



Let's go further

## Standard Contractual Clauses

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

between

*Electronic signed*

(the data controller)

and

EG A/S  
Industrivej Syd 13 C  
7400 Herning  
CVR-nr. 34 08 06 31

(the data 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.



Let's go further

## 1. Table of Contents

2. Preamble .....	3
3. The rights and obligations of the data controller.....	4
4. The data processor acts according to instructions .....	4
5. Confidentiality .....	4
6. Security of processing .....	4
7. Use of sub-processors.....	5
8. Transfer of data to third countries or international organisations .....	6
9. Assistance to the data controller .....	7
10. Notification of personal data breach .....	8
11. Erasure and return of data.....	9
12. Audit and inspection .....	9
13. The parties' agreement on other terms .....	9
14. Commencement and termination .....	10
15. Data controller and data processor contacts/contact points.....	10
Appendix A Information about the processing .....	12
Appendix B Authorised sub-processors.....	14
Appendix C Instruction pertaining to the use of personal data .....	16
Appendix D The parties' terms of agreement on other subjects .....	22



Let's go further

## 2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
2. 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 (General Data Protection Regulation).
3. In the context of the provision of Xena, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
5. Four appendices are attached to the Clauses and form an integral part of the Clauses.
6. 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.
7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.
8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
9. Appendix D contains provisions for other activities which are not covered by the Clauses.
10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.



Let's go further

### 3. The rights and obligations of the data controller

1. The data 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<sup>1</sup> data protection provisions and the Clauses.
2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

### 4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data 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 data 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.
2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

### 5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data 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.
2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

### 6. Security of processing

---

<sup>1</sup> References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".



Let's go further

1. Article 32 GDPR 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 data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data 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:

- a. Pseudonymisation and encryption of personal data;
  - b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. According to Article 32 GDPR, the data processor shall also – independently from the data 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 data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
  3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

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

## 7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.



Let's go further

The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data 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 data controller can be found in Appendix B.

3. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data 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 the GDPR.

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

4. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data 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 data controller.
5. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.
6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data 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 Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

## **8. Transfer of data to third countries or international organisations**

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



Let's go further

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
  - a. transfer personal data to a data controller or a data processor in a third country or in an international organization
  - b. transfer the processing of personal data to a sub-processor in a third country
  - c. have the personal data processed in by the data processor in a third country
4. The data 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.
5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

## 9. Assistance to the data controller

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

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

- a. the right to be informed when collecting personal data from the data subject
- b. the right to be informed when personal data have not been obtained from the data subject
- c. the right of access by the data subject
- d. the right to rectification
- e. the right to erasure ('the right to be forgotten')
- f. the right to restriction of processing
- g. notification obligation regarding rectification or erasure of personal data or restriction of processing
- h. the right to data portability
- i. the right to object



Let's go further

- j. the right not to be subject to a decision based solely on automated processing, including profiling
2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:
  - a. The data 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 supervisory authority, The Danish Data protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
  - b. the data 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;
  - c. the data 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);
  - d. the data controller's obligation to consult the competent supervisory authority, The Danish 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 data controller to mitigate the risk.
3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

## 10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below





Let's go further

which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

- a. 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;
  - b. the likely consequences of the personal data breach;
  - c. 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.
4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

## **11. Erasure and return of data**

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

## **12. Audit and inspection**

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.
3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

## **13. The parties' agreement on other terms**

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.



Let's go further

#### 14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.
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.
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.
4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.
5. Signature

On behalf of the data controller

Name  
Position  
Phone number  
E-mail address

*Electronic signed*

Date

Signature

On behalf of the data processor

Navn Aleksander Bjaaland

Stilling CEO

25-01-2021 | 08:49 CET

Date Underskrift

DocuSigned by:

CBF1B62108084E0...

#### 15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:
2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.



Let's go further

Contact points at EG

Name	Data Protection Office
Position	
Telephone	+45 7013 2211
E-mail	agreement@eg.dk

Contact point on behalf of the data controller in case of security breach

Name  
Position  
Telephone  
E-mail



Let's go further

## Appendix A Information about the processing

The Clauses are entered into as part of or with reference to the Parties' agreement concerning the supply of one or more IT services by the data processor to the data controller (the Main Agreement).

### A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The Clauses are entered into as part of or with reference to the Parties' agreement concerning the supply of one or more IT services by the data processor to the data controller (the Main Agreement).

### A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Delivery of IT service (s) may include the processing of ordinary, sensitive, and confidential personal data.

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

Ordinary and sensitive personal information

#### Ordinary personal information (cf. General Data Protection Regulation Art. 6)

- Name
- Address
- E-mail
- Phone number
- Citizenship
- Date of birth
- Gender
- Marital status
- Job title
- Job ID
- Bank account information
- Pictures
- IP and Cookie information
- Other common personal information

#### Sensitive personal information (cf. General Data Protection Regulation Art. 9):

- Race or ethnic origin



Let's go further

- Political beliefs
- Religious beliefs
- Philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data
- Health-related data, including abuse of medicine, narcotics, alcohol etc.
- The sexual relation or sexual orientation of a physical person

**Personal data relating to criminal convictions and offenses (cf. General Data Protection Regulation Art. 10):**

- Criminal convictions
- Criminal offenses

**Information regarding national identification number (cf. Databeskyttelseslovens § 11)**

- CPR Number (Danish Civil Registration Number)

**A.4. Processing includes the following categories of data subject:**

- Employees
- Users, Patients, Citizens, Customers, Clients or similar
- Children (0 – 12 years)
- Youth (13 – 18 years)
- Relatives
- Collaborators
- Other

**A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:**

The data processor's processing of personal data is terminated as part of the termination of the Main Agreement between the parties.



Let's go further

## Appendix B Authorised sub-processors

### B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR OR DUNS	ADDRESS	DESCRIPTION OF DATA PROCESSING	TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES
Global Connect	26759722	Hørskættø 3, 2630 Taastrup	Hosting	NO
Team.blue.Denmark A/S	29412006	Højvængen 4, 8660 Skanderborg, Danmark	Hosting	NO
Ping IT	34471967	Vandmanden 24, 9200 Aalborg SV, Danmark	Safe destruction of hardware	NO
EG A/S	84667811	Industrivej Syd 13 Cm 7400 Herning, Danmark	HR, IT, Service, Infrastructure	NO
B4restore	27719945	Åhave Parkvej 31, 8260 Viby J, Danmark	Backup og assistance in connection with EG's restore task	NO
ABBY.com	73258605	Landsberger Str. 300, Munich 80687, Tyskland	OCR Scanning of appendix and documents	YES
Link Mobility	30077520	Ørestads Boulevard 108, 4. 2300 København S Danmark	SMS Gateway	NO
Zendesk Inc	961919805	1019 Markets street, San Francisco, CA 94103 USA	Supportsystem for support	YES
SendGrid, Inc (Twilio Inc.)	5384944	375 Beale Street, Suite 300, San Francisco CA 94105	Communicationsplatform (CPaaS) to make and receiving calls, sending and receiving text messages	YES



Let's go further

		USA		
Sinch	26361710	Fruebjergvej 3, 2100 København Ø Danmark	Platform for distribution of text messages	NO
LiveChat, Inc.	79581998	101 Arch Street, 8th Floor, Boston MA 02110, USA	Chatfunktion	Yes

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

## B.2. Prior notice for the authorisation of sub-processors

The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).



Let's go further

## **Appendix C Instruction pertaining to the use of personal data**

### **C.1. The subject of/instruction for the processing**

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The following processing activities are covered by the Clauses: Implementation, operation, support, testing, maintenance of Xena (as described in separate agreements between the Parties), which may involve access to personal information.

The Data Processor must ensure that the IT solution can integrate with the Data Controller's other suppliers, partners, data processors or IT systems, after which the Data Controller's personal information can be transferred via API or similar to a third party. The Data Processor is therefore instructed to open with the third parties selected by the Data Controller at any time.

#### **Especially regarding AABYY**

In connection with the delivery of the service to the Data Controller, the Data Processor uses AABYY as a sub-data processor. AABYY uses Microsoft as a sub-sub-processor. The Data Controller is aware that the use of this sub-sub-processor may involve the transfer of personal data to third countries. Upon entering into this Data Processor Agreement, the Data Controller has given approval for the use of this sub-data processor and sub-sub-data processor as well as instructions on the transfer of personal data to third countries in this context.

#### **Especially regarding Zendesk**

In connection with the delivery of the service to the Data Controller, the Data Processor uses Zendesk as a sub-data processor located in several countries. Information can be transferred to third countries when Zendesk maintains, for example, implements patches or security updates in the Zendesk platform, as well as in connection with storage.

Zendesk uses Amazon Web Services, Inc and Google, Inc. as sub-sub-data processors. The Data Controller is aware that the use of this sub-sub-processor may also involve the transfer of personal data to third countries.

#### **Especially regarding Twilio**

In connection with the delivery of the service to the Data Controller, the Data Processor Twilio uses sub-data processors located in several countries.

Information can be transferred to third countries when using Twilio's SendGrid Service and in connection with storage. Twilio uses Zayo and Centurylink as sub-sub-data processors. The Data Controller is aware that when using these sub-data processors for storage, personal data may also be transferred to third countries.

#### **Especially regarding LiveChat**





Let's go further

In connection with the delivery of the service to the Data Controller, the Data Processor uses LiveChat as a sub-processor located in the USA. Information may be transferred to third countries in connection with the user using the chatbot function on the website.

### **C.2. Security of processing**

The level of security shall take into account:

The data processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with the processing activities that the data processor performs for the data controller.

The technical and organizational measures are determined taking into account the current technical level, the implementation costs, the nature, scope, coherence and purpose of the processing in question, as well as the risks of varying probability and seriousness for the rights and freedoms of natural persons.

In assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

The data processor is then entitled and obliged to make decisions about which technical and organizational security measures must be implemented in order to establish the necessary (and agreed) level of security.

### **C.3. Assistance to the data controller**

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

At the specific request of the data controller, the data processor, taking into account the nature of the processing, assists the data controller as far as possible by appropriate technical and organizational measures in compliance with the data controller's obligation to respond to requests for data subjects' rights.

If a data subject submits a request for the exercise of his rights to the data processor, the data processor shall notify the data controller without undue delay.

Taking into account the nature of the processing and the information available to the data processor, the data processor, upon specific request, assists the data controller in ensuring compliance with the data controller's obligations in relation to:

- Implementation of appropriate technical and organizational measures
- Security breach



Let's go further

- Notification of breach of personal data security to the data subject
- Conducting impact assessments
- Prior consultations with the supervisory

#### C.4. Storage period/erasure procedures

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

#### C.5. Processing location

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

The processing of personal data takes place at the data processor's addresses as well as the listed data processors and the addresses of their sub-processors.

Storage must take place in Microsoft data centers located within the EU. In order to fulfill delivery obligations under an agreement on settlement solution, the data processor may carry out processing from its own location when this is necessary for carrying out tasks under an agreement on settlement solution.

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

##### ABBYY

Sub-processor	
Name of company	ABBYY Europe GmbH
Address	Landsberger Str. 300, Munich, 80687
Country	Tyskland
Duns number	329563402
Does the Data Processor have a data processor agreement with the sub-data processor	Yes
Who is the sub-processor	ABBYY provides a retrieval tool for retrieving information in documents, including invoices. This is a cloud-based solution.
Data processing (s) in which sub-data processor participates	ABBYY processes the data uploaded in connection with the use of the search tool.
Categories of data that sub-processor will process	Contact Information Key information for the contract Customer history Billing and payment information
Storage of data at the sub-data processor	Data is stored on servers in Germany and Ireland.



Let's go further

Transfer to third country and instructions	In connection with the delivery of the service to the Data Controller, the Data Processor uses ABBYY as a sub-data processor. ABBYY uses Microsoft as a sub-sub-processor. The Data Controller is aware that the use of this sub-sub-processor may involve the transfer of personal data to third countries. Upon entering into this Data Processor Agreement, the Data Controller has given approval for the use of this sub-data processor and sub-sub-data processor as well as instructions on the transfer of personal data to third countries in this context.
Basis of transfer is used for third country transfers?	The EU Commission's Standard Contracts are not concluded directly between the Data Controller (the data exporter) and Microsoft (the data importer). As the use of the EU Commission's Standard Contracts presupposes that the Data Controller is a direct party to the agreement in the transfer basis, the sub-data processor, ABBYY, is authorized to enter into such an agreement on behalf of the Data Controller. This means that the Data Controller must be considered a data exporter in relation to the EU Commission's Standard Contracts, and that the Data Controller in connection with the transfers of information to Microsoft agrees to be bound by the obligations imposed on the data exporter by the EU Commission's Standard Contracts. The content of this Instruction and / or Data Processor Agreement is not considered to change the content of the EU Commission's Standard Contracts.

### Zendesk

Sub-processor	
Name of company	Zendesk, Inc
Address	1019 Market Street, San Francisco, CA 94103
Country	USA
Duns number	961919805
Does the Data Processor have a data processor agreement with the sub-data processor	Yes
Who is the sub-processor	Zendesk provides Software as a Service for handling support requests in a cloud-based solution. They provide a support case support system that handles all inquiries regarding support cases.
Data processing (s) in which sub-data processor participates	Zendesk processes the data uploaded in connection with a support case.



Let's go further

Categories of data that sub-processor will process	All categories of data uploaded by the support user in connection with a support case.
Storage of data at the sub-data processor	Data is stored on servers within the EEA or US
Transfer to third country and instructions	<p>In connection with the delivery of the service to the Data Controller, the Data Processor uses Zendesk as a sub-data processor located in several countries. Information can be transferred to third countries when Zendesk maintains, for example, implements patches or security updates in the Zendesk platform, as well as in connection with storage.</p> <p>Zendesk uses Amazon Web Services, Inc and Google, Inc. as sub-sub-data processors. The Data Controller is aware that the use of this sub-sub-processor may also involve the transfer of personal data to third countries.</p>
Transfer to third country and instructions	<p>Zendesk, Inc. - United States – Binding corporate rules</p> <p>Zendesk Pty. Ltd - Australia – Binding corporate rules</p> <p>Zendesk, Inc. - Philippines – Binding corporate rules</p> <p>Zendesk Singapore Pte. Ltd. - Singapore – Binding corporate rules</p> <p>Zendesk Brasil Software Corporativo LTDA - Brazil – Binding corporate rules</p> <p>Kabushiki Kaisha Zendesk - Japan – Binding corporate rules</p> <p>Smooch Technologies ULC Canada – Binding corporate rules</p>

**Twilio**

Sub-processor	
Name of company	Twilio (Sendgrid)
Address	375 Beale Street, Suite 300, San Francisco 04105
Country	USA
Duns number	53723673
Does the Data Processor have a data processor agreement with the sub-data processor	Yes
Who is the sub-processor	Twilio provides cloud-based software (SendGrid Services) which is a communication platform (CPaaS) for programmatically making and receiving calls, sending and receiving text messages via an email API.
Data processing (s) in which sub-data processor participates	Twilio behandler de data der er nødvendige for at kunne levere løsningen og derved data, hvor databehandler kan kontakte dataansvarlige eller registrerede (slutkunde).



Let's go further

Categories of data that sub-processor will process	Twilio processes the data necessary to be able to deliver the solution and thereby data, where the data processor can contact data controllers or registered (end customer).
Storage of data at the sub-data processor	Data is stored in the US at Zayo and Centurylink
Transfer to third country and instructions	In connection with the delivery of the service to the Data Controller, the Data Processor Twilio uses sub-data processors located in several countries. Information can be transferred to third countries when using Twilio's SendGrid Service and in connection with storage. Twilio uses Zayo and Centurylink as sub-sub-data processors. The Data Controller is aware that when using these sub-data processors for storage, personal data may also be transferred to third countries.
Transfer to third country and instructions	Twilio Australia Pty Ltd, - Binding corporate rules Twilio Canada Corp. - Binding corporate rules Twilio Colombia S.A.S - Binding corporate rules Twilio Hong Kong Limited - Binding corporate rules Twilio Inc., - Binding corporate rules Twilio Japan G.K. - Binding corporate rules Twilio Singapore Pte. - Binding corporate rules Teravoz Telecom Telecomunicacoes Ltda. - Binding corporate rules Twilio Technology India Private Limited - Binding corporate rules Twilio UK Limited - Binding corporate rules

### LiveChat

<b>Underdatabehandler</b>	
Virksomhedens navn	LiveChat, Inc
Adresse	101 Arch Street, 8th Floor, Boston MA 02110, USA
Land	USA
CVR-nummer eller Duns	79581998
Har Databehandleren en databehandleraftale med underdatabehandleren	Ja
Hvem er underdatabehandleren	LiveChat provides a chatbot which allows the user to submit chat messages in connection with delivery requests, support questions or the like.
Databehandling(er), som underdatabehandler deltager i	LiveChat processes the data entered into the chatbot.
Kategorier af data som underdatabehandler vil behandle	Name, e-mail and possibly other categories of data that are entered in the chatbot.



Let's go further

Opbevaring af data hos underdatabehandleren	Data is stored in USA.
Overførsel til tredjeland og instruks	In connection with the delivery of the service to the Data Controller, the Data Processor uses LiveChat as a sub-processor located in the USA. Information may be transferred to third countries in connection with the user using the chatbot function on the website.
Hvilket overførselsgrundlag avendes ved tredjelandsoverførslen?	LiveChat, Inc. - United States – Standard Contractual Clauses

#### **C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor**

The Data Processor shall annually obtain for its own account an audit report of type ISAE 3402 or of type ISAE 3000 or equivalent from an independent third party concerning the data processor's compliance with the GDPR, data protection provisions of other Union or national law and the Clauses.

The data processor shall make available to the data controller all information necessary to demonstrate compliance with the requirements of the Clauses. The data processor hereby provides the opportunity for and contributes to audits, including inspections carried out by the data controller or another auditor authorized by the data controller.

If an audit is performed by someone other than the data controller himself, this other auditor must be independent and non-competitive with the data processor and otherwise be subject to a duty of confidentiality and secrecy either as a result of law or as a result of a confidentiality agreement on which the data controller can support the direct auditor in question directly.

The data processor shall immediately notify the data controller if an instruction to make information available or allow for audits and inspections in the data processor's opinion is in breach of the GDPR or data protection provisions of other EU or national law.

## **Appendix D The parties' terms of agreement on other subjects**

### **D 1. Deviations from the agreement**

#### Section 7.5



Let's go further

The parties have agreed the following exception from the Clauses section 7.6, which is not applicable to the Clauses.

Section 7.5 has the following wording:

*The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.*

## **D 2. Cloudløsninger**

If the data processor processes the data controller's personal data in a hybrid solution, which means that the data controller's IT environment includes components located in the data processor's data centers and components located outside the data processor's data centers (hereinafter Cloud), the following is agreed:

If the data processor provides a solution to the data controller that includes a Cloud Part, the data processor's subcontractor on that Cloud Part may store and process the data controller's personally identifiable information in accordance with the subcontractor's applicable standard terms.

If the data processor's deliveries are part of a hybrid solution where the data controller has a contractual relationship directly with one or more providers of Cloud Services, and the data processor must process, but not store, the data controller's personal data in the Cloud Part, the data processor's processing takes place under this Agreement. responsible for the storage and processing of data by another Cloud Provider.

This clause takes precedence over Clause 7 of the Agreement above, which deals with the use of sub-processors

## **D. 3 Betalbar ydelse**

The data processor is entitled to a separate payment for services in accordance with points 9, 10 and for participating in audits in accordance with point 12 and point C7 of Annex C.

If the data processor's work with handling security breaches is due to a breach by the data processor, the data processor will not be entitled to payment for this work.



Let's go further

## Changelog

CHANGE	VERSION
1.1.	Clauses 9.2. and 10.4., ( <i>Corrected cross-references</i> ).
1.2 – January 2021	Added LiveChat as a sub-processor