and assistance obligations.

6.4 Transfers Outside EEA (Third Countries)

The Data Processor shall store and process Personal Data within the EU/EEA, unless otherwise set out in these Clauses (including the Annexes) or instructed in writing by The Data Controller.

Where a Sub-processor processes Personal Data outside the European Economic Area (EEA) or another jurisdiction recognised by the European Commission as providing an adequate level of protection, such transfer shall be carried out in accordance with the safeguards and mechanisms set out in the Data Transfers provisions of this Agreement.

The Data Processor shall ensure that any Sub-processor is bound by contractual obligations that provide a level of protection for Personal Data equivalent to those set out in this Agreement and applicable Personal Data Legislation.

6.5 Compliance and Evidence

The Data Processor shall verify that sub-processors comply with their contractual obligations and shall provide evidence of such compliance to The Data Controller upon request.

7 OBLIGATION AFTER THE TERMINATION OF SERVICES

7.1 Return or Deletion of Data

Upon termination or expiry of the Main Agreement and this Agreement, the Data Processor shall, at the choice of The Data Controller, either return or securely delete Personal Data processed under this Agreement.

Such return or deletion shall be initiated without undue delay and completed within the timeframes set out in Appendix A / Appendix C, taking into account technical deletion cycles, backup retention, phased decommissioning of systems, and any retention required by applicable law.

Where Personal Data is retained beyond termination due to legal obligations, backup routines, or the agreed retention schedule, such data shall remain subject to the confidentiality and security obligations set out in this Agreement until deleted or irreversibly anonymized.

Upon request, the Data Processor shall provide written confirmation of deletion or a description of the retained data and the basis for such retention.

7.2 Retention for Legal Obligations

Where Union or Member State law requires retention of Personal Data beyond termination, the Data Processor shall notify The Data Controller and ensure that such data remains subject to the confidentiality and security obligations set out in this Agreement until deletion.

8 DATA TRANSFERS

8.1 Transfers Within EEA

Personal Data shall primarily be stored and processed within the EU/EEA.

8.2 Transfers Outside EEA (Third Countries)

A transfer of Personal Data outside the EU/EEA shall take place only where necessary for the performance of the Services and only on The Data Controller's documented instructions. Such documented instructions may be set out in these Clauses, including the Annexes, and shall include the Controller's authorization of sub-processors engaged in accordance with Clause 6 where such sub-processors are located outside the EU/EEA.

8.3 Safeguards for Third-Country Transfers

Where Personal Data is transferred outside the EU/EEA under Clause 8.2, the Data Processor shall implement appropriate safeguards in accordance with Chapter V GDPR, including the latest EU Standard Contractual Clauses or an adequacy decision adopted by the European Commission, or other valid transfer mechanism under Chapter V GDPR. The Data Processor shall maintain agreements with its Sub-processors requiring EU/EEA data residency wherever feasible and shall provide documentation of such safeguards upon request.

8.4 Transparency and Documentation

The Data Processor shall maintain records of all transfers and make them available to The Data Controller upon request. The Data Processor shall notify The Data Controller of any intended changes to Sub-processors that may involve such transfers.

8.5 Clarification Regarding SCC Status

The Parties acknowledge that the provisions of this Agreement are intended to

comply with Article 28 GDPR and do not constitute standard contractual clauses under Article 46(2)(c) or (d) GDPR. These clauses cannot be relied upon as a transfer tool for international data transfers.

9 TERM AND TERMINATION

9.1 Effective Date and Duration

This Agreement shall enter into force on the date of signature by both Parties and shall remain in effect for the duration of the Main Agreement, or as long as the Data Processor processes Personal Data on behalf of The Data Controller.

9.2 Automatic Termination

This Agreement shall automatically terminate upon termination or expiry of the Main Agreement, subject to the obligations set out in Clause 7 regarding return or deletion of Personal Data.

9.3 Termination for Cause

Either Party may terminate this Agreement with immediate effect if the other Party materially breaches its obligations under this Agreement and fails to remedy such breach within 30 days of written notice.

9.4 Survival of Obligations

The provisions relating to confidentiality, liability, audit rights, and obligations after termination (Clause 7) shall survive termination of this Agreement for as long as necessary to fulfill their purpose.

10 MANAGEMENT AND NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

10.1 This Clause (10) constitutes the Parties' complete and exclusive agreement regarding the management, notification, investigation, and documentation of Personal Data Breaches under this Agreement.

10.2 Initial Breach Notification

The Data Processor shall notify The Data Controller's designated contact person without undue delay and, where feasible, no later than twenty-four (24) hours after becoming aware of a Personal Data Breach.

If and to the extent it is not possible to provide all required information at the same time, the Data Processor may provide The Data Controller with the information in phases without undue further delay.

10.3 Investigation and Mitigation

The Data Processor shall without undue delay investigate a Personal Data Breach and undertake appropriate measures to mitigate possible adverse effects of the breach, identify its cause(s), and prevent similar Personal Data Breaches.

The Data Processor shall cooperate with The Data Controller in order to protect the rights and freedoms of natural persons. The Parties shall coordinate any remedial and mitigating actions undertaken or planned.

10.4 Information to be Provided

The notification referred to in Clause 10.2 shall include, to the extent known:

a) the nature of the Personal Data Breach
b) the categories and approximate number of Data Subjects and records affected
c) the likely consequences of the breach and
d) the measures taken or proposed to address the breach and mitigate its possible adverse effects.

10.5 Assistance with Supervisory Authority Notification

The Data Controller is responsible for notifying the competent supervisory authority in accordance with Article 33 GDPR. The Data Processor shall provide reasonable information and assistance to enable The Data Controller to comply with this obligation, including updates as new information becomes available.

10.6 Breach Documentation

The Data Processor shall document all Personal Data Breaches, including the facts relating to the breach, its effects, and the remedial actions taken. This documentation shall be made available to The Data Controller upon request to enable compliance with Article 33(5) GDPR.

10.7 Communication with Data Subjects

Where notification to affected Data Subjects is required under Article 34 GDPR, the Data Processor shall assist The Data Controller in preparing and delivering such communication.

10.8 Investigation and Cooperation

The Data Processor shall cooperate, upon request, with the competent supervisory authority in the performance of its tasks, including providing access to relevant information and systems necessary for investigations or audits, as required by applicable law.

11 RELATIONSHIP TO THE MAIN AGREEMENT

11.1 Integration

This Data Processing Agreement forms an integral part of the Main Agreement between the Parties concerning the provision of telecommunication Products,

Services and, where applicable, Operator Services.

11.2 Hierarchy of Terms

In the event of any conflict between the provisions of this Agreement and the Main Agreement, the provisions of this Agreement shall prevail solely with respect to data protection and privacy obligations.

11.3 Scope

Except as expressly provided in this Agreement, all commercial terms, service levels, and other provisions remain governed by the Main Agreement.

11.4 Amendments

Any amendment to the Main Agreement shall not affect the validity or enforceability of this Agreement unless such amendment expressly refers to and modifies this Agreement in writing.

11.5 Survival

The obligations set out in Clauses 7 (Obligations After Termination) and 9.4 (Survival of Obligations) remain in effect notwithstanding termination of the Main Agreement.

11.6 Limitation of Liability

Except to the extent otherwise required by applicable Personal Data Legislation, the provisions of the Main Agreement relating to limitation of liability, exclusion of indirect damages, dispute resolution and other general contractual provisions shall apply also to claims arising under or in connection with this Data Processing Agreement.

Nothing in this Agreement shall be interpreted as expanding the liability of either Party beyond what follows from the Main Agreement or applicable mandatory law.

12 ADDITIONS AND AMENDMENTS

12.1 Written Form

Any addition or amendment to this Agreement shall be made in writing and communicated to The Data Controller in accordance with the notification process set out in Clause D.2 of this Agreement. For the avoidance of doubt, such amendments shall not require physical signatures or separate written approval by the Parties. Electronic communication of the updated Agreement and continued use of the services after the objection period shall constitute acceptance of the amendment.

12.2 Amendments and Updates

The Data Processor may update this Agreement, including its Appendices, where

reasonably necessary to reflect:

a) changes in applicable Personal Data Legislation;

b) binding guidance or decisions issued by competent supervisory authorities or the European Data Protection Board; or

c) changes to the Services or processing activities that do not materially reduce the level of protection for Personal Data or materially increase the obligations of The Data Controller.

Any such updates shall be notified to The Data Controller in accordance with the procedure set out in Appendix D.

12.3 Regulatory Compliance

The Parties agree to implement any amendments necessary to maintain compliance with applicable Personal Data Legislation, including GDPR and related guidance, without undue delay. Such amendments shall not require renegotiation of commercial terms unless expressly agreed.

12.4 Appendices and Schedules

Updates to appendices and schedules forming part of this Agreement (including the list of sub-processors) shall follow the same notification process as described in Clause D.2. These updates shall not require separate written approval or signatures but will be deemed accepted if no objection is raised within the objection period specified in Clause D.2.

12.5 Version Control and Communication

All amendments shall be dated, version-controlled and communicated to the other Party promptly. The Data Processor shall maintain a record of all amendments and make it available to The Data Controller upon request.

This Agreement has been executed in two (2) originals, of which each Party has taken one.

Place:	Place:
Date:	Date:
Customer Name	**Destiny Sweden AB**
_____	_____
By:	By:

Appendix A - Information about the Processing.

This Appendix supplements Clause 2 (Initial Provisions), 3 (Definitions), and 7 (Obligations After Termination). In case of conflict, the main clauses prevail.

1 The purpose of the Processor's processing of personal data on behalf of the Controller

1.1 The following purposes form the basis of the Processor's processing of personal data on behalf of the Controller, including but not limited to the following examples:

The Processor provides cloud storage, hosting, storage, and backup services to the Controller for the purpose of delivering the agreed communication and collaboration services.

1.2 Provision of one or more of the following services, as applicable to the Controller's use of the Services:

- Mobile telephony
- IP telephony
- PBX functionality
- Integration between internal systems and the Processor's communication platform
- Contact center solutions
- Voice recording
- Online and/or telephone-based meeting functionality
- Related and ancillary services necessary to deliver the above services

2 The Processor's processing of personal data on behalf of the Controller shall mainly pertain to processing activities necessary to provide and operate the Services in accordance with the Main Agreement.

2.1 Such processing activities include, by way of example, the processing necessary to deliver the Services, including the following examples:

The Processor uses personal data provided by the Controller to deliver the requested Services. For example, to enable users to search for colleagues in the PBX system, to display availability status, or to enable integrations with internal systems used by the Controller.

The Processor processes and stores the personal data necessary to enable correct billing of the Services, for example by storing Call Data Records (CDRs) for each call made, in order to calculate usage-based charges.

Where the Controller uses Swedish telephone numbers, the Processor processes number-related information in accordance with applicable telecommunications legislation (LEK – Lag om elektronisk kommunikation). The Processor does not disclose subscriber information to public directory services unless the Controller has obtained the required consent or provided corresponding documented instructions.

2.2 The Processing activities that the Data Processor may perform under the Main Agreement are

Provision of services to Data Controller
- Technical Support including fault correction in accordance with Service Level Agreements (SLA)/ Maintenance & Support Agreements (M&S)
- Application maintenance
- Application development
- Testing activities
- Analyzing and statistical activities
- Marketing activities on behalf of Data Controller (Such marketing activities shall be performed solely on the documented instructions of The Data Controller and only where expressly agreed between the parties)
- Data cleansing, correction of corrupted data

For the avoidance of doubt, the Data Processor may also process personal data relating to The Data Controller's employees, representatives, or users for its own legitimate business purposes, including account management, product communication, service updates, marketing of the Data Processor's services, and product development.

In relation to such processing, the Data Processor acts as an independent Data Controller and not as a Data Processor on behalf of The Data Controller. Accordingly, such processing falls outside the scope of this Data Processing Agreement and is governed by the Data Processor's applicable privacy notice.

2.3 Use of Personal Data

Except as expressly provided in this Agreement or required by applicable law, the Data Processor shall process Personal Data solely for the purpose of providing, operating, supporting and securing the Services for The Data Controller.

The Data Processor shall not use Personal Data processed on behalf of The Data Controller for its own independent purposes, including product development, analytics, profiling, training of artificial intelligence models or other secondary purposes, unless such processing is based on The Data Controller's documented instructions or the Personal Data has been irreversibly anonymized so that it no longer constitutes Personal Data under applicable law.

2.4 Development of apps and customer portals and provision of services in relation hereto:

a) The processor provides services in relation hereto, including IT architecture and development resources

2.5 AI-supported services and use of Customer Content

To the extent that the Services include AI-based, automated or machine-learning-supported functionalities (including but not limited to voice recording, transcription, analysis of calls or meetings, chat functionality or similar features), Customer Content, including call recordings, transcripts, chat content, audio material and text

material, shall be processed solely for the purpose of providing, securing, maintaining, supporting and improving the Services and AI Services within the Controller's use of the Services.

Customer Content containing Personal Data shall not be used to train, develop or improve general-purpose or third-party artificial intelligence or machine learning models, nor for any other secondary purpose, unless expressly instructed by The Data Controller or otherwise expressly agreed in writing.

For the avoidance of doubt, this restriction applies to identifiable Customer Content and does not prevent the Data Processor from using data that has been effectively anonymized in accordance with Clause 2.5.

2.6 Anonymization and Use of Anonymized Data

To the extent technically feasible and in accordance with applicable Personal Data Legislation, the Data Processor may anonymize Personal Data processed under this Agreement.

Anonymization shall be carried out using industry-recognized techniques designed to ensure that:

- The data subject is no longer identifiable by any means reasonably likely to be used by the Data Processor or any third party.
- The anonymization is irreversible.
- The anonymized data cannot be re-identified through combination with other data available to the Data Processor.
- The anonymization process does not result in the disclosure of Personal Data, confidential information, or trade secrets.

Data that has been effectively anonymized and no longer constitutes Personal Data under applicable law shall fall outside the scope of this Agreement and the GDPR.

The Data Processor shall implement appropriate technical and organizational measures to prevent re-identification of anonymized data and shall not attempt to re-identify such data.

Upon reasonable request, the Data Processor shall provide general information regarding the anonymization methodology applied.

Use of Anonymized Data

Where Personal Data has been anonymized in accordance with this Clause 2.6, the Data Processor may use such anonymized data for legitimate business purposes, including:

- Monitoring and improving the performance, security, and reliability of the Services.
- Developing, testing, and improving features and functionalities, including AI-supported functionalities.
- Statistical analysis and service optimization.

- Product development and quality assurance.

Such use shall not involve re-identification of data subjects and shall not permit the identification of the Controller, its users, or its customers.

3 The processing includes the following types of personal data about data subjects.

3.1 The processing includes personal data relating to the following categories of data subjects:

a) the Controller’s employees and other authorized users of the Services
b) authorized users of the Controller and external individuals or organizations communicating with such users via the Services
c) other individuals whose personal data is processed by the Controller through use of the Services.

name, address, phone number, e-mail, username for one or several systems, password to one or several systems, billing and accounting documents, IP-address, information about users' used device, various categories of personal data processed in connection with the delivery and use of the Services, the scope and content of which are determined by the Controller, personal data stored in the Controller’s systems to which access is granted by the Controller for the purposes of support, maintenance or troubleshooting, various personal data provided or recorded by the customer or the customer's customers without the organization's active processing and identification thereof.

The categories of personal data processed may include, without limitation, the following:

- Name
- UserID
- Password
- Email address
- Phone number
- IP Address
- User generated content (such as call lists etc.)
- User behavior (trouble shooting, crash reports etc.)
- Billing information - formats for calls, SMS and data (CDR files)

In addition, users may also upload personal data such as profile pictures, job title, address, further contact details, and similar user-generated content.

The following special categories of personal data may be incidentally and unintentionally processed where such information is voluntarily disclosed by users through use of the Services. The Data Processor does not actively seek, require, structure, or determine the processing of special categories of personal data, and such processing occurs solely as a consequence of user-generated content and on the documented instructions of the Controller:

- Chat conversations, where the Controller’s users choose to disclose such information when using chat or messaging functionality.
- Call recordings, where call recording functionality is enabled by the Controller and users disclose such information during recorded calls.

3.2 Information containing personal identification numbers may be processed where required by applicable law, for example in connection with phone number porting where the ported number belongs to an end user.

3.3 The Processor shall implement appropriate measures designed to ensure that access to Personal Data is restricted to authorized personnel on a need-to-know basis.

4 Processing includes the following categories of data subject

4.1 Current employees and former employees of the Controller; employees and other authorized users of the Controller (where the Controller is a legal entity); end users and other individuals communicating with or whose personal data is processed by the Controller through use of the Services; and employees of the Controller's customers, where applicable.

5 The Processor's processing of personal data on behalf of the Controller shall commence upon the commencement of the Clauses. The processing has the following duration:

5.1 Processing continues for the duration of the Main Agreement. Upon termination, return or erasure shall be carried out in accordance with Clause 7 of this Agreement.

Appendix B - Approved Sub-Processors.

This Appendix supplements Clause 6 (Sub-processing). In case of conflict, the main clauses prevail.

1 Approved sub-processors

1.1 https://www.dstny.se/om/gdpr/sub-processors

The sub-processor registry distinguishes between sub-processors engaged for core service delivery and sub-processors engaged for optional supplementary services. Sub-processors engaged in optional services process Personal Data only where the Controller has activated or uses the relevant service.

2 Notification and Objection Procedure for Sub-Processor Changes

2.1 Notification of Changes

Where the Data Processor intends to add or replace a sub-processor, the Data Processor shall notify The Data Controller in writing prior to such change.

- When such changes occur, The Data Processor will notify the individual designated as the Administrator of the Agreement within The Data Controller's organization.
- All notifications will be sent from dpo@dstny.se and will include a summary of the changes introduced such as the identity of the proposed sub-processor and a description of the services to be provided.
- If additional individuals within The Data Controller's organization wish to

receive these notifications, they may subscribe via https://dstny.se/dpa.
- It is the responsibility of The Data Controller to ensure that any additional recipients are registered through this process.

2.2 Objection Period and Procedure

The Data Controller may object to the proposed sub-processor within 30 calendar days of receipt of the notification, provided that the objection is based on reasonable and documented data protection grounds relating to the proposed sub-processor.

Any objection must be submitted by email to dpo@dstny.se and must clearly state:

- That the communication is an objection to the change.
- The identity of the Customer making the objection.
- The specific change(s) that are considered unacceptable, including the reason(s) for the objection.

2.3 Consequences of Objection

a) Where The Data Controller raises a valid objection, the Parties shall cooperate in good faith to seek a commercially reasonable resolution.
b) If no such resolution can be reached, The Data Controller may terminate the affected Services without penalty.
c) Where the affected Services cannot reasonably be provided without the proposed sub-processor, and no alternative solution is available, The Data Controller may terminate the Agreement with respect to those Services.

2.4 Deemed Acceptance

If no objection is received within the objection period, The Data Controller shall be deemed to have accepted the proposed sub-processor.

Appendix C - Instruction Pertaining to the use of Personal Data.

This Appendix supplements Clause 5 (Obligations of the Data Processor), 7 (Obligations After Termination), and 8 (Data Transfers). In case of conflict, the main clauses prevail.

1 The subject of/instruction for the processing

1.1 Delivers telecommunication products, services and, where applicable, operator services to The Data Controller.

2 Security measures shall comply with Clause 5.

2.1 Security of processing

The level of security shall take into account:

The nature, scope, context and purposes of the processing activity
as well as the risk for the rights and freedoms of natural persons, the Processor must implement an appropriate level of security.

2.2 The Processor shall determine and implement appropriate technical and organizational security measures in accordance with Article 32 GDPR, taking into account the risks associated with the processing.

2.3 Organizational security

a) All personnel are regularly trained in personal data handling and best practices recommendations for security, in cooperation with the Data Processing Officer.
b) Appropriate personnel screening and vetting measures are applied, where permitted by applicable law and proportionate to the role and associated risks.
c) Written privacy agreement between The Data Processor and Data Processors Personnel.

2.4 Systems security

a) Secure software development practices are implemented in accordance with recognized industry standards, such as the OWASP Top 10 (as updated from time to time), where applicable.
b) Firewall security
c) Logging and monitoring measures are implemented to support the detection, investigation, and prevention of unauthorized access and security incidents, where appropriate.
d) Appropriate authentication mechanisms are implemented, including role-based access and credential management, commensurate with the risks associated with the processing.
e) Audit system for log files, with securely stored information
f) Data retention policy and systems when user is removed, personal data is also removed.
g) Encryption for data in transit is implemented using TLS version 1.2 or higher, or equivalent or stronger cryptographic protocols, for HTTPS and SIP/TLS, in accordance with recognized industry standards and the requirements of Article 32 GDPR.
h) Secured backups for data loss prevention.

2.5 Physical security

a) Physical access to facilities used for the processing of Personal Data is restricted and logged through appropriate access control measures.
b) Appropriate alarm and intrusion detection systems are implemented at facilities used for the processing of Personal Data, where proportionate to the risks associated with such facilities.
c) Physical security controls, such as video surveillance and/or physical supervision, are implemented where appropriate and in accordance with applicable law.

3 Assistance to the Controller

3.1 The Processor shall insofar as this is possible – within the scope and the extent of the

assistance specified below – assist the Controller in accordance with Clause 8.1 and 8.2 by implementing the following technical and organizational measures:
If the Controller receives a request for the exercise of one of the rights of the data subjects in accordance with applicable data protection law, and a proper reply to the request requires assistance from the Processor, the Processor shall assist the Controller with the necessary and relevant information and documentation as well as appropriate technical and organizational security measures.

a) If the Controller requires the Processor's assistance to respond to a request from a data subject, the Controller shall submit a written request for assistance to the Processor. The Processor shall provide such assistance in accordance with Clause 5.5 of this Agreement.
b) If the Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other people than the Controller, and the
c) request concerns personal data processed on behalf of the Controller, the Processor shall without undue delay forward the request to The Controller.

4 Storage period/erasure procedures

4.1 Return or erasure shall follow Clause 7.

a) Personal Data will be Processed for as long as necessary for the purpose of providing the service under the Main Agreement.
b) After termination of services, data is phased out within 6 months for: Provision of services to Data Controller.
c) Application maintenance, Application development.
d) Technical support (incl. fault corrections in accordance with Service Level Agreements), Testing activities.

4.2 Within 24 months:

a) Analytics and statistical activities.

5 Processing location

5.1 Processing of the personal data under the Clauses shall take place at the Processor's own locations or at locations of approved Sub-processors as specified in Appendix B (and/or the Processor's Sub-processor registry, where applicable), unless otherwise authorized in writing by the Controller.

5.2 Personal Data is located in Sweden at local data centers and within the borders of the EEA for cloud services, except where third-country transfers are set out in this Annex and/or are otherwise instructed in writing by the Controller. The Data Processor can provide a detailed list of processing locations upon request.

6 Transfers outside EEA

6.1 Transfers outside the EU/EEA shall comply with Clause 8. Where required for the performance of the Main Agreement, the Data Processor transfers Personal Data to the following third country/countries: United States of America (USA). Such transfers are carried out on the basis of a valid transfer mechanism under Chapter

V GDPR, including (where applicable) the data importer's certification under the EU-U.S. Data Privacy Framework (see certified organizations here: https://www.dataprivacyframework.gov/list) and/or the latest EU Standard Contractual Clauses.

6.2 If the Controller does not provide documented instructions in these Clauses (including this Annex) or subsequently in writing with regard to a transfer of personal data to a third country, the Processor is not entitled to carry out such transfer within the scope of these Clauses.

6.3 Transfer of personal data shall in all cases only be carried out in accordance with these Clauses, on the documented instructions of the Controller and to the extent permitted by applicable data protection law.

6.4 Where, in accordance with these Clauses, the Processor transfers personal data to Sub-processors in third countries outside the EU/EEA, the Processor shall ensure that a valid transfer mechanism pursuant to Chapter V GDPR is in place and that corresponding obligations are imposed on the Sub-processor.

7 Procedures for the Controller's audits, including inspections, of the processing of personal data being performed by the Processor. Reference to Clauses 5.8 – 5.10.

7.1 The Processor shall, upon the Controller's written request, document to the Controller that the Processor is complying with his obligations under these Clauses and the Instruction, and with the relevant articles in the GDPR in regards to the personal data being processed on behalf of the Controller.

7.2 According to Clause C.7.1 The Processor's documentation shall be sent to the Controller within a reasonable time after receiving the request.

7.3 The Processor must provide the Controller with documentation of continuous compliance with the provisions. These self-audit reports must be prepared at least once per year and shall follow the principles and control objectives of ISO/IEC 27701:2019.

Such self-audit reports may be used by the Controller as part of its information gathering and assurance activities and must be signed by the Processor's management.

7.4 Regardless of Clause C.7.3, the Processor shall provide for and contribute to audits and inspections performed by auditors appointed by the Controller or by competent public authorities, to the extent necessary and proportionate to verify the Processor's compliance with these Clauses and applicable data protection law.

The auditor must be subject to confidentiality under law or agreement. The Controller must notify such audits in writing with at least 30 calendar days' notice.

7.5 Audits and inspections under Clauses C.7.3 and C.7.4 shall be conducted in a risk-based, proportionate, and non-duplicative manner.

Where a valid and up-to-date self-audit report or third-party audit report

reasonably covers the scope of a proposed audit, the Parties shall cooperate in good faith to avoid overlapping audits and may agree to rely on existing documentation, unless additional auditing is required due to regulatory obligations, substantiated compliance concerns, or instructions from a competent supervisory authority.

7.6 Procedures for audits, including inspections, of the processing

of personal data being performed by sub-processors.

7.7 The Data Processor shall, at a minimum, conduct an annual review of the sub-processors at its own expense.

Appendix D - The Parties' terms of Agreement on Other Subjects.

This Appendix supplements Clause 5 (Obligations of the Data Processor) and 12 (Additions and Amendments). In case of conflict, the main clauses prevail.

1 Note on the procedure for The Data Controller's audits in Clause C.7

1.1 In order to ensure an appropriate level of security and operational integrity, physical inspections of the Data Processor's data centre facilities are not carried out in practice.

Instead, the Data Processor demonstrates compliance with its obligations under this Agreement through documented assurance measures, including the provision of annual self-audit reports prepared in accordance with Clause C.7.3 and aligned with the principles and control objectives of ISO/IEC 27701:2019.

Such documentation is intended to provide The Data Controller with a meaningful and proportionate means to verify compliance in accordance with Article 28 GDPR.

2 Update of the Data Processing Agreement

2.1 The Parties acknowledge that this Data Processing Agreement may be updated from time to time to reflect changes in applicable data protection law, binding guidance issued by supervisory authorities or the European Data Protection Board, or established data protection practice.

- The Data Processor may introduce such updates, including clarifications, where necessary to maintain compliance with applicable Personal Data Legislation.
- Such updates shall not materially reduce The Data Controller's rights or increase its obligations under this Agreement.
- Any updates shall be communicated to The Data Controller in accordance with the notification procedure set out in Clause D.2.2 and shall apply only to the extent permitted under applicable data protection law and this Agreement.

For transparency and reference purposes, the current version of the Data Processing Agreement is made available at https://dstny.se/dpa

2.2 Notification Process

- When such changes occur, the Data Processor will notify the individual designated as the Administrator of the Agreement within The Data Controller's organization.
- All notifications will be sent from dpo@dstny.se and will include a summary of the changes introduced.
- If additional individuals within The Data Controller's organization wish to receive these notifications, they may subscribe via https://dstny.se/dpa.
- It is the responsibility of The Data Controller to ensure that any additional recipients are registered through this process.

2.3 Objection Period and Procedure

After receiving a notification about a change, The Data Controller has 14 calendar days to object if the change cannot reasonably be accepted. Any objection must be submitted by email to dpo@dstny.se and must clearly state:

- That the communication is an objection to the change.
- The identity of the Customer making the objection.
- The specific change(s) that are considered unacceptable, including the reason(s) for the objection.

If no objection is received within the objection period, continued use of the services after this period shall constitute acceptance of the updated agreement.

This provision does not apply to changes in the use of sub-processors, which are regulated in Clause 6 and Appendix B of the agreement.

2.4 Any updates to the Services, sub-processing arrangements or processing activities shall not materially reduce the level of protection for Personal Data or the rights of The Data Controller under this Agreement.

3 AI-Supported Functionalities – Regulatory Allocation of Responsibilities

The Parties acknowledge that:

The Data Controller determines the purposes for which AI-supported functionalities are used within its organization and remains responsible for ensuring that such use complies with applicable law, including conducting any required risk assessments, impact assessments or internal governance measures required under data protection or artificial intelligence legislation.
For the avoidance of doubt, the Customer's use of AI-supported functionalities remains subject to the restrictions set out in the Section 5 of the General Terms to the Main Agreement regarding prohibited or restricted AI use cases, including high-risk AI systems under Regulation (EU) 2024/1689 (EU AI Act).

The Data Processor is responsible for ensuring that AI-supported components under its control are developed, maintained, and operated in accordance with applicable legal requirements relevant to its role as a service provider.

The Data Processor shall, upon reasonable request, provide information necessary to enable The Data Controller to assess the compliance of its use of AI-supported functionalities with applicable law, taking into account the nature of the Services and the Data Processor's role.

Nothing in this clause shall be interpreted as permitting the use of AI-supported functionalities in prohibited or restricted use cases defined elsewhere in the Agreement.

Nothing in this Appendix shall be interpreted as transferring The Data Controller’s statutory responsibilities under applicable law to the Data Processor, nor as limiting the Data Processor’s independent legal obligations where such obligations apply.