PERSONAL DATA PROCESSING AGREEMENT

The Customer

and

Destiny Sweden AB

1 PARTIES

1.1 **The Customer** hereinafter the "**Data Controller**"; and

1.2 **Destiny Sweden AB,** Reg. No. 556377-2317, Lumaparksvägen 11, 120 31 Stockholm, hereinafter the "**Data Processor**".

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

2 INITIAL PROVISIONS

2.1 The Parties have entered into an agreement regarding certain mobile and telecommunication services (hereinafter the "**Main Agreement**") under which the Data Processor will process Personal Data on behalf of the Data Controller.

2.2 The Parties have entered into this personal data processing agreement (including any schedules), hereinafter the "**Agreement**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the processing of Personal Data by the Data Processor on behalf of the Data Controller.

3 DEFINITIONS

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

"Personal Data Legislation"	means applicable Swedish legislation regarding the processing of Personal Data or the common EU rules on data protection, especially the General Data Protection Regulation (EU) 2016/679 (GDPR); and
"Third Country"	means a country or territory outside the European Economic Area ("**EEA**").

The specific concepts and terms which relate to processing of Personal Data and which are not defined in the Agreement shall have the same meaning as in applicable Personal Data Legislation.

4 OBLIGATIONS OF THE DATA CONTROLLER

4.1 The Data Controller shall ensure that processing of Personal Data, including instructions to the Data Processor, is executed in accordance with applicable Personal Data Legislation (including securing any required notices and obtaining any

required consents and/or authorizations, or otherwise securing a lawful basis for Processing under applicable Personal Data Legislation).

4.2 By entering into this Agreement, the Data Controller confirms that the technical and organizational measures that are described in Appendix Schedule 1 have been found to be appropriate to protect the Personal Data under the scope of this Agreement and that Data Processor hence has provided sufficient guarantees according to Art. 28 (1) of the GDPR.

5 OBLIGATIONS OF THE DATA PROCESSOR

5.1 The Data Controller instructs the Data Processor to only process Personal Data according to its lawful instructions, that have been described in Schedule 1 (instructions to the Data Processor). It is the Data Controller's responsibility to ensure that the instructions are not contrary to Personal Data Legislation.

5.2 In addition to what otherwise follows from the Agreement, the Data Processor undertakes:

a) to assist the Data Controller in ensuring compliance with the obligations deriving from applicable Personal Data Legislation, taking into account the nature of Processing and the information available to the Data Processor;

b) to immediately inform the Data Controller if, in the Data Processors opinion, an instruction infringes the applicable Personal Data Legislation and the Data Processor is then not obligated to carry out the relevant Processing until the parties have decided how to solve the matter or until a supervisory authority declares the instruction as lawful.

c) to implement appropriate technical and organisational measures according to Schedule 1 in order to protect and safeguard the Personal Data that is Processed against Personal Data Breaches (Data Processor may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are not less protective of the Personal Data as those set out in Appendix 1);

d) to maintain records of all categories of Processing performed on behalf of the Data Controller, including name and contact details and, where applicable, transfers of Personal Data to a Third Country or international organisation and, where possible, a general description of the technical and organisational security measures;

e) to ensure that only authorised persons can Process Personal Data, and ensure that these persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

f) to without undue delay refer any third party requesting information relating to the Personal Data to the Data Controller, unless such reference is prohibited under criminal law (*e.g.* to preserve the confidentiality of a law enforcement investigation) and on request cooperate with relevant supervisory authority in the performance of its tasks and without undue delay inform the Data Controller of this;

g) to assist the Data Controller through appropriate technical and organisational measures, to the extent possible, so that the Data Controller can fulfil its obligation to respond to a request following a data subject exercising its rights under applicable Personal Data Legislation;

h) to, considering the type of Processing and the information available to the Data Processor, at the request of the Data Controller, assist the Data Controller in ensuring that the obligations regarding carrying out an impact assessment for data protection and preceding consultation with responsible supervisory authority, are met in accordance with applicable Personal Data Legislation;

i) to transfer Personal Data belonging to the Data Controller, to a third country, provided that: (a) the third country according to a decision issued by the EU Commission provides an adequate level of protection for Personal Data which comprises the Processing of Personal Data; (b) Data Processor ensures that there are appropriate safeguards in place in accordance with Personal Data Legislation, e.g. standard data protection clauses adopted by the EU Commission under applicable Personal Data Legislation, that comprises the transfer and the Processing of Personal Data; or (c) if there are any other exemptions under applicable Personal Data Legislation that comprise the Processing of Personal Data; and

j) to make available to the Data Controller, upon the Data Controller's request, information in order to demonstrate compliance with the obligations of Data Processor laid down in Art. 28 GDPR. The audit shall be carried out by the Data Controller or such independent third party that the Data Controller appoints (that is not a competitor to the Data Processor), provided that such person is bound by a duty of confidentiality (which the Data Processor in its reasonable opinion considers to be acceptable). Data Controller shall bear any costs arising out of or in connection with an audit.

6 SUB-PROCESSING

6.1 The Data Processor has the right to engage or replace third parties as sub-processors for the Processing of Personal Data in accordance with this Agreement (so called "Sub-processing") provided that the Data Processor and the Sub-processor enters into a written contract and that the Sub-processing complies with requirements at least as strict as set out in this Agreement and under Personal Data Legislation. For purpose of ensuring the lawful transfer of Personal Data to any Third Country (where such has been approved by the Data Controller under the terms set

out herein), the Data Controller authorises the Data Processor in each such case to enter into standard contractual clauses (SCC) (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en) with any sub-processors in the Data Controller's name and on its and the Data Processor's behalf. The Data Processor shall further keep the Data Controller informed of any new appointments or replacement of Sub-processors and provide the Data Controller with the possibility to object to a change of Sub-processors.

6.2 The Data Processor shall maintain records of sub-processors who are Processing Personal Data and shall at the reasonable request of the Data Controller provide a list of these.

6.3 The Data Processor shall remain liable to the Data Controller for the performance of any sub-processor's obligations.

7 OBLIGATION AFTER THE TERMINATION OF SERVICES

7.1 The Parties agree that on the termination of the Main Agreement, the following shall apply. The Data Processor shall (and, where applicable, ensure that the sub-processor shall) delete all Personal Data, unless the Data Processor is required to store the Personal Data under Union or national law, or the Data Controller instructs the Data Processor to return the Personal Data (if so, the Data Processor's shall delete existing copies of such data (unless not required to store the Personal Data under Union or national law).

8 TERM AND TERMINATION

8.1 This Agreement shall enter into force when signed by the Parties and shall remain in force as long as the Data Processor Processes Personal Data on behalf of the Data Controller.

8.2 A Party is entitled to terminate this Agreement with immediate effect should the other Party commit a material breach of its obligations pursuant to this Agreement which is not remedied within thirty (30) days of such Party being notified of such breach by the non-defaulting Party. Instructions given to the Data Processor in conflict with applicable Personal Data Legislation shall always constitute a material breach of the Agreement and the Main Agreement.

8.3 Termination of this Agreement shall be without prejudice to any rights and obligations of either Party against the other which may have accrued up to the date of such termination.

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

9.1 The Data Processor shall without undue delay notify the Data Controller's designated contact person after having become aware of a Personal Data Breach. If and to the extent it is not possible to provide all information at once, the Data Processor may provide the Data Controller with the information in batches without further delay.

9.2 The Data Processor shall without undue delay investigate a Personal Data Breach and undertake measures to mitigate possible adverse effects of the Personal Data 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 registered natural persons. The Parties undertake to coordinate remedial and mitigating actions which are undertaken and planned.

10 RELATIONSHIP TO THE MAIN AGREEMENT

10.1 If not explicitly stated otherwise, the terms and conditions (including but not limited to provisions of limitations of liability) of the Main Agreement shall also apply to the Agreement.

11 ADDITIONS AND AMENDMENTS

No amendments or additions to this Agreement may be made except in writing, duly signed by each of the Parties.

SCHEDULE 1

INSTRUCTIONS TO THE DATA PROCESSOR

1 PURPOSE WITH THE PROCESSING

The purpose with the Processing is to ensure that Destiny can deliver, support and fulfill its responsibilities as your communications provider.

2 PROCESSING ACTIVITIES

The Processing activities that the Data Processor will 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
- Analysing and statistical activities
- Marketing activities on behalf of Data Controller (when expressly agreed with Data Controller)
- Data cleansing, correction of corrupted data

3 CATEGORIES OF DATA SUBJECTS

The categories of data subjects affected are

- Data Controller´s employees and consultants and Data Controller´s representatives

4 CATEGORIES OF PERSONAL DATA SUBJECT TO PROCESSING

The Personal Data that may be Processed are

- Name
- UserID
- Password
- Email address
- Phone number
- IP Address
- User generated content (such as call lists etc.)
- User behaviour (trouble shooting, crash reports etc.)
- Billing information

In addition, users may also upload personal data such as profile pictures, job title, address, further contact details etc.

5 SENSITIVE PERSONAL DATA

The sensitive Personal Data that may be Processed are

- Chat conversations in cases the customer's users are using that function/service.
- Call recording if the call recording service is a part of the Data Processor's service.

6 PERSONAL IDENTIFICATION NUMBER

Information containing personal identification number is subject to Processing in the case of phone number porting, where the phone number ported, belongs to the end user and not the customer.

7 SECURITY

Organizational security

- All personnel is regularly trained in personal data handling and best practices recommendations for security, in cooperation with the Data Processing Officer.
- Background checks made prior to employment on personnel.
- Written privacy agreement between the Data Processor and Data Processor's Personnel.

Systems security

- OWASP 2017 guidelines has been followed to secure http interface to protect against high risk problem areas where applicable.
- Firewall security
- Monitoring and surveillance systems.
- Authentication systems for secure access.
- Audit system for log files, with securely stored information
- Data retention policy and systems when user is removed, personal data is also removed.
- Only encryption TLS 1.2 is allowed for HTTPS and SIP/TLS.
- Secured backups for data loss prevention.

Physical security

- Restricted and logged access at physical facilities containing personal data
- Alarm system at physical facilities containing personal data
- Video surveillance and/or physical supervision at facilities containing personal data.

8 ACCESS TO THE REGISTER

Support, Sales, Backoffice, Delivery and Technical Operations personnel at the Data Processor.

9 SUB-PROCESSORS

The Data Processor has a general mandate from the Data Controller to contract sub-contract sub-processors, necessary for the services the Data Controller has requested.

The Data Processor confirms that sub-processors used, have signed a sub-data processor agreement on terms corresponding to this Agreement with such sub-data processor.

The sub-processors engaged by the Data Processor are listed in Schedule 2.

10 PLACE OF PROCESSING

Personal Data is located in Sweden at local data centres and within the borders of the EEA for cloud services. The Data Processor can provide a detailed list of location upon request.

11 TRANSFER TO THIRD COUNTRIES

Any transfer of Personal Data outside the EEA to a country which has not received an adequacy decision by the European Commission shall be governed by appropriate safeguards as laid down in Chapter V of the GDPR.

12 DATA RETENTION

Personal Data will be Processed for as long as necessary for the purpose of providing the service under the Main Agreement.

After termination of services, data is phased out within 6 months for:
Provision of services to Data Controller,
Application maintenance,
Application development,
Technical support (incl. fault corrections in accordance with Service Level Agreements),
Testing activities,

Within 24 months:
Analysing and statistical activities,
Marketing activities (when expressly agreed with Data Controller),

13 AUDIT

The Data Controller may once a year perform an audit to make sure the Data Processor is in compliance with the GDPR in practice.
The Data Controller must submit a written request within a minimum of 4 weeks before the Data Controller wishes to perform an audit.
The Data Processor has the right to deny the request in cases where there may be integrity- or security risks involved.

SCHEDULE 2

List of Sub-processors

Updated 2022-04-05

Name	Type of Service	Country
Amazon S3	Storage	Germany
Advantops AB (fd Voiceprovider AB	Contact center	Sweden
Apsis Group AB	Newsletters etc.	Sweden
Aurora Innovation AB	Call booking	Sweden
Destiny Analytics	Statistics provider	Ireland
Destiny for Service Providers AB	Technology provider	Sweden
Dustin Group AB	Network consultants	Sweden
Emvico AB	Software development	Sweden
Fortnox AB	Customer billing	Sweden
Generic Mobile		Sweden
GTT	International numbers	Sweden
ID-Kollen i Sverige	Identification service	Sweden
IT Consultants AB	IT Consultants	Sweden
Leissner data AB	Technology provider	Sweden
Line Carrier	International numbers provider	Finland
Microsoft Office 365	Email correspondence, documents	Ireland, The Netherlands
Promobility AB	Hardware distributor	Sweden
Puzzel AB	Contact center	Sweden, Norway
Relation & Brand AB	Customer Delivery system	Sweden

Responda AB	Answering service	Sweden
Setera	International numbers	Sweden
Svenska Coegi AB	IT Consultants	Sweden
Tele2 AB	Internet service provider	Sweden
Telenor Sverige AB	Service Provider	Sweden
Upsales Nordic	Customer registry	Sweden
Westcon AB	Hardware distributor	Sweden
Zendesk Inc.	Ticketing system	Ireland, Germany
Zisson AB	Contact center	Sweden