Enalyzer Data Processing Agreement

BETWEEN:

The **Customer** defined as the **"Controller"**

and

Enalyzer defined as the **"Processor"**

collectively referred to as **"Parties"** and individually referred to as **"Party".**

WHEREAS

I.   Processor offers various online software services including among others a survey and reporting tool to Controller via Processor's online platform (the "Software Services"), as well as consultancy, support and/or education services (the "Consultancy Services") which include processing of "Personal Data" (as defined under clause 1.4). All services provided by the Processor to the Controller, including the Software Services and the Consultancy Services, shall be deemed the Processor's Services. In that capacity, the Processor is a data processor in a legal sense.

II.   Controller intends to use Processor's Services. By usage of Processor's Services, Controller may share Personal Data of its Data Subjects with Processor and is in that capacity a data controller in a legal sense.

III.   Parties acknowledge and agree that Controller solely determines the means and purposes for the processing of Personal Data by Processor.

IV.   The purpose of the Data Processing Agreement is to ensure the Parties' compliance with Article 28(3) of the General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the GDPR") stipulating specific requirements to the content of a data processing agreement.

V.   In this Data Processing Agreement, the Parties wish to set out the subject matter and duration of the processing of Personal Data, the nature and purpose of the processing, the type of Personal Data and categories of data subjects and the obligations and rights of the Parties.

VI.   In the event of any discrepancies between this Data Processing Agreement and any other agreements between the Parties, including the Agreement (as defined in clause 1.2), concerning a matter in relation to the processing of Personal Data, the terms of this Data Processing Agreement shall prevail, except for specific changes to Appendices to this Data Processing Agreement made in a Software Service Order or a Consultancy Service Order.

THE CONTROLLER AND THE PROCESSOR HAVE AGREED

as follows in order to ensure adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals with regard to the processing of Personal Data as specified in Appendix 1:

1. **Definitions**

   1. In addition to the definitions used elsewhere in this Data Processing Agreement, the definitions set out below shall apply and have the meaning set out therein.

   2. **'Agreement'** shall mean the agreement entered into between the Controller and the Processor regarding the use of Processor's Services that incorporates Enalyzer's General Terms and Conditions and this Data Processing Agreement.

   3. **'Data Processing Agreement'** shall mean this data processing agreement including its appendices, which forms an integral part of the data processing agreement.

   4. **'Personal Data'** shall mean any information Processed by Processor in connection with the provision of the Processors' Services under this Data Processing Agreement relating to an identified or identifiable natural person (**'Data Subject'**); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity of that person.

   5. **'Processing'** shall mean any operation or set of operations by Processor in connection with the Data Processing Agreement, which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

   6. **'Sub-processor'** shall mean any processor engaged by the Processor for the Processing of Personal Data on behalf of the Controller.

   7. **'Third Country'** shall mean countries outside the EU.

   8. **'Third Party'** shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to Process the Personal Data based on the Agreement.

   9. **'Personal Data Breach'** shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

   10. **'Processor's Services'** shall mean (i) the various online software services (the "Software Services") rendered by Processor pursuant to the Agreement, including among others provision of a survey and reporting tool and hosting of Controller's data, including Personal Data and/or (ii) consultancy, support and/or education services (the

"Consultancy Services") provided by the Processor from time to time to the Controller pursuant to the Agreement.

11. **'EU'** shall mean the European Union including the European Economic Area (EEA).

2. **Scope and details of Processing and instruction to the Processor**

1. The details of the Processing of Personal Data, and in particular the categories of Data Subjects, types of Personal Data and the purposes for which they are Processed, are specified in **Appendix 1**.

2. The Controller hereby authorises the Processor to Process the Personal Data on behalf of the Controller on the terms and conditions set out in this Data Processing Agreement. The Processor shall Process the Personal Data only on documented instructions from the Controller, see **Appendix 2**.

3. The Parties agree that this Data Processing Agreement shall constitute the instructions as of the date of the Data Processing Agreement.

4. The Controller may at any time amend or specify the instructions in accordance with clause 11 of this Data Processing Agreement. Notwithstanding the foregoing, clause 11 can only be amended according to written mutual agreement between the Parties.

3. **Security measures**

1. The Processor agrees to implement appropriate technical and organisational measures in such a manner that the Processing of the Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subjects.

2. The details of the security measures taken by Processor in this respect of the Processing of Personal Data are specified in Appendix 2.

3. The Parties agree that the technical and organisational measures and level of security set out in Appendix 2 are sufficient to comply with the Processor's obligations set lout in this clause 3 at the time of the conclusion of this Data Processing Agreement.

4. If the Controller after the conclusion of this Data Processing Agreement based on its own security and risk assessment requests that the Processor shall implement additional security measures or other technical or organisational measures than agreed to in Appendix 2, such request shall be handled in accordance with and is subject to clause 11 of this Data Processing Agreement.

4. **Obligations of the Controller**

1. The Controller agrees to ensure that the Controller always collects and Processes Personal Data in accordance with and do not violate the relevant provisions of the GDPR and other applicable EU and national data protection law in the Member State in which, the Controller is established.

2. The Controller shall immediately notify the Processor in writing after becoming aware of any possible unauthorised use of log-in information, passwords, credentials or other security breaches in the Controller's systems, at the Controller's premises or otherwise under the Controller's responsibility that are or may be related to or have an impact on the Processor's Processing of Personal Data under this Data Processing Agreement.

5. **Obligations of the Processor**

The Processor agrees:

1. to Process the Personal Data in accordance with the security measures set out in Appendix 2 and any measures that may have been mutually agreed in accordance with clause 11 of this Data Processing Agreement;

2. to Process Personal Data only in accordance with the written instructions from the Controller, cf. clause 2 of this Data Processing Agreement, including with regard to transfers of Personal Data to a Third Country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

3. where necessary and taking into account the nature of the Processing, to assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation by law to respond to requests for exercising the Data Subjects' rights laid down in chapter III of the GDPR;

4. where necessary and taking into account the nature of the Processing, to assist the Controller in its compliance with an obligation to carry out a data protection impact assessment ("DPIA") and prior consulting of supervisory authorities where required, cf. articles 35 and 36 of the GDPR;

5. to provide Controller upon request and within reasonable time the information necessary to demonstrate compliance with the obligations laid down in this clause 5;

6. to cooperate (including representatives of Processor), on the Controller's request, with the supervisory authority in the performance of its tasks;

7. to allow for and contribute during normal business hours to reasonably necessary audits including inspections, conducted by an external qualified auditor mandated by the Controller, solely for the purpose of fulfilment of the Controller's obligations laid down in Article 28 of the GDPR and for accurately stipulated research questions in this connection provided that such external qualified auditor is subject to and bound by confidentiality obligations as stipulated in clause 12 of this Data Processing Agreement;

8. to make an annual audit report available on the Processor's website with information regarding the Processor's compliance with the Data Processing Agreement. The report shall be prepared at the Processor's expense based on applicable, acknowledged audit standards, e.g. ISAE 3000 or 3402 or similar;

9. to notify Controller in the event of a Personal Data Breach as set out in clause 7 of this Data Processing Agreement;

10. to notify Controller in the event that a supervisory authority contacts Processor in relation to the Processing of Personal Data, insofar as permitted by law.

6. **Cost for Processor's assistance and audits**

1. If the Controller requires assistance from the Processor or the Processor's Sub-processors pursuant to clauses 5.3, 5.4, 5.5, 5.6 and/or 5.7, the Processor shall be entitled to payment from the Controller for such assistance at the hourly rates and compensation of costs as set out in **Appendix 3**.

2. If the Controller requires additional audit reporting or additional other similar documentation than what is covered and comprised by the annual audit report prepared by the Processor, see clause 5.8, the Processor shall be entitled to payment from the Controller for the preparation of such additional reporting and documentation in accordance with the hourly rates and compensation of costs as out in Appendix 3.

3. Notwithstanding clauses 6.1 and 6.2, Processor is not entitled to payment for assistance or additional reporting or documentation if the Controller's request arises out of circumstances, which are attributable to Processor's breach of security or Processor's breach of its obligations as set out in this Data Processing Agreement.

7. **Personal Data breach**

1. Processor will notify the Controller without undue delay after becoming aware of a Personal Data Breach.

2. The aforementioned notification shall describe the nature of the Personal Data Breach including where possible: (i) the (estimated) time of the Personal Data Breach; (ii) the likely consequences of the Personal Data Breach and (iii) reasonable measures taken or proposed by the Processor to mitigate the consequences of the Personal Data Breach.

8. **Records of Processing activities**

1. The Processor shall maintain, in written and electronic form, records of all categories of Processing activities carried out on behalf of the Controller according to the Agreement.

2. The Processor shall make the records available to the supervisory authority on request.

9. **Deletion of Personal Data**

1. In relation to the Software Services the Processor will give Controller access to system functionality in order for the Controller to delete and/or return (i.e. export) any and all of Controller's data including the Personal Data during the term of the Data Processing

Agreement and/or upon the termination of the Data Processing Agreement, see clause 14.

2. In relation to the Consultancy Services the Processor will delete and/or return any and all of Controller's data including the Personal Data at the deletion date specified in the Service Order, or in the absence of a specified date after termination of the Data Processing Agreement, or otherwise earlier if requested by the Controller, and in any event within the timeframes referenced in clause 9.3 below. For the avoidance of doubt the Controller's data including the Personal Data that is stored and processed as part of the Software Services, if any, is in any event deleted in accordance with clause 9.1.

3. The process and timeframes for deletion of Controller's data including the Personal Data are described in **Appendix 4**.

4. If Controller requests the Processor's assistance to delete and/or return (i.e. export) the Controller's data including the Personal Data the Processor is Processing as part of the Software Services during the term of the Data Processing Agreement and/or upon the termination of the Data Processing Agreement, see clause 14, such assistance shall be rendered by Processor at Controller's expense and the Processor shall be entitled to payment at the hourly rates and compensation of costs set out in Appendix 4.

10. **Sub-processing**

1. The Processor shall not engage a Sub-processor, unless this is approved by the Controller by (i) a general or specific authorisation according to **Appendix 5** to this Data Processing Agreement, or (ii) specific instruction from the Controller.

2. In the event that Processor engages Sub-processors for carrying out Processing activities on behalf of the Controller in accordance with Appendix 5, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on that Sub-processor by way of a contract or other legal act under EU or national 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 this Data Processing Agreement.

3. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, thereby giving the Controller the opportunity to object to such changes. However, the Controller cannot object to any intended changes concerning the addition or replacement of Sub-processors if the new Sub-processor provides sufficient guarantees with respect to implementation of appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR as outlined in this Data Processing Agreement. If the Controller does not object to changes concerning the addition or replacement of Sub-processors within 30 days from the Processor's notification of the intended changes, such changes shall be deemed to be accepted by the Controller.

4. Processor shall remain liable to the Controller for a Sub-processor's fulfilment of its data protection obligations.

5. The Controller may request in writing that the Processor demonstrates its Sub-Processor's compliance with the obligations laid down in Article 28 of the GDPR. In such case, the Processor shall be entitled to fulfil this obligation by the audit reports (or similar documentation) that the respective Sub-Processors prepare and make available for this purpose. The foregoing is on the condition that such audit reports etc. contain information stating that the Sub-Processor in question complies with the GDPR and provided that such audit report(s) or similar documentation shall be based on applicable, acknowledged audit standards, such as ISAE 3000 or 3402 or similar standards. Any additional audit reporting or additional other similar documentation requested by the Controller will be at the Controller's cost and expenses and the Processor shall be entitled to payment at the hourly rates and compensation of costs set out in Appendix 3.

11. **Change of instructions**

1. Prior to any change of the instructions given by the Controller, see clause 2, the Parties shall to the widest possible extent discuss in good faith, and if possible agree on, reasonable terms for the implementation of such changes, including the implementation period and the related costs.

2. The Processor shall use reasonable endeavours to comply with any legislative changes. However, the Processor shall not be obligated to implement any change of the instructions if the Parties cannot in good faith agree to reasonable terms for the implementation. If the Parties fail to agree in good faith to reasonable terms regarding change of the instructions each Party shall be entitled to terminate this Data Processing Agreement with a written notice of 60 days, provided that such changes are deemed necessary to comply with the GDPR or other applicable EU or national data protection laws and regulation. The Agreement and any other agreement between the Parties involving Processing of Personal Data shall automatically terminate at the same time.

3. Unless otherwise agreed the following applies:

i. The Processor shall without undue delay initiate implementation of agreed changes of the instructions and shall ensure that such changes are implemented without undue delay in relation to the nature and extent of the changes;

ii. The Processor is entitled to payment of all costs directly connected with changes of the instructions, including implementation costs and increases costs for delivery of the Services;

iii. The Controller must without undue delay be informed of the indicative estimate of the implementation period and the related costs;

iv. Changes to the instructions are not regarded as being in force until the time when such changes have been implemented, provided that the implementation of such changes is carried out in accordance with this clause 11.3;

v. The Processor is exempt from liability towards the Controller for failure to deliver the Services to the extent (including in terms of time) that delivery of the Services will be contrary to the changed instructions, or delivery in accordance with the changed

instructions is impossible. This may be the case in the event that (i) the changes cannot be made due to technical, practical or legal reasons, (ii) the Controller explicitly states that the changes are to apply before implementation is possible, or (iii) during the period until the Parties carry through any necessary changes of the Data Processing Agreement in accordance with the amendment procedures herein.

12. **Confidentiality**

1. Neither Party shall disclose any confidential information. This information includes, but is not limited to Personal Data, documents marked "confidential", information of which the confidential nature must be assumed and information that has not been made publicly available by any Party.

2. A Party may only disclose confidential information when obliged by applicable law or unless otherwise agreed upon, signed in writing.

3. Processor ensures that persons authorised by it to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. The Processor must ensure that the persons performing work for the Processor and who have access to Personal Data, only process such Personal Data as instructed by the Controller, unless processing is required under applicable EU law or national legislation.

13. **Liability**

1. The Processor is liable for damages in accordance with the general rules of Danish substantive law subject to the terms set out in this clause 13 and the limitations set out in the Processor's General Terms and Conditions. The terms set out in this clause 13 only applies to the Processor's liability related to Software Services.

2. Notwithstanding any limitations of the Processor's liability set out in this clause 13, the Processor shall be liable for documented loss suffered or costs incurred by the Controller due to the Processor's wilful misconduct or gross negligence or due to the Processor's failure to comply with its mandatory obligations towards a supervisory authority.

3. The Processor has taken out a Professional Indemnity & Cyber Insurance with an insurance coverage of EUR 1,250,000 per claim and in the annual aggregate (the "Insurance Policy"). The Insurance Policy covers liability of the Processor in relation to the Software Services, and may as such serve as additional security for the Controller. In any case, the Processor's liability is limited to the amount that is paid out in that specific case under the Insurance Policy, and if applicable, increased by the deductible.

4. If for whatever reason, the Insurance Policy does not entitle Processor to any payment, the Processor's liability will in any case be limited to direct damages, with a maximum amount of three (3) times the sum invoiced to Controller pursuant to the Agreement in the foregoing twelve (12) months after a claim was made.

5. The Processor shall not be liable to pay damages for any indirect, consequential or incidental loss or damages including but not limited to loss of goodwill, loss of expected profit and/or loss of operation, arising out of or in connection with the Data Processing Agreement.

6. The Processor shall not be liable for loss or damages if caused by the Controller's failure to comply with its obligations according to applicable EU or national data protection laws and regulations or this Data Processing Agreement. Nor shall the Processor be liable for loss or damages in the event of the Controller's breach of the Agreement and/or other agreement between the Parties involving Processing of Personal Data, or the Controller's failure to comply with its obligations towards a supervisory authority.

7. Any claims put forward by the Controller for compensation of damages will expire 12 months after the date on which the Controller became aware of or ought to have become aware of said damage.

14. Term and Termination of the Data Processing Agreement

1. The commencement date of the Data Processing Agreement is the same date as the commencement date of the Agreement.

2. The termination of the Data Processing Agreement does not affect provisions relating to confidentiality and those provisions, which by nature are intended to survive the termination.

3. This Data Processing Agreement forms an integral part of the Agreement, and consequently terminates simultaneously with the termination of the Agreement.

4. A Party may terminate the Agreement in the event of the other Party's material breach of this Data Processing Agreement. Where such breach is capable of being remedied, a Party may only terminate the Agreement if the breaching Party has not remedied such breach within 30 days after giving written notice of such breach and the consequences of failure to remedy the breach.

5. Notwithstanding termination of this Data Processing Agreement according to this clause 14, the Data Processing Agreement shall be force for as long as the Processor Processes Personal Data on behalf of the Controller, for example in respect of the deletion processes described in Appendix 4.

15. Governing Law and amendments

1. Any disputes related to this agreements to which these terms apply, shall be brought before the courts, with the City Court of Copenhagen as the court of first instance.

2. Danish substantive law shall apply without regard to its principles of conflicts of law.

3. In the event that Parties agree to amend the Agreement, except for amendments made in a Software Service Order or Consultancy Service Order, said amendments shall be attached to the Data Processing Agreement in an additional Appendix 6. Amendments to the Data Processing Agreement are only valid if the provisions concerned in the Data

Processing Agreement are explicitly referred to (when applicable) and explicitly derogated from; and only if signed and dated by both Parties.

Appendix 1 Details of Processing of Personal Data

This Appendix forms part of the Data Processing Agreement.

Description of the activities by the Processor relevant to the Processing of Controller's Personal Data:

1. Depending on the scope and nature of the Agreement, the activities to be performed by the Processor under this Agreement relevant to the Processing of Personal Data may include the following:

2. Provision of various online data processing services including among others a survey and reporting tool via software solutions and platform made available from enalyzer.com (Software Services).

3. Hosting of Personal Data.

4. Provision of consultancy, support and/or education services (Consultancy Services).

2.   Third Party Integration Services

2.1. As part of the Agreement, when using Enalyzer the Controller can choose to utilize – and in such case instructs the Processor to use – various integration services and/or applications using third party software ("Third Party Integration Services"). Some of these Third Party Integration Services are made available to the Controller by the Processor's Sub-processors (see Appendix 5), whereas other Third Party Integration Services are offered to the Controller by independent service providers that are not Sub-processors of the Processor. In such case, the Controller must enter into a separate agreement with the third party service provider.

3.   Data Subjects

3.1. The Controller will import Personal Data to the Processor's Services for Processing by Processor that may concern any of the following categories of Data Subjects, including but not limited to:

3.1.1.   Controller's employees, board members and officers

3.1.2.   Controller's customers, clients and other business partners

3.1.3.   Citizens of Controller

3.1.4.   Students, pupils and other users of public and private institutions

3.1.5.   Children

3.1.6.   Patients and relatives

3.1.7.   Private users

3.1.8.   Business Users

3.1.9.   Members of foundations, unions, associations and/or political originations

4.   Categories of data

4.1. The Personal Data Processed may fall within any of the following categories of data:

4.2. Personal Data covered by GDPR article 6 including but not limited to contact information such as name, address, phone and/or mobile, gender, age, date of birth, preferences, employment position, family status etc.;

4.3. National identification number;

4.4. Personal Data covered by GDPR article 9)*;

4.5. Personal Data relating to criminal convictions and offences (cf. GDPR art. 10).

 GDPR art. 9 includes: data revealing racial or ethnic origin, political opinions, religious and/or philosophical beliefs, trade union membership, processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health and/or data concerning a natural person's sex life or sexual orientation.

For the processing of Personal Data covered by art. 9 the Controller must obtain explicit consent from the Data Subjects.

Appendix 2 Instructions - Processing of Personal Data

This Appendix forms part of the Agreement.

A. Security of Processing

1. 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 the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a. encryption of Personal Data when transmitted via public networks and in connection with remote access to Controller's systems;

b. the ability to ensure the 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 testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

3. The Processor hosts the data, including Personal Data, of the Controller via Microsoft Cloud Azure. The online hosting Services are delivered from data centres solely situated within EU, in Ireland and the Netherlands.

4. The particular security measures to be taken out by the Processor under this Agreement are specified in more detail on www.enalyzer.com (Processor's Security and Privacy Protection Policies). The Controller hereby agrees that in respect of the Processor's Processing of the Controller's Personal Data under this Agreement the foregoing security measures constitute appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

B. Third Party Integration Services

1. If the Controller – or the Processor on behalf of the Controller – uses integration services and/or applications using third party software ("Third Party Integration Services") where the Controller must enter into a separate agreement with the independent third party service provider, see Appendix 1, clause 2, the Controller hereby authorises and instructs the Processor to perform the following Processing on behalf of the Controller:

a. provide, transmit or transfer the data, including Personal Data, of the Controller to the third party provider of the relevant Third Party Integration Service, provided and only to the extent this is necessary for the performance and use by Controller of the said integration services and/or applications; and

b. Process data, including Personal Data, of the Controller that are transferred from the third party provider of the relevant Third Party Integration Service to the Controller's Services with Processor.

2. It is the sole responsibility and liability of the Controller to ensure the necessary basis of lawful Processing for the transfer of the Controller's Personal Data to and from any third party provider of a Third Party Integration Service that is used by the Controller via Enalyzer.

3. Enalyzer shall not be responsible or liable for the Processing by any third party provider of the Controller's Personal Data in this respect.

C. Processing location

1. Processing of the Personal Data is performed by Enalyzer at Enalyzer's office address (Refshalevej 147, 1432 Copenhagen, Denmark) and otherwise on locations agreed from time to time with the Controller and remotely via secure virtual private network.

2. Processing of Personal Data performed by Sub-Processor's is done at the locations set out in Appendix 5.

Appendix 3 Costs for Assistance and Audits

This Appendix forms part of the Agreement.

1.   In the event that Controller requires assistance from the Processor or any of the Sub-processors pursuant to this Agreement, such assistance is charged as follows:

i)   payment for time spend per person, including preparation, at an hourly rate of € 150 excluding VAT (if applicable); and

ii)   payment of reasonable costs and expenses incurred during the course of providing a task or otherwise as a necessary part of such task or other assistance.

2.   Notwithstanding clause 1, in the event that the applicable hourly rate charged by a Sub-processor for the required assistance exceeds the hourly rate of € 150, Enalyzer shall be entitled to payment of the difference between the hourly rate set out in clause 1 and the rate charged by the Sub-Processor.

3.   All costs and expenses of audits or inspections required and conducted by the Controller or its representatives in respect of the Processor's or the Processor's Sub-processors' compliance with article 28 of the GDPR shall be borne solely by Controller unless otherwise specifically follows from the Agreement.

Appendix 4 Deletion of Data

This Appendix forms part of the Agreement.

A. Data deletion processes and periods

The processes and periods for deletion of the Controller's data including Personal Data is described below.

Notwithstanding the termination of the Agreement, the Processor's Processing of the Controller's Personal Data during the deletion periods set out below is to be regarded as taking place according to the Controller's instructions, see also clause 14 of the Agreement. It is the sole responsibility of the Controller that its data including the Personal Data is deleted in compliance with the GDPR.

B. The Controller's deletion of data during the term of the Agreement

During the term of the Agreement, the Controller can (i) independently delete or export its data Processed as part of the Software Services, including the Personal Data at any time by using the system functionality for deletion/export, and/or (ii) instruct Processor to delete its data Processed as part of the Consultancy Services.

Upon deletion of the data by the Controller, cf. (i), the Processor will automatically delete the data within a period of up to 90 days, depending on the type of data (e.g. data concerning respondents will be deleted in 10 days and a whole survey project will be deleted in 90 days). If Processor receives a request to delete data Processed as part of the Consultancy Services, cf.

(ii), subject to sub-processor deletion procedures and limitations, the Processor will delete the data within reasonable time after having received the request.

If the Controller deletes an organization, the Processor will automatically delete all data Processed as part of the Software Services after 110 days.

In all cases, backups of data are *in any case* kept by the Processor for thirty (30) days after the automatic deletion has been made, where after the backups will be deleted by the Processer, unless Union or Member State law requires storage of the Personal Data.

C. Deletion or export of data Processed as part of the Software Services upon Controller's request

The Controller may at any time request the Processor's assistance to perform deletion of or to export data Processed as part of the Software Services, including Personal Data, subject to separate payment for these services at an hourly rate of 150 Euro.

Upon receipt of such written request from the Controller, the Processor will within a maximum of five (5) working days immediately delete or export Controller's data in accordance with the Controller's instructions.

Backups of all data are *in any case* kept by the Processor for thirty (30) days after deletion where after the backups will be deleted by the Processer, unless Union or Member State law requires storage of the Personal Data.

D. Deletion of data after termination or expiry of the agreement

In the event that the Controller deletes its Enalyzer account, the Agreement in respect of Software Services will automatically terminate. For the avoidance of doubt it will not affect any agreed Consultancy Services. In such case a grace period of twenty (20) days will take effect. The grace period is provided in case the Controller's deletion of the account was due to a mistake.

Unless prior to the expiry of the grace period (i) the Controller informs the Processor in writing that the Controller's deletion of the account was a mistake, or (ii) the Parties otherwise agree to continue the Agreement, the deletion process will automatically initiate after the expiry of the grace period and the Controller's data Processed as part of the Software Services, including the Personal Data, will be automatically deleted after ninety (90) days by the Processor.

The Processor will by default initiate deletion of the Controller's data Processed as part of the Consultancy Services at the deletion date specified in the Consultancy Service Order. The Controller's data Processed as part of the Consultancy Services will be deleted from all systems used by the Processor as soon as possible after deletion has been initiated, and no later than six months thereafter. In the absence of a specified date the data will be deleted following expiry of the Agreement, which will either be when all agreed Consultancy Services has been delivered, or if it can otherwise be concluded that no further Consultancy Services will be delivered. In such cases the Controller's data Processed as part of the Consultancy Services, including the Personal Data, will automatically be deleted by the Processor no later than two years after the expiry.

Backups of all data are *in any case* kept by the Processor for thirty (30) days after deletion where after the backups will be deleted by the Processer, unless Union or Member State law requires storage of the Personal Data.

Appendix 5 Sub-Processors and Transfer to Third Countries Outside EU

This Appendix forms part of the Agreement.

A. General Authorisation for use of Sub-processors

1. The Controller hereby gives the Processor its prior general authorisation to use Sub-processors. A list of Sub-processors currently used by the Controller is set out in the table set out below.

B. Required Sub-Processor

Microsoft Azure is the underlying infrastructure for the entire Enalyzer software platform including hosting, database and backup storage. As a consequence, Microsoft is a required Sub-processor in relation to all services provided by Enalyzer. All data is kept within EU and provided by highly secure and scalable hosting centres in Ireland and the Netherlands. For more information on Microsoft Azure visit www.enalyzer.com.

Name	Corporate Address	Processing Location	Hosting Platform	Description of processing activity
Microsoft Corporation	1 Microsoft Way Redmond, WA 98052 USA	Dublin, Ireland (EU) Amsterdam, The Netherlands (EU)	Microsoft Azure	Hosting Enalyzer Platform
Microsoft Corporation	1 Microsoft Way Redmond, WA 98052 USA	Dublin, Ireland (EU) Amsterdam, The Netherlands (EU)	Microsoft Azure	Customer project management in MS Teams (only for Consulting Services)

C. Optional Sub-Processors – Software Services

Certain features or Services within the Enalyzer platform, can be chosen by the user. In these cases, the following Sub-processors apply (to the extent the related features or services are chosen by the user).

Name	Corporate Address	Processing Location	Hosting Platform	Description of processing activity
MailJet (Mailgun Technologies Inc.)	112 E Pecan St. #1135 San Antonio, TX 78205 USA	Frankfurt, Germany (EU) Saint-Ghislain, Belgium (EU)	Google Cloud	Sending of e-mails. E.g. invitations to surveys and reports. Mailjet is hosting the e-mail engine.
SendGrid (Twilio Inc.)	375 Beale St. #300 San Francisco, CA 94105 USA	Herndon, VA (USA) Las Vegas NV (USA) Chicago, IL (USA)	Amazon Web Services	Sending of e-mails. E.g. invitations to surveys and reports. Sendgrid is hosting the e-mail engine.
Zapier Inc.	548 Market St. #62411. San Francisco, CA 94104-5401 USA	US-East-1, North Virginia (USA)	Amazon Web Services	3. party integration platform to more than 1500 apps.
Zendesk	989 Market St San Francisco, CA 94103 USA	Frankfurt, Germany (EU) Dublin, Ireland (EU)	Amazon Web Services	Support system. E.g. when users request support through a ticket within Enalyzer or by sending a mail to support@enalyzer.com (only for Software Services)

D. Optional Sub-Processors – Consulting Services

The Customer may decide to make use of certain supplementary features and services in connection with Consulting Services provided by Enalyzer. In these cases, the following Sub-processors apply (to the extent the Customer has decided to make use of the relevant features and services).

Name	Corporate Address	Processing Location	Hosting Platform	Description of processing activity
MailJet (Mailgun Technologies Inc.)	112 E Pecan St. #1135 San Antonio, TX 78205 USA	Frankfurt, Germany (EU) Saint-Ghislain, Belgium (EU)	Google Cloud	Sending of e-mails. E.g. invitations to surveys and reports. Mailjet is hosting the e-mail engine.
SendGrid (Twilio Inc.)	375 Beale St. #300 San Francisco, CA 94105 USA	Herndon, VA (USA) Las Vegas NV (USA) Chicago, IL (USA)	Amazon Web Services	Sending of e-mails. E.g. invitations to surveys and reports. Sendgrid is hosting the e-mail engine.
Zapier Inc.	548 Market St. #62411. San Francisco, CA 94104-5401 USA	US-East-1, North Virginia (USA)	Amazon Web Services	3. party integration platform to more than 1500 apps.
Zendesk	989 Market St San Francisco, CA 94103 USA	Frankfurt, Germany (EU) Dublin, Ireland (EU)	Amazon Web Services	Support system. E.g. when users request support through a ticket within Enalyzer or by sending a mail to support@enalyzer.com (only for Software Services)
Airtable (Formagrid Inc)	799 Market St, Floor 8, San Francisco, CA 94103 USA	US-East-1, North Virginia (USA) US-West-2, Oregon (USA)	Amazon Web Services	Provider of a generic tool to supplement Enalyzers reporting on e.g., customer action plans and target group validation (only for Consultancy Services)

Formstack LLC	11671 Lantern Road Suite 300 Fishers, Indiana, IN 46038 USA	US-East-1, North Virginia (USA) US-West-2, Oregon (USA)	Amazon Web Services	Create PDF reporting documents for non standard Enalyzer reporting (only for Consulting Services)
Mailparser (SureSwift Capital Inc)	113-1834C Oak Bay Avenue, V8R 0A4 Victoria, British Columbia Canada	US-East-1, North Virginia (USA)	Amazon Web Services	Extract data from emails & attachments and get structured data back (only for Consulting Services)
Files.com/Brick FTP (Action Verb LLC)	7135 Bermuda Rd Las Vegas, NV, 89119-4308 USA	Frankfurt, Germany (EU)	Amazon Web Services	Exchanging files, e.g., respondent data (only for Consulting Services)
HostedSftp	100-51 Breithaupt Street Kitchener, ON, N2H 5G5 Canada	West Virginia, (USA)	Amazon Web Services	Exchanging files, e.g., respondent data (only for Consulting Services)
Stackerapp (Stacker Software Ltd)	417 Mile end road, E3 4PB London UK	Saint-Ghislain, Belgium (EU)	Google Cloud	Online presentation overlay to Airtable databases. E.g., used for customer facing action plan tools and target group validation (only for Consulting Services)

E. Transfer of Personal Data to third countries outside EU

1. Controller hereby authorizes the Processor to transfer Personal Data for processing by its Sub-Processors at their processing locations in the third countries or territories outside EU, that are specified in above table. Processor must ensure that the transfer of the Personal Data to the third countries mentioned in the above table is lawful, including i.e. that, there is legal basis ensuring an adequate level of protection of the transferred Personal Data.

2. The legal basis for such transfer may be in the form of:

a. The Commission's decision in accordance with Art. 45(3) of the GDPR that the third countries, territories or one or more specified sectors within a third country, or an international organisation in question ensures an adequate level of protection; or

b. Standard Contractual Clauses (SCC) (Controller-Processor).

Controller hereby authorises Processor to enter into Standard Contractual Clauses (SCC) (Controller-Processor) on behalf of the Controller for the transfer to Sub-Processors outside EU in order to provide for a legal basis of transfer including such other appropriate safeguards as is required in order to ensure the lawful processing of the Personal Data in compliance with the GDPR.

Transfer of data pursuant to the EU-US Data Privacy Framework is covered by the legal basis for the transfer set out in 2.a. above.