Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Dstny customers
-
- -
DK
Company registration number:
hereinafter "The Controller"

and

Dstny A/S (og koncernforbundne selskaber)
Skodsborgvej 305 D
2850 Nærum
DK
Company registration number: 28313160
hereinafter "The Processor"

each a "Party"; together the "Parties"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

This is version 5, last updated 21.05.2024 15:56.

1. **Content**

2. Preamble

2.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the Controller and the Processor, when processing personal data on behalf of the Controller.

2.2 The parties are aware that the Controller is themself processing some or all of the personal data governed by the Clauses on behalf of another ultimate controller. In regard to this ultimate controller the Controller and Processor, thus function as processor and sub-processor respectively. The parties do not consider this fact to affect their obligations interpartes.

2.3 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (GDPR).

2.4 In the context of the provision of mobile telephony, IP telephony, communication services and software (PBX, collaboration etc.), network infrastructure, security and related services, the Processor will process personal data on behalf of the Controller in accordance with the Clauses.

2.5 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.6 Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.7 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.8 Appendix B contains the Controller's conditions for the Processor's use of sub-processors and a list of sub-processors authorised by the Controller.

2.9 Appendix C contains the Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Processor and how audits of the Processor and any sub-processors are to be performed.

2.10 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.11 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.12 The Clauses shall not exempt the Processor from obligations to which the Processor is subject pursuant to the General Data Protection Regulation (GDPR) or other legislation.

2.13 Insofar as the Controller is in fact processing the relevant personal data on behalf of another ultimate data controller, this agreement shall function as a sub-processor agreement, in which case, Controller and Processor, shall be taken to mean processor

and sub-processor respectively.

3. The rights and obligations of the Controller

3.1 The Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

3.2 The Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3 The Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Processor is instructed to perform, has a legal basis.

4. The Processor acts according to instructions

4.1 The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2 The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1 The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2 The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1 GDPR, Article 32, stipulates that, taking into account 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, the Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

6.1.1 Pseudonymisation and encryption of personal data;

6.1.2 the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

6.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 According to GDPR, Article 32, the Processor shall also – independently from the Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Controller shall provide the Processor with all information necessary to identify and evaluate such risks.

6.3 Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to GDPR, Article 32, by inter alia providing the Controller with information concerning the technical and organisational measures already implemented by the Processor pursuant to GDPR, Article 32, along with all other information necessary for the Controller to comply with the Controller's obligation under GDPR, Article 32.

If subsequently – in the assessment of the Controller – mitigation of the identified risks require further measures to be implemented by the Processor, than those already implemented by the Processor pursuant to GDPR, Article 32, the Controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1 The Processor shall meet the requirements specified in GDPR, Article 28(2) and (4) in order to engage another processor (a sub-processor).

7.2 The Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the Controller.

7.3 The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall inform in writing the Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in

advance, thereby giving the Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the Controller can be found in Appendix B.

7.4 Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and GDPR.

The processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Processor is subject pursuant to the Clauses and GDPR.

7.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the Controller's request – be submitted to the Controller, thereby giving the Controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Controller.

7.6 If the sub-processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in GDPR, Articles 79 and 82 – against the Controller and the Processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1 Any transfer of personal data to third countries or international organisations by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.

8.2 In case transfers to third countries or international organisations, which the Processor has not been instructed to perform by the Controller, is required under EU or Member State law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3 Without documented instructions from the Controller, the Processor therefore cannot within the framework of the Clauses:

8.3.1 transfer personal data to a controller or a processor in a third country or in an international organization

8.3.2 transfer the processing of personal data to a sub-processor in a third country

8.3.3 have the personal data processed by the Processor in a third country

8.4 The Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

9. Assistance to The Controller

9.1 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the Processor shall, insofar as this is possible, assist the Data Controller in the Controller's compliance with:

9.1.1 the right to be informed when collecting personal data from the data subject

9.1.2 the right to be informed when personal data have not been obtained from the data subject

9.1.3 the right of access by the data subject

9.1.4 the right to rectification

9.1.5 the right to erasure ('the right to be forgotten')

9.1.6 the right to restriction of processing

9.1.7 notification obligation regarding rectification or erasure of personal data or restriction of processing

9.1.8 the right to data portability

9.1.9 the right to object

9.1.10 the right not to be subject to a decision based solely on automated processing, including profiling

9.2 In addition to the Processor's obligation to assist the Controller pursuant to Clause 6.3, the Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:

9.2.1 The Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent data protection agency, unless the personal data breach is

unlikely to result in a risk to the rights and freedoms of natural persons;

9.2.2 The Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

9.2.3 The Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

9.2.4 The Controller's obligation to consult the competent data protection agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by The Controller to mitigate the risk.

9.3 The Parties shall define in Appendix C the appropriate technical and organisational measures by which The Processor is required to assist the controller as well as the scope and the extent of the assistance required. This applies to the obligations forseen in Clause 9.1 and 9.2.

10. Notification of personal data breach

10.1 In case of any personal data breach, the Processor shall, without undue delay after having become aware of it, notify the Controller of the personal data breach.

10.2 The Processor's notification to the Controller shall, if possible, take place within immediately and no later than 24 hours after the processor has become aware of the breach of the personal data security after the Processor has become aware of the personal data breach to enable the Controller to comply with the Controller's obligation to notify the personal data breach to the data protection agency, cf. GDPR, Article 33.

10.3 In accordance with Clause 9.2.1, the Processor shall assist The Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to GDPR, Article 33(3), shall be stated in the Controller's notification to the competent data protection authority:

10.3.1 The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

10.3.2 the likely consequences of the personal data breach;

10.3.3 the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4 The parties shall define in Appendix C all the elements to be provided by the Processor when assisting the Controller in the notification of a personal data breach to the competent data protection agency.

11. Erasure and return of data

11.1 On termination of the provision of personal data processing services, the Processor shall be under obligation to delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so unless Union or Member State law requires storage of the personal data.

11.2 The following EU or Member State law applicable to the Processor requires storage of the personal data after the termination of the provision of personal data processing services:

11.2.1 Due to the Danish Bookkeeping act (Bogføringsloven) section 10, we are required to store documentation for a period of 5 years.

The Processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12. Audit and inspection

12.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in GDPR, Article 28, and the Clauses and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

12.2 Procedures applicable to the Controller's audits, including inspections, of the Processor and sub-processors are specified in C.7 .

12.3 The Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

13.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

14.1 The Clauses are binding upon the Parties.

14.2 Both Parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the Parties.

14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Controller pursuant to Clause 11.1 and Appendix C.4, the Clauses may be terminated by written notice by either Party.

14.5 The Data Processor is bound by the Data Processor Agreement without the Parties' signatures. The Data Processor Agreement is thus concluded without physical / digital signatures, as the Data Processor Agreement is binding in accordance with the requirement of GDPR, article 28(3), first sentence.

15. The controller and the processor contacts/contact points

15.1 The Parties may contact each other using the following contacts/contact points

15.2 The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Contact information for The Controller:
The to any applicable contact information, which was received at the conclusion of the contract and through ongoing cooperation.

Contact information for The Processor:
Carsten Thomsen
dpo@dstny.dk

Appendix A Information about the processing

1. **The purpose of the Processor's processing of personal data on behalf of the Controller is:**

1.1 The following purposes form the basis of the Processor's processing of personal data on behalf of the Controller:

a) The processor provides cloud storage, hosting, storage, and backup to the controller.

Provision of one or more of the following services
- Mobile telephony
- IP telephony
- Internet access
- MPLS
- PBX functionality
- Integration between internal systems and our communication platform
- Firewall and Security
- Call center solutions
- Voice recording
- Meeting functionality online / by telephone
- Related services to the above services

2. **The Processor's processing of personal data on behalf of the Controller shall mainly pertain to (the nature of the processing):**

2.1 The data processor uses data from the data controller in order to deliver the requested services. For example, to make it possible to search for a colleague in the telephone system (PBX), to be able to see if the colleague is availeble, or to enable a desired integration.

The data processor save the required information to enable billing of the requested services, for example a CDR (Call Data Record) is saved for each call made, to ensure that the billing is done correctly.

If the customer have Danish telephone numbers, Dstny must, according to the Telecommunications Act (Bekendtgørelse af lov
om elektroniske kommunikationsnet og -tjenester) section 31, provide number information to public directory services.

2.2 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

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

3.1 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 personal data which are recorded in connection with the delivery of the service and cannot be precisely defined, various personal data on customers' systems to which access is granted, various personal data provided or recorded by the customer or the customer's customers without the organization's active processing and identification thereof

Billing formats for calls, SMS and data (CDR files)

3.2 The Processor may process personal data about the Controller's employees in connection with the Processor's sales, marketing and product development. This processing of personal data is not covered by the Clauses, because the Processor acts as a controller regarding of this processing. Instead, reference is made to the Processor's privacy policy which can be found on the Processor's website or upon request.

4. Processing includes the following categories of data subject

4.1 current employees, former employees, customers' employees (when customers are companies)

5. The Processor’s processing of personal data on behalf of the Controller may be performed when the Clauses commence. The processing has the following duration:

5.1 The processing of personal data shall be performed until the Processor's services has been terminated, after which the personal data is either returned or erased in accordance with Clause 11. The Processor's processing of personal data is performed as long as the underlying commercial agreement(s) consists.

Appendix B Authorised Sub-processors

1. Approved sub-processors

1.1 On commencement of the Clauses, the Controller authorises the engagement of the following sub-processors:

General sub-processors:

SuperOffice Danmark A/S (CVR-nr.:20020695)
Delta Park 46, st.
2665 Vallensbæk Strand
Denmark
Data processing: Super Office processes data for Dstny using their Customer Relationship Management solution

Microsoft Corporation (CVR-nr: 13612870)
One Microsoft Way
Redmond, WA 98052-6399
USA
Data processing: Microsoft processes data for Dstny using their document management software and Microsoft Teams

Zendesk's United States Representative:
Zendesk, Inc.
Attn: Hasani Caraway, General Counsel & Chief Privacy Officer
1019 Market Street
San Francisco, CA 94103, United States
Data processing: Zendesk processes data for Dstny using their ticketing system to handle customer service and support inquiries

Product-specific sub-processors:

Destiny for Service Providers AB (CVR-nr.: 556890-1747)
Lumaparksvägen 9
120 31 Stockholm
Sverige
Databehandling: Destiny for Service Providers AB processes data for Dstny using their communication platform Connect 3.0.

OCH A/S c/o Telia Company Danmark A/S (CVRnr.: 18936909)
Holmbladsgade 139
2300 København S
Denmark
Data processing: OCH A/S runs the common number database in Denmark, and is the common reference point for exchanging information about ported telephone numbers in Denmark. Dstny uses OCH when importing and exporting telephone numbers in Denmark.

NPS.TODAY ApS (CVRnr.: 36464917)
Bredgade 41, 2. tv.

1260 København K
Denmark
Data processing: NPS.TODAY processes data for Dstny using the product Net Promoter Score - SMS Survey.

InMobile ApS (CVRnr.: 31426472)
Axel Kiers Vej 18L
8270 Højbjerg
Danmark
Databehandling: InMobile processes data for Dstny using the 3CX telephony solution.

1.2 The Processor has the Controller's general authorisation for the engagement of sub-processor(s) from the above list. The Processor shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the data exporter to exercise its right to object.

Appendix C Instruction pertaining to the use of personal data

1. The subject of/instruction for the processing

1.1 Delivers Telephony, network and PBX functionality to the Data responsible.

2. Security of processing

2.1 The level of security shall take into account:

Taking 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 leve of security.

The Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Controller:

Security
The Processor shall implement the following security measures:

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 9.1 and 9.2 by implementing the following technical and organisational measures:

3.1.1 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.

3.1.2 If the Controller needs the Processor's assistance in order to reply to a request from a data subject, the Controller must send a written requst for assistance to the Processor and the Processor shall in response provide the necessary help or documentation as soon as possible and no later than 7 calendar days after receiving the request.

3.1.3 If the Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Controller, and the request concerns personal data processed on behalf of the Controller, the

Processor shall without undue delay forward the reuest to The Controller.

4. Storage period/erasure procedures

4.1 Upon termination of the provision of personal data processing services, the Processor shall either delete or return the personal data in accordance with Clause 11.1 unless the Controller – after the signature of the contract – has modified the Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

5. Processing location

5.1 Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Controller's prior written authorisation:

At the Processor's own headquarter or at the headquarters of approved sub-processors as specified in Appendix B.

6. Instruction on the transfer of personal data to third countries

6.1 Personal data is only being processed by the Processor on the locations specified in clause C.5. Transfers to the United States occur on the basis of the data importer's certification under the EU-U.S. Data Privacy Framework (see certified organizations here.) The Data Processor transfers personal data to the following countries not subject to an adequacy decision on the basis of Article 45 of Regulation (EU) 2016/679t in order to fulfill the Main Agreement: USA.

6.2 If the Controller does not provide a documented instruction in these Clauses or subsequently with regards to the transfer of personal data to a third country, the Processor is not entitled to carry out such transfers within the scope of these Clauses.

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

6.4 Where, in accordance with these clauses, The Processor transfers personal data to sub-data processors in third countries outside the EU / EEA, the Processor must independently secure a legal basis for the transfer in accordance with Chapter 5 of GDPR.

7. Procedures for the Controller's audits, including inspections, of the processing of personal data being performed by the Processor

7.1 The Processor shall, upon the Controller's written request, document to the Controller that the Processor

7.1.1 is complying with his obligations under these Clauses and the Instruction, and

7.1.2 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 a year and shall follow the principles and control objectives of the ISAE 3000 auditing standard, as laid down by Common Strategic Framework (CSF) - Danish Auditors and the Danish Data Protection Agency (and/or alternatively internationally recognized standards such as ISO/IEC 27701:2019). Self-audit reports may be conducted as part of the controller's information gathering and must be signed by the processor's management. In order to cover the The Data Controller's need for insight and assurance of the Data Processor's secure processing of the personal data, The Data Processor must audit The Data Processor's compliance with the the Clauses every 18 months, including the specified implemented security measures, by an external independent third party and send the complete records to the Data Controller.

7.4 Regardless of Clause C.7.3, The Processor shall furthermore provide for and contribute to audits and inspections every 12 months, performed by auditors appointed by the Controller, the public authorities in the competent jurisdiction, to the extent necessary to verify the Processor's compliance with these Clauses and the applicable data protection law. The auditor in question must be subject to confidentiality under law or agreement. The Controller must notify the audits in writing with 30 calendar days.

Appendix D The Parties' terms of agreement on other subjects

1. Note on the procedure for the Data Controller's audits in Annex C point 7

1.1 According to our documentation for compliance with the Data Processor agreement, reference is made to the procedure in Annex C point 7.3, as it will not be possible in practice to carry out a physical inspection of our data centres.

2. Update of the Data Processing Agreement

2.1 It is always the latest version of the data processing agreement that applies between the parties, see https://dstny.dk/databehandleraftale.

The data processor reserves the right to continuously make changes to, including clarifications of, the agreement.
These changes will typically be a result of new recommendations from e.g. The Danish Data Protection Authority or the EU Commission as well as changes in practice and legislation in the area.

The Data Controller is therefore encouraged, to sign up to receive notifications, when there are changes to the agreement:
https://dstny.dk/databehandleraftale

After receiving a notification about a change, the Data Controller has 14 working days to object, if the change cannot reasonably be accepted.

This provision does not apply to changes in the use of sub-processors, which are regulated in section 7 of the agreement.