NASSTAR

DATA PROCESSING TERMS

NASSTAR

Contents

1 Introduction

These Data Processing Terms shall form part of and be incorporated into each Contract in relation to which Nasstar processes personal data.

2 Relationship of the parties

2.1 The parties agree that they may each process various types of personal data in relation to the performance and receipt of the Services and the parties' respective business operations.

2.2 Each party shall comply with its obligations under these Data Processing Terms and under Data Protection Laws with respect to the types of personal data it processes in connection with the Contract and according to its responsibilities as a controller, processor or joint controller (as appropriate) for the relevant personal data, as described in the Nasstar Data Processing Schedule.

3 Controller obligations

Whenever a party is acting in a capacity as a controller in relation to personal data, it shall comply in all respects with Data Protection Laws and shall:

a) process such data fairly and lawfully;

b) implement appropriate technical and organisational measures to protect such personal data against Data Security Incidents; and

c) provide all assistance reasonably required by the other party in order for that other party to comply with such obligations, including with respect to data subject access requests.

4 Processor obligations

4.1 Where a party (the "**Processor**") is processing personal data on behalf of the other party, whether as a processor or sub-processor, and not as a controller or joint controller, the following provisions shall apply:

4.2 Purpose limitation

The Processor shall process the personal data as necessary: (i) to perform its obligations under the Contract including these Data Processing Terms; (ii) to comply with its obligations under Law; and (c) to enhance the Services (the "**Permitted Purpose**"), except where otherwise required by any Law. In no event shall the Processor process the personal data for its own purposes or those of any third party.

4.3 Documented instructions

The Processor shall process the personal data only on documented instructions from the other party, which may include the instructions set out in the Contract including these Data Processing Terms, and shall immediately inform the other party if, in its opinion, an instruction infringes Data Protection Laws.

4.4 Categories of personal data

a) The parties agree that the categories of personal data that are processed in connection with the Contract may include CRM Data, User Data, Communications Data and Content Data. The Nasstar Data Processing Schedule identifies when Nasstar processes such categories of personal data in the provision of services to its customers and whether Nasstar is acting as a controller or Processor for the purposes of such processing.

b) Nasstar may amend or update the Nasstar Data Processing Schedule from time to time by making available a revised version.

c) In the event that Nasstar wishes to amend its responsibility as a controller or Processor as set out in the Nasstar Data Processing Schedule or materially change the categories of personal data that Nasstar processes as a Processor in connection with the provision of the Services, Nasstar will endeavour to give the Customer at least 30 days' written notice of the change.

d) Where Nasstar is acting as a Processor, it is the Customer's responsibility to determine if any further details of Nasstar's activities need to be recorded in the Contract to comply with Data Protection Laws and Nasstar shall act in good faith to cooperate with any reasonable request to do so.

4.5 International transfers

The Processor shall not permit any processing of personal data outside European Economic Area or the United Kingdom (as appropriate) unless:

a) the Processor first puts in place adequate transfer mechanisms to ensure the transfer is in compliance with Data Protection Laws;

b) the Processor or the relevant Authorised Sub-Processor is required to transfer the personal data to comply with Law, in which case the Processor will notify the other party of such legal requirement prior to such transfer unless such Law prohibits such notice from being given to the other party; or

c) the Processor is entitled to rely on a permitted derogation under Data Protection Laws in order to transfer the personal data outside of the European Economic Area or the United Kingdom (as appropriate), which may include circumstances where (among other things): (i) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (ii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; or (iii) the transfer is necessary for the establishment, exercise or defence of legal claims.

4.6 For the purposes of paragraph 4.5a), the adequate transfer mechanisms may include: (i) transferring the personal data to a recipient in an Adequate Territory, (ii) transferring the personal data to a recipient that has achieved binding corporate rules authorisation in accordance with Data Protection Laws, or (iii) transferring the personal data to a recipient that has executed Standard Contractual Clauses and, where appropriate, additional safeguards. Where the Processor is established within the European Economic Area or the United Kingdom (as

appropriate) and transfers personal data to a sub-processor located outside of the European Economic Area or the United Kingdom (as appropriate), the Processor shall have the right to enter into Standard Contractual Clauses and, where appropriate, additional safeguards with the sub-processor for and on behalf of the Controller, whether on a named or an undisclosed basis.

4.7 Confidentiality of processing

The Processor shall ensure that any person that it authorises to process the personal data (including the Processor's staff, agents and subcontractors) (each an "**Authorised Person**") shall be under an obligation (whether under contract or statute) to keep the personal data confidential.

4.8 Security

The Processor shall implement appropriate technical and organisational measures to protect the personal data from Data Security Incidents. Such measures shall have regard to the state of the art, the costs of implementation 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. Where Nasstar is the Processor, it shall comply with its Security Policy.

4.9 Sub-processing

a) The Processor shall be authorised to engage third parties to process personal data on behalf of the controller, provided that it notifies the other party of such engagement (each, an "**Authorised Sub-Processor**").

b) Where Nasstar is Processor and the Customer is Controller, the Customer hereby gives its specific written authorisation to the third parties listed as Authorised Sub-Processors in the Nasstar Data Processing Schedule processing personal data on the Customer's behalf and to Nasstar transferring and/or disclosing the Customer's personal data to those Authorised Sub-Processors, if and to the extent this is required either for the provision of the Services or their proper operation or for troubleshooting and incident rectification or otherwise to enable Nasstar to comply with its obligations under the Contract.

c) The Processor will ensure that there is in place a written contract between the Processor and the Authorised Sub-Processor that specifies the Authorised Sub-Processor's processing activities and imposes on the Authorised Sub-Processor terms equivalent in all material respects as those imposed on the Processor in this paragraph 4. The Processor will remain responsible for the acts and omissions of Authorised Sub-Processors in respect of their processing of personal data as if they were its own.

d) Where the Processor is instructed by the other party to grant access to personal data to a third party who is contracted to the other party (a "**Contracted Third party**"), the Contracted Third party shall not be a sub-processor of the Processor for the purposes of this paragraph 4.9 and the other party shall have sole responsibility for putting in place an appropriate data processing agreement or data transfer agreement (as appropriate) with the Contracted Third party which complies with Data Protection Laws.

4.10 Cooperation

The Processor shall:

a) taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising data subjects' rights;

b) assist the controller in implementing appropriate technical and organisational measures against Data Security Incidents, completing data protection impact assessments and notifying Data Security Incidents to the competent supervisory authority or to the data subjects concerned, as required by Data Protection Laws and taking into account the nature of the processing and the information available to the Processor.

If compliance with this paragraph 4.10 requires: (i) a change to the Services performed by Nasstar, (ii) a change to the Contract under which the relevant Services are provided, or (iii) the expenditure of material effort or cost that is not provided for in the Contract, then either Nasstar or the Customer may raise this in accordance with the change control procedure set out in the Contract or, in the absence of any such change control procedure, by discussing the same in good faith. For the avoidance of doubt, Nasstar shall not be required to provide any assistance under this paragraph 4.10 which would result in any change or expenditure referred to in paragraph (i) to (iii) of this paragraph 4.10, except if and to the extent that a suitable change is agreed to the Contract.

4.11 Data protection impact assessments

If the Processor believes or becomes aware that its processing of personal data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform the other party and provide the other party with assistance to conduct a data protection impact assessment in accordance with paragraph 4.10.

4.12 Data Security Incidents

a) Upon becoming aware of a Data Security Incident, the Processor shall inform the other party without undue delay and shall provide such timely information and assistance in accordance with paragraph 4.10 as the other party may require in order for the other party to fulfil its data breach reporting obligations under Data Protection Laws and to mitigate the effects of the Data Security Incident.

b) Where Nasstar is acting as the Processor, the Customer understands and accepts that the performance by Nasstar of certain Services may carry a risk to the Customer of loss or corruption of data. Nasstar's obligations in respect of data backup or retention shall be set out in the applicable Contract. The Customer understands and accepts that, save as stated otherwise in a Contract, the Customer shall bear full responsibility for the loss or corruption of data that may result from a Data Security Incident.

4.13 Subject access requests

The Processor shall promptly notify the other party if it receives a request from a data subject to exercise their rights in respect of their personal data and shall provide such assistance to the other party as may be required in accordance with paragraph 4.10

4.14 Deletion or return of personal data

Upon termination or expiry of the Contract, the Processor shall (at the other party's election) destroy or return to the other party all personal data (including all copies of the personal data) in its possession or control (including any personal data that is processed by an Authorised Sub-Processor). This requirement shall not apply to the extent that the Processor is required by any Law to retain some or all of the personal data, in which event the Processor shall isolate and protect the personal data from any further processing except to the extent required by such Law. The Processor shall be entitled to render such charges or recover such costs associated with destroying or returning personal data to the controller or joint controller (as appropriate) as provided in the Contract or, if no such charges or costs are provided in the Contract, the Processor's reasonable costs.

4.15 Information and audit

The Processor shall make available to the other party all information necessary to demonstrate compliance with the obligations set out in this paragraph 4 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, except if and to the extent that providing such information or permitting such an audit would place the Processor in breach of Law or cause it to infringe the rights (including rights in intellectual property or confidential information) of any of the Processor's other customers. No more than one audit may be carried out in any calendar year, except if and when required by instruction of a competent data protection authority. The Processor shall be entitled to recover its costs of complying with this paragraph 4.15. Where the Processor has appointed a third party auditor to assess any of its technical or organisational measures to protect against Data Security Incidents for the purposes of any industry certification or otherwise (such as ISO27001 compliance), the Processor may share a copy of the auditor's certificate, in lieu of providing other information or allowing for other audits by the controller or another auditor under this paragraph 4.15.

5 Authorised disclosures

5.1 Notwithstanding any other provision of these Data Processing Terms but subject to applicable Data Protection Law, the Customer agrees that Nasstar may be required to disclose certain personal data:

a) to Government agencies or law enforcement authorities in accordance with Law;

b) to third party providers or licensors who are required to disclose certain personal data to Government agencies or law enforcement authorities in accordance with Law;

c) to third party providers for the proper operation of the Services (including to third party providers of products and/or services used in the provision of the Services or in connection with the provision of trouble shooting or other support services in connection therewith); and/or

d) to third party licensors whose software is licensed to the Customer in connection with the provision of the Services and who require such personal data for licence audit purposes, in each case where relevant to the Services provided by Nasstar to the Customer.

Nasstar will comply with the terms of any transfer mechanisms implemented in accordance with paragraphs 4.5 and 4.6.

5.2 This paragraph 5 shall be without prejudice to any obligations of the Customer under any of the other provisions of the Contract or Law to provide information to Nasstar concerning its use of the Services.

6 Notices

Any notices to Nasstar under these Data Processing Terms should be sent by email to dpo@nasstar.com or in writing via letter to Nasstar Data Protection Officer, 19-25 Nuffield Road, Poole, Dorset, England, BH17 0RU. All notices under paragraphs 4.12 (Data Security Incidents) and 4.13 (Subject Access Requests) should be notified via email to dpo@nasstar.com marked as high importance.

7 Priority

7.1 These Data Processing Terms shall take priority over any other terms of the Contract to the extent of any conflict or inconsistency between any provision of these Data Protection Terms and any other provision of the Contract.

7.2 Notwithstanding paragraph 7.1, these Data Processing Terms shall remain subject to any limitations and exclusions of liability set out in the Contract.

8 Definitions

8.1 In these Data Processing Terms, unless the context otherwise requires, these terms will be given the following meanings:

"Adequate Territory": a territory outside of the European Economic Area or the United Kingdom (as appropriate) that has been designated by the European Commission or the competent United Kingdom authority (as appropriate) as ensuring an adequate level of protection pursuant to Data Protection Laws without the need for further safeguards;

"Authorised Sub-Processor" has the meaning given in paragraph 4.9;

"**Communications Data**": any data processed for the purpose of the conveyance or billing of any electronic communication or communication on an electronic communications network, including SMS, MMS, email and internet connection records, and any Location Data. Communications Data may include records of connections to particular telephone numbers, devices and users and the dates, times and durations of such connections;

"**Content Data**": the content (comprising any speech, music, sounds, visual images or data of any description) of any electronic communication by a User, including the content of electronic messages, such as SMS, MMS and email, and web pages requested to the extent that it is not Communications Data;

"Contracted Third party" has the meaning given in paragraph 4.9;

"**CRM Data**": any personal data of staff or representatives of a party which is processed by the other party for the purposes of managing the Services, administering a Contract or marketing products or services to that party;

"**Data Protection Law**": all applicable Laws relating to data protection, the processing of personal data and privacy which may include: (a) the GDPR as incorporated into UK law pursuant to s.3 of the European Union (Withdrawal Act) 2018 (as amended) ("**UK GDPR**"); (b) any applicable national laws and regulations that implement, supplement or amend the GDPR or UK GDPR, including the Data Protection Act 2018 in the United Kingdom; (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (and any similar or equivalent applicable national laws and regulations); and (d) any other Law relating to data protection, the processing of personal data and privacy;

"Data Security Incident": the accidental or unlawful destruction, loss, alternation, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"**European Economic Area**"; the Member States of the European Economic Area as it is made up from time to time, comprising the Member States of European Union and such other countries that are party to the Agreement on the European Economic Area that entered into force on 1 January 1994;

"**GDPR**": 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, and repealing Directive 95/46/EC (General Data Protection Regulation);

"**Location Data**": any data processed in an electronic communications network indicating the geographic position of the terminal equipment of a User, geographic location derived from geographic identifiers associated with the access network or any other identifiers with known or presumed coordinates for the network elements to which a User is connected;

"Nasstar Data Processing Schedule": Nasstar's record (as updated by Nasstar from time to time) describing the categories of personal data that it processes in connection with each of the Services that it offers to its customers and Nasstar's responsibility as a controller or processor with respect to the processing. The Nasstar Data Processing Schedule is available at:

- http://www.nasstar.com/DPA-processing-responsibilities; or
- https://www.nasstar.com/sites/default/files/2022-02/Data_Processing_Schedule_Communications_Services_Feb_2022.pdf in respect of those Services where the applicable Service Description states that the Nasstar Data Processing Schedule (Communications Services) applies;

"Permitted Purpose": has the meaning given in paragraph 4.2;

"Standard Contractual Clauses": means: (i) where the GDPR applies, the standard contractual clauses for the transfer of personal data to controllers or processors (as appropriate) established in third countries approved by the European Commission from time to time (available online at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm), as such standard contractual clauses may be amended or replaced by the European Commission from time to time ("**EU SCCs**") and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" or the "International Data Transfer Agreement" issued (in each case) by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 as such may be amended or replaced by the Information Commissioner's Office from time to time ("**UK Addendum**");

"TCA": the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland of the other part;

"User Data": personal data regarding Users which is not Communications Data, Content Data or CRM Data. Such personal data include user IDs, passwords, authenticators, addresses (including MAC addresses, IP addresses and email addresses) and telephone numbers; and

"**personal data**", "**controller**", "**joint controller**", "**processor**", "**data subject**", "**process**" or "**processing**", "**subject access request**", and any other terms that are defined under Data Protection Laws and used in a Contract shall be given their meanings under Data Protection Laws.

8.2 All other terms shall be interpreted in accordance with the Contract.