encode

DATA PROCESSING AGREEMENT (DPA)
(Revised 23 March 2020)

As part of the Agreement, the following Data Processing Agreement ("DPA") applies between the Data Processor, Encode A/S and the Data Controller, the Customer, unless otherwise expressly specified in other agreements between the parties.

The purpose of the DPA is to regulate, how the Data Processor shall process personal data on behalf of the Data Controller and in order to meet the requirements of the GDPR including Article 28(3) and to ensure the protection of the rights of the data subject.

Two appendices are attached to this DPA and form an integral part of the DPA.

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

Appendix B contains a list of the Data Processor's use of sub-processors.

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

The DPA 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.

1. 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 data protection provisions and this DPA.

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 others, for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

2. 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. 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 this DPA.

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.

3. 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.

4. Security of processing

1. The Data Processor's security policy is defined on the basis of the ISO 27002 standard.

2. 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.

3. 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.

4. 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.

5. Use of sub-processors

1. 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 fourteen (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). The list of sub-processors already authorised by the Data Controller can be found in Appendix B

2. The Data Controller acknowledges and agrees that the Data Processor´s Affiliates may be retained as Sub-processors and that the Data Processor and its Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

3. If the Data Controller has reasonable grounds to object to the data processor's use of a new sub-processor then the Data Controller shall promptly, but in no case later than fourteen (14) days following the Data Processor's written notice, provide notice to the Data Processor in writing. Should the Data Processor choose to retain the objected-to sub-processor, the Data Processor will notify the Data Controller at least fourteen (14) days before authorising the sub-processor to process personal data and then the Data Controller may terminate the relevant portion(s) of the Agreement within thirty (30) days. Upon any termination by the Data Controller pursuant to this section, the Data Processor shall refund the Data Controller any prepaid fees for the terminated portion(s).

6. 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.

2. The Data Processors must not allow processing of Personal Data to take place outside the EU / EEA without the Data Controllers consent.

3. The Clauses of this DPA shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the DPA cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

7. 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
   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, 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, 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, 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.

8. 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. In accordance with Clause 7(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 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.

9. 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 is done unless Union or Member State law requires storage of the personal data.

10. 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 this DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

2. 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.

11. Liability

1. Each party shall indemnify and hold harmless the other party against all losses, liabilities fines and sanctions arising from any claim and proceedings and supervisory authority action arising from any breach by the Data processor of this DPA.

2. Each party's total aggregate liability of the Agreement, including events arising out of this DPA shall be limited to the greater of the total Fees paid or payable under this agreement during the 12 months immediately preceding the date on which the claim arose or DKK 10,000,000 (ten million Danish kroner).

Appendix A Information about the processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

The Data Processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by the Data Controller when using the Services.

Categories of data subjects and types of personal data subject to processing:

The Data Controller may submit Personal Data to the Services, the extent of which is determined and controlled by the Data Controller, and may include, but is not limited to Personal Data relating to the following categories of data subjects:

a) Prospects, customers, business partners and vendors of Customer (who are natural persons)
b) Employees or contact persons of Customer's prospects, customers, business partners and vendors
c) Employees, agents, advisors, freelancers of Customer (who are natural persons)
d) Customer's Users authorized by Customer to use the Services

In order to support the Services Data Processor will collect:

a) General personal information, including email, name, IP addresses.

The Data Controller may submit personal data to the Services, the extent of which is determined and controlled by the Data Controller, and may include, but is not limited to Personal Data relating to the following categories of personal data:

a) Title
b) Position
c) Additional contact information (company, phone, physical business address)
d) Biometric data (images or videos)

The Data Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Appendix B Authorised sub-processors

Approved sub-processors

On commencement of this DPA, the Data Controller authorises the engagement of the following sub-processors:

NAME	LOCATION	DESCRIPTION OF PROCESSING
Sentia	Denmark	Infrastructure as a Service
Google Cloud Platform	United Kingdom and Belgium	Infrastructure as a Service and Google Cloud Platform services
Amazon Web Services	Ireland	Infrastructure as a Service and AWS services
Zendesk, Inc.	European Economic Area (EEA) and the United States (US)	Zendesk Support Service

The Data Controller shall on the commencement of this DPA 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.

Encode group sub-processors

The following entities are members of the Encode Group. Accordingly, they function as sub-processors to provide the Services:

ENTITY NAME	SERVICE LOCATION (COUNTRY WHERE PROCESSING IS PERFORMED)	DESCRIPTION OF PROCESSING
Encode Marketing Software Limited	United Kingdom	Providing service support
Encode Marketing Software Spain S.L.	Spain	Providing service support