

ANALYZER DATA PROCESSING AGREEMENT

(for Processing within the EU)

Applicable to the agreement(s) entered into by Analyzer A/S and the customer regarding use of Analyzer's services.

BETWEEN:

Customer, hereinafter referred to as: "**Controller**"

and

Analyzer Software A/S, CVR-No. 32443591, having its registered office at Refshalevej 147, 1431 Copenhagen, Denmark, hereinafter referred to as: "**Processor**"

Collectively referred to as "**Parties**" and individually referred to as "**Party**"

LIST OF CONTENTS:

1. DEFINITIONS	3
2. SCOPE AND DETAILS OF PROCESSING	4
3. SECURITY MEASURES	5
4. OBLIGATIONS OF THE CONTROLLER	5
5. GENERAL OBLIGATIONS OF THE PROCESSOR	6
6. PERSONAL DATA BREACH	7
7. RECORDS OF PROCESSING ACTIVITIES	7
8. COSTS FOR ASSISTANCE AND AUDITS	8
9. DURATION OF PERSONAL DATA STORAGE	8
10. SUB-PROCESSING	8
11. CHANGE OF INSTRUCTIONS	9
12. CONFIDENTIALITY	10
13. LIABILITY	11
14. TERM AND TERMINATION OF THE AGREEMENT	11
15. GOVERNING LAW AND AMENDMENTS	12
16. ACCEPTANCE AND EXECUTION	12
APPENDIX 1 DETAILS OF PROCESSING OF PERSONAL DATA	13
APPENDIX 2 SECURITY OF PROCESSING	15
APPENDIX 3 COSTS FOR ASSISTANCE AND AUDITS	16
APPENDIX 4 DELETION OF DATA	17
APPENDIX 5: SUB-PROCESSORS	18

WHEREAS

- i. Processor offers various online data processing services including among others a survey and reporting tool to Controller via Processor's online platform and/or consultancy services as further defined in article 1.8 ("Processor's Services") which includes processing of personal data and is in that capacity a processor in a legal sense.
- ii. Controller intends to use Processor's Services. By usage of Processor's Services, Controller may share Personal Data (as defined under article 1.2) of its Data Subjects with Processor and is in that capacity a 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 this 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. Parties acknowledge that modification of the Agreement may impair its validity in the light of the aforementioned legislation.
- vi. In this Agreement 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 Parties
- vii. In the event of any discrepancies between this Agreement and any other agreements between the Parties, including the Main Agreement, concerning a matter in relation to the Processing of Personal Data, the terms of this Agreement shall prevail.

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

- 1.1. In addition to the definitions used elsewhere in this Agreement, the definitions set out below shall apply and have the meaning set out therein.
- 1.2. '**Agreement**' shall mean this data processing agreement including its appendices;
- 1.3. '**Personal Data**' shall mean any information in connection with the Service 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 identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- 1.4. **'Processing'** shall mean any operation or set of operations in connection with the Service Agreement which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
 - 1.5. **'Third Country'** shall mean countries outside the EU and European Economic Area (EEA).
 - 1.6. **'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, who are authorized to process the Personal Data;
 - 1.7. **'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;
 - 1.8. **'Main Agreement'** shall mean the Agreement between Controller and Processor regarding use of Processor's Services and/or the Consultancy Agreement between Controller and Processor;
 - 1.9. **'Processor's Services'** shall mean (i) the various online data processing services rendered by Processor pursuant to the Main Agreement, including among others provision of a survey and reporting tool and hosting of Controller's data, including Personal Data and/or (ii) consultancy services provided by the Processor according to the Main Agreement, and/or (iii) support and/or education services provided by the Processor from time to time to the Controller;
 - 1.10. **'EU'** shall mean the European Union including the European Economic Area (EEA).

2. Scope and details of Processing

- 2.1. 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 Agreement. The Processor shall Process the Personal Data only on documented instructions from the Controller. The Parties agree that this Agreement shall constitute the instructions as of the date of the Agreement. The Processor may – unless otherwise specifically is set out in the Agreement – apply all relevant means, including software, servers and IT systems.

- 2.2. The Controller may at any time amend or specify the instructions in accordance with article 11. Notwithstanding the foregoing, article 11 can only be amended according to mutual agreement between the Parties.
- 2.3. 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**, which forms an integral part of the Agreement.

3. Security measures

- 3.1. 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 other applicable national and EU data protection law and ensure the protection of the rights of the Data Subjects.
- 3.2. The details of the security measures taken by Processor in this respect for the Processing of Personal Data are specified in **Appendix 2**, which forms an integral part of the Agreement.
- 3.3. 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 out in this clause 3 at the time of the conclusion of this Agreement.
- 3.4. If the Controller after the conclusion of this 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 Agreement.

4. Obligations of the Controller

The Controller agrees:

- 4.1. To ensure that the Personal Data collected by Controller is done in accordance with 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 (and where applicable has been notified to the relevant authorities of that Member State) and does not violate the relevant provisions of that Member State.
- 4.2. That Controller shall indemnify Processor for any cost, charge, damages, expenses, administrative fines or loss or damage it has suffered or incurred due to a violation by Controller of the GDPR or applicable EU or national data protection law or this Agreement.

5. General obligations of the Processor

The Processor agrees:

- 5.1. to process the personal data in accordance with the security measures set out in Appendix 2;
- 5.2. to process Personal Data only in accordance with the instructions from the Controller, cf. clause 2, 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;
- 5.3. 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;
- 5.4. 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 and prior consulting or supervisory authorities, cf. articles 35 and 36 of the GDPR;
- 5.5. to provide Controller upon request and within reasonable time the information necessary to demonstrate compliance with the obligations laid down in this clause 5;
- 5.6. to cooperate (including representatives of Processor), on the Controller's request, with the supervisory authority in the performance of its tasks;
- 5.7. 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;
- 5.8. to once a year make an audit report available on the Processor's website with information indicating that the Processor complies with the Agreement. The report shall be based on applicable, acknowledged audit standards, e.g. ISAE 3000, ISO 27001 or similar;
- 5.9. to notify Controller in the event of a Personal Data Breach as set out in clause 6;

- 5.10. To notify Controller in the event that a supervisory authority contacts Processor, insofar as permitted by law.

6. Personal Data breach

- 6.1. Processor will notify the Controller without undue delay after becoming aware of a Personal Data Breach.
- 6.2. The aforementioned notification shall describe the nature of the Personal Data Breach including where possible: (i) the categories and number of Data Subjects concerned and the categories and number of registrations of Personal Data, (ii) the (estimated) time of the Personal Data Breach; (iii) the likely consequences of the Personal Data Breach; (iv) reasonable measures taken or proposed by the Processor to mitigate the consequences of the Personal Data Breach and (v) information about the data protection officer or other contact person where additional information can be obtained.
- 6.3. The Controller shall immediately notify the Processor in writing of any possible unauthorised use of log-in information, passwords, credentials or other security breaches related to the Service Agreement.
- 6.4. If the Processor cannot give all of the above information at the same time the Processor is entitled to give the above information without undue delay after it becomes available.
- 6.5. If a Personal Data Breach is not due to circumstances that are caused by the Processor or its Sub-processors the Processor shall be entitled to charge the Controller for assistance requested by the Controller in this respect of this clause 6 in accordance with the conditions set out in Appendix 3, which forms an integral part of the Agreement.
- 6.6. If the Controller becomes aware of a Personal Data Breach that influences or is likely to influence the Processor's or its Sub-processor's operations the Controller shall as soon as possible and without undue delay inform the Processor hereof in writing and to the widest extent possible provide the same information (where applicable) as stipulated in clause 6.2 and 6.3.

7. Records of Processing activities

- 7.1. 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 Main Agreement, containing:
 - (i) the name and contact details of the Processor and any Sub-processors and where applicable their respective representatives and/or data protection officer;
 - (ii) name and contact details of the Controller;
 - (iii) the categories of Processing carried out on behalf of the Controller;
 - (iv) where applicable, transfers of Personal Data to a Third Country or an international organisation, including the identification of that Third

Country or international organisation, and, in the case of transfer referred to in the 2nd subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;

(v) a general description of the technical and organisational security measures as referred to in Appendix 2 and subsequent amendments thereto.

7.2. The Processor shall make the records available to the Controller and the supervisory authority on request.

8. Costs for assistance and audits

8.1. In the event Controller requires assistance of Processor or the Processor's Sub-processors pursuant to this Agreement (including, but not limited to clauses 5.3, 5.4, 5.5, 5.6, 5.7 clause 6.5 and/or clause 7.2), this assistance is charged under the conditions set out in **Appendix 3**, which forms an integral part of the Agreement.

8.2. The annual audit report made available on the Processor's website according to clause 5.8 shall be prepared at the Processor's expense. Any additional audit reporting or additional other similar documentation requested by the Controller shall be prepared and made available according to separate agreement and at the expense of the Controller and is charged under the conditions set out in Appendix 3.

9. Duration of Personal Data storage

9.1. 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 Agreement. Upon expiry of the Agreement the Processor will delete all of Controller's data including the Personal Data, unless Union or Member State law requires storage of the Personal Data.

9.2. The process and timeframes for deletion of Controller's data including the Personal Data is described in **Appendix 4**, which forms an integral part of the Agreement.

9.3. If Controller requests the Processor's assistance to delete and/or return (i.e. export) the Controller's data including the Personal Data during and upon the expiry of the Agreement such assistance shall be rendered by Processor at Controller's expense and is charged under the conditions set out in Appendix 4.

10. Sub-processing

10.1. The Processor shall not engage a sub-processor for the Processing of the Personal Data on behalf of the Controller ("Sub-processor"), unless this is approved by the Controller by (i) a general or specific authorisation according

to **Appendix 5** to this Agreement or (ii) specific instruction from the Controller.

- 10.2. 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 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 Agreement.
- 10.3. 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 with not less than 30 days' notice, 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 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.
- 10.4. Processor shall remain liable to the Controller for the performance of its Sub-processor's obligations.
- 10.5. If the Controller requests the Processor to document its Sub-Processor's compliance with the obligations laid down in Article 28 of the GDPR the Processor shall be entitled to fulfil this obligation by referring the Controller to the relevant audit reports or similar documentation made available by the respective Sub-Processors with information indicating that the Sub-Processor in question complies with the GDPR, provided that such audit report(s) or similar documentation shall be based on applicable, acknowledged audit standards, e.g. ISAE 3000, ISO 27001 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 is charged under the conditions set out in Appendix 3.

11. Change of instructions

- 11.1. Prior to any change of the instructions 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.
- 11.2. 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 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 Main Agreement and other agreement between the Parties involving Processing of Personal Data shall automatically terminate at the same time.

11.3. 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 hereof is carried out in accordance with this clause 11.2.
- (v) The Processor is exempt from liability for failure to deliver the Services to the extent (incl. 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 e.g. 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 Agreement in accordance with the amendment procedures herein.

12. Confidentiality

- 12.1. Neither Party is permitted to 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.
- 12.2. A Party may only disclose confidential information when obliged by applicable law or unless otherwise agreed upon, signed in writing.
- 12.3. Processor ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 12.4. 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

- 13.1. The Processor shall be liable for damages in accordance with the general rules of Danish law subject to the limitations set out in this clause 13.
- 13.2. 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 Agreement.
- 13.3. 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 Agreement or in the event of the Controller's breach of the Main Agreement and/or other agreement between the Parties involving Processing of Personal Data, the Controller's failure to comply with its obligations towards a supervisory authority or penalties imposed by a supervisory authority due to the Controller's breach or failure to comply.
- 13.4. In any case the liability of Processor is limited to the amount that is paid out in that specific case under Processor's liability insurance policy, and if applicable increased by the deductible.
- 13.5. If for whatever reason the aforementioned insurance policy does not entitle Processor to any payment, the Processor's liability will be in any case limited to direct damages, with a maximum of three (3) times the sum invoiced to Controller pursuant to the Main Agreement in the foregoing six (6) months after a claim was made, however, not in any event exceeding a maximum of € 10,000, unless the damage has resulted from a wilful misconduct or gross negligence on the Processor's part.
- 13.6. Notwithstanding the foregoing, the limitations of the Processor's liability set out in this article shall not apply to loss suffered or costs incurred by the Controller due to the Processor's failure to comply with its obligations towards a supervisory authority or penalties imposed by a supervisory authority due to the Processor's material breach.
- 13.7. Any claims by the Controller for compensation of damages will expire one year 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 Agreement

- 14.1. The effective date of the Agreement is determined by the effective date of the Main Agreement.

- 14.2. The termination of the Agreement does not affect provisions relating to confidentiality, and those provisions which by nature are intended to survive the termination.
- 14.3. This Agreement forms an integral part of the Main Agreement, and consequently terminates simultaneously with the termination of the Main Agreement.
- 14.4. A Party may terminate the Main Agreement in the event of the other Party's material breach of this Agreement. Where such breach is capable of being remedied, a Party may only terminate the Main 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.

15. Governing Law and amendments

- 15.1. The legal relationship between Controller and Processor is exclusively governed by the laws of Denmark without regard to its principles of conflicts of law. Disputes between parties will, in the first instance, be exclusively resolved by the District Court of Copenhagen, Denmark.
- 15.2. In the event that Parties agree to amend the Agreement, said amendments shall be attached to the Agreement in an additional **Appendix 6**. Amendments from the Agreement are only valid if the provisions concerned are explicitly referred to (when applicable) and explicitly derogated from; and only if the appendix is signed and dated by both Parties.

16. Acceptance and execution

- 16.1. This Agreement is binding on the Processor.
- 16.2. By Controller's log-in to its Analyzer account and access and continued use of the Processor's Service as of 25 May 2018 the Controller agrees to this Agreement and accepts to be bound by its terms and conditions.

Appendix 1 Details of Processing of Personal Data

This Appendix forms part of the Agreement.

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

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

- 1.1.1. Provision of various online data processing services including among others a survey and reporting tool via software solutions and platform made available from analyzer.com.
- 1.1.2. Hosting of Personal Data.
- 1.1.3. Provision of various consultancy Services.
- 1.1.4. Provision of support and/or education Services.

1.2. As part of the Main Agreement the Controller may also choose to use third party integration services and/or applications made available by the Processor on Enalyzer.com in cooperation with the third party providers of such integration services and applications. If the Controller uses such third party integration services and/or applications it hereby authorises the Processor to:

- i) provide, transmit or transfer the data, including Personal Data, of the Controller to the third party provider of the relevant integration service and/or application, 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
- ii) Process data, including Personal Data, of the Controller that are transferred from the third party provider of the relevant integration service and/or application to the Controller's Services with Processor.

1.3. 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 an integration service and/or application that is used by the Controller via Enalyzer.com and the Processing by any third party provider of the Controller's Personal Data in this respect.

2. Data Subjects

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

- 2.1.1. Controller's employees, board members and officers
- 2.1.2. Controller's customers, clients and other business partners
- 2.1.3. Citizens of Controller
- 2.1.4. Students, pupils and other users of public and private institutions
- 2.1.5. Children
- 2.1.6. Patients and relatives
- 2.1.7. Members of foundations, unions, associations and/or political originations
- 2.1.8. Private users
- 2.1.9. Business Users

3. Categories of data

- 3.1. The Personal Data Processed may fall within any of the following categories of data.
- 3.2. Non-sensitive data (cf. GDPR article 6) of any kind 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.
- 3.3. National identification numbers.
- 3.4. Sensitive data (cf. GDPR article 9)*.
- 3.5. Data relating to criminal convictions and offences (cf. GDPR art. 10).

***Sensitive data 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

Please note that for the processing of sensitive data, explicit consent of the Data Subject is required.

Appendix 2 Security of Processing

This Appendix forms part of the Agreement.

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 Itadel A/S. The online hosting Services are delivered from one or more of Itadel's data centres solely situated within EU.
4. Itadel provides the security measures as described in detail on www.enalyzer.com.
5. Particular security measures to be taken out by the Processor under this Agreement are specified in detail on www.enalyzer.com (Processor's Security and Privacy Protection Policies).

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 Processor's Sub-processors pursuant to this Agreement, such assistance is charged as follows:
 - 1.1. payment for time spend per person, including preparation, at an hourly rate of € 150,- excluding VAT (if applicable), and
 - 1.2. 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. 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.

Data deletion

The Processor operates with different timeframes of deletion of the Controller's data depending on the circumstances. These are described below.

I. The Controller deletes data during the Term of the Agreement

During the term of the Agreement the Controller can delete its data in two (2) ways:

1. Delete a whole survey project. In this case, it will take ninety (90) days before the data regarding the survey project are deleted.
2. Delete respondents in a survey project. In this case, the data regarding respondents will be deleted instantly.

In both 1 and 2, backups of all data are *in any case* kept by the Processor for thirty (30) days after deletion.

II. Deletion after expiry of the Agreement

Upon expiry of the Agreement the deletion process will automatically initiate within a maximum of five (5) working days after the date of expiry. Hereafter a grace period of thirty (30) days will take effect. The grace period is provided, in case the Controller and Processor mutually agree to re-enter into or continue the Agreement. If not, all of the Controller's data will be deleted after ninety (90) days.

Backups of all data are *in any case* kept by the Processor for thirty (30) days after deletion.

III. Deletion or export of data upon Controller's request

The Controller may at any time request the Processor's assistance to perform deletion or export of data subject to separate payment for these services at an hourly rate of 150 Euro.

Upon receipt of such written request the Processor will within a maximum of five (5) working days, immediately delete or export all of Controller's survey project data.

Backups of all data are *in any case* kept by the Processor for thirty (30) days after deletion.

Notwithstanding the expiry of the Agreement the Processor's Processing of the Controller's Personal Data during the deletion periods stipulated in the above clauses is to be regarded as taking place according to the Controller's instructions.

Appendix 5: Sub-processors

This Appendix forms part of the Agreement.

I. General Authorisation

1. The Controller hereby gives the Processor its prior general written authorisation to the Processor to use Sub-processors. A list of the Sub-Processors' used by the Processor at the date of the Agreement is made available hereunder:
2. **Itadel A/S**
 - 2.1. The Processor has entered into an agreement with Itadel A/S whereby Itadel is a Sub-processor to the Processor acting (on the Controller's behalf) to provide hosting Services via Itadel's hosting solution and IT platform. All of Controller's data including Personal Data are hosted in one or more of Itadel's data centers situated within EU. The Hosting services do not take place in countries outside EU. More information about Itadel's hosting solution and IT platform can be found on Enalyzer.com.
 - 2.2. In the event of Itadel's termination of its agreement with the Processor (in whole or in part) regarding the hosting Services, the Processor shall endeavour to provide a new hosting Service to the Controller within the EU as soon as reasonably possible. The Processor is entitled to terminate the Agreement in whole or in part with a prior notice of sixty (60) days.
3. **Processor reserves the right to change hosting provider**
 - 3.1. In addition to the hosting solution offered by Processor to Controller via Itadel A/S, cf. clause 2 above, the Processor has also engaged with Microsoft Corporation as hosting provider via the Microsoft Azure Cloud Platform from data centres in Ireland and/or the Netherlands. The hosting Services provided via Microsoft Azure Cloud Platform are fully compliant with the GDPR and provide as a minimum the same security level as the Itadel hosting solution. However, the Microsoft Azure Cloud Platform does not apply to the Controller at the time of Conclusion of the Agreement. More information about the Microsoft Azure Cloud Platform can be found on Enalyzer.com.
 - 3.2. The Processor reserves the right to move the hosting of all of the Controller's data including Personal Data from Itadel's hosting solution to the Microsoft Azure Cloud Platform. All of Controller's data including Personal Data will in such case henceforth be hosted by Microsoft Corporation on the Microsoft Azure Cloud Platform in Ireland and/or the Netherlands. The hosting Services to be provided by Microsoft Azure will not take place in countries outside EU.
 - 3.3. The Controller hereby accepts that the Processor can change the provider of hosting services to the Controller from Itadel A/S as to Microsoft Corporation's Microsoft Azure Cloud Platform, provided that (i) Processor will notify Controller in writing with not less than 60 days prior to such change to come into effect, and(ii) the hosting Services to be provided by Microsoft Corporation on the Microsoft Azure Cloud Platform will be on similar terms as set out in this Agreement and ensure at least the same level of security and other technical and organisational measures as agreed by the Controller and the Processor in Appendix 2 to this Agreement at the time of such change.

4. **Other Sub-processors**

- 4.1. If the Controller and the Processor has entered into a Consultancy Agreement as part of the Main Agreement, the Processor may engage Sub-processors for the provision of the consultancy Services to the Controller.
- 4.2. If the Processor uses one or more Sub-processors for the provision of consultancy services this is regulated in detail in the Main Agreement (Consultancy Agreement). The Processor will notify the Controller in accordance with clause 10.3 of the Agreement if changes in the Sub-processors applied for the provision of the consultancy Services are made.