Data Processing Agreement

BETWEEN

(1) **UNCOVER LEGAL B.V.,** registered in Amsterdam the Netherlands, with its address at offices at Churchill-laan 115h, 1078 DN, Amsterdam, the Netherlands, registered with the Dutch Chamber of Commerce with number 86232657 ("**Uncover**" or "**Data Processor**"); and

(2) The free trial customer having accepted the applicability of this Data Processing Agreement by logging into the Uncover Free Trial environment (the "**Customer**" or "**Controller**");

Each a "**Party**" and together the "**Parties**",

1. Definitions and interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Data Processing Agreement shall have the following meaning:

"**Data Breach**" means a breach related to Personal Data as referred to in article 4.12 of the GDPR';

"**Data Processing Agreement**" means this agreement, which, together with its annexes, constitute a data processing agreement within the meaning of article 28.3 of the GDPR;

"**Data Protection Authority**" means a supervisory authority defined in article 4.21 of the GDPR;

"**Data Subject**" means a natural person who can be identified, directly or indirectly;

"**DPIA**" means Data Protection Impact Assessments;

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

"**Personal Data**" means all information referred to in article 4.1 of the GDPR, processed by Data Processor on the basis of the Service Agreement and/or Data Processing Agreement for the benefit of Controller;

"**Services Agreement**" means the agreement between the Parties to which this Data Processing Agreement is attached as Schedule 3;

"**Sub Processor**" means a third-party processor engaged by Data Processor;

2. General provisions

2.1 This Data Processing Agreement applies to the Personal Data processed by Uncover, acting as a Data Processor, on behalf of the Customer, acting as a data Controller, as described in this Data Processing Agreement.

2.2 Data Processor processes the Personal Data on the instructions of and for the purposes as determined by Controller and as described in more detail in Appendix 1.

2.3 Data Processor provides Controller with all reasonable information in its possession that Controller requires to comply with the GDPR.

2.4 Controller guarantees that it acts in accordance with the GDPR and other applicable data protection laws and that the nature, use and/or processing of the Personal Data are not unlawful and that it does not violate any third party's rights.

2.5 Data Processor will inform Controller if Data Processor finds that the instructions of Controller conflict with the laws and regulations in force.

2.6 Administrative fines imposed on Controller by a Data Protection Authority cannot be recovered from Data Processor, unless such fine is imposed on Controller due to breach of the obligations of Data Processor under this Data Processing Agreement which cause the Controller to be unable to comply with the GDPR.

3. Term and termination

3.1 This Data Processing Agreement will be in force as long as the Services Agreement is in force. Upon termination of the Service Agreement, this Data Processing Agreement ends by operation of law without any further (legal) act being required.

3.2 If the Data Processing Agreement is terminated, Data Processor shall delete all Personal Data it stores and which it has obtained from Controller, except for Personal Data that is processed by the machine learning models from Uncover and that is anonymized, fragmented and not traceable to any individual, group of individuals or company, unless Data Processor is prevented from removing the Personal Data in full or in part by applicable law.

4. Security

4.1 Data Processor shall implement the technical and organizational security measures set out in Appendix 2 to this Data Processing Agreement in order to assist Controller in ensuring compliance with Article 32 GDPR. In determining appropriate technical and organizational security measures, the Parties will take

account of the current possibilities for technical and organizational protection, the implementation costs and the nature, scope and context of the Personal Data processing. Data Processor does not guarantee that its technical and organizational security measures shall be effective under all circumstances.

4.2 Controller acknowledges and confirms that the technical and organizational security measures set forth in Appendix 2 provide an appropriate level of security as required under the GDPR.

4.3 Data Processor shall be entitled to adjust the technical and organizational security measures it has implemented if, to its discretion, such is necessary for a continued provision of an appropriate level of security. Such adjustments are deemed to become part of Appendix 2.

5. Data Breaches

5.1 If the Data Processor discovers a Data Breach, it shall notify Controller without undue delay. In doing so, Data Processor will indicate as soon as possible what events and circumstances have led to the Data Breach and what measures have been taken to remedy the Data Breach.

5.2 Controller will decide whether a Data Breach must be notified to a Data Protection Authority and/or to the Data Subjects concerned. Any such notification will be submitted by Controller and not by Data Processor.

5.3 Upon Controller's request, Data Processor shall assist Controller to meet its notification obligations under the GDPR by providing all the necessary information available to Data Processor.

6. The rights of Data Subjects, Data Protection Impact Assessments

6.1 Data Processor will provide Controller all reasonable assistance to enable Controller to satisfy requests from Data Subjects for the exercise of their rights under the GDPR. If Data Processor is directly approached by a Data Subject, it shall refer the Data Subject to Controller.

6.2 If the Controller is required to perform a DPIA pursuant to the GDPR, or if the DPIA indicates that the Data Protection Authority must be consulted, Data Processor will provide Controller with reasonable assistance that may be expected from Data Processor in this respect.

6.3 Data Processor is entitled to charge Controller for the costs associated with providing reasonable assistance as stipulated in this article 6 after submitting a prior written statement of the costs to Controller.

7. Confidentiality

7.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

7.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision, order issued by a competent government authority or for the performance of the Service Agreement and/or Data Processing Agreement.

8. Sub-Processing

8.1 In Appendix 1 to this Data Processing Agreement, Data Processor has specified the Sub-Processors it engages. Controller grants Data Processor permission to hire the Sub-Processors listed in Appendix 1 and authorizes Data Processor to replace Sub-Processors and/or add other Sub-Processors. Data Processor shall notify Controller of any changes concerning the addition or replacement of the Sub-Processors hired by Data Processor. Controller shall be entitled to object to such changes and to terminate the Service Agreement and Data Processing Agreement as per the date that the change will come into force.

8.2 Data Processor will enter into an agreement with a Sub-Processor in which the Sub-Processor, in particular with regard to security obligations, is subject to similar requirements as laid down in this Data Processing Agreement.

8.3 When engaging a Sub-Processor, the Data Processor remains responsible for the fulfillment of its obligations arising from this Data Processing Agreement.

9. International aspects

9.1 Data Processor processes the Personal Data exclusively within Europe.

10. Auditing rights

10.1 Controller is entitled, with prior written notification with due observance of a period of two weeks and no more than once per calendar year, or whenever a Data Breach has occurred on the side of Data Processor, to conduct an investigation at Data Processor (hereinafter referred to as an Audit), to check whether the applicable laws and regulations and the provisions of this Data Processing Agreement are complied with. For this, Controller has the right to engage an independent third party, provided that this third party maintains confidentiality.

10.2 Data Processor will provide Controller reasonable cooperation, if and insofar as required for the Audit conducted by or on behalf of the Controller.

10.3 Controller will share the Audit-results with Data Processor within a reasonable period after completion of the Audit. If irregularities are found, the Parties will decide by mutual agreement in which manner and within which period these will be adjusted and remedied.

10.4 Data Processor shall be entitled to invoice Controller for any costs related to the Audit and/or any costs resulting from implementing the measures referred to in this article 10, except where it concerns an Audit due to a Data Breach which has occurred on the side of Data Processor.

11. LIABILITY

The exclusions and limitations of liability as agreed by the Parties in the Service Agreement, of which the Terms & Conditions to the Services Agreement form an integral part, will apply to the liability of each of the Parties arising from or in connection with this Data Processing Agreement and the Service Agreement. This means that the total liability arising from the Service Agreement and Data Processing Agreement jointly, will never exceed the maximum liability set forth in the Service Agreement of which the Terms & Conditions form an integral part.

12. GENERAL TERMS

12.1 In the event of any contradiction between the provisions of this Data Processing Agreement and the Services Agreement, the provisions of this Data Processing Agreement will prevail, unless the Parties expressly agree otherwise in writing.

12.2 The Parties may only amend this Data Processing Agreement in writing.

12.3 Obligations pursuant to this Data Processing Agreement, which by their nature are intended to continue even after termination of this Data Processing Agreement, such as but not limited to the article on liability, will continue to exist after termination of this Data Processing Agreement.

13. GOVERNING LAW AND JURISDICTION

13.1 This Data Processing Agreement is exclusively governed by Dutch law.

13.2 Any disputes that may arise from this Data Processing Agreement will be submitted exclusively to the competent court in Amsterdam.

The remainder of this page is intentionally left blank

Appendix 1 – General Information

1. PURPOSE AND DURATION OF PROCESSING

1.1 Data Processor processes Personal Data on behalf of Controller in the performance of Data Processor's Services for the duration of the Services Agreement. These services include Controller's right to use and access the Uncover platform which uses the Personal Data to provide the Services.

1.2 In order to provide the Services, Data Processor uses Personal Data provided by Controller and uses detection methods (such as machine learning models). Data Processor uses the results of activities performed by Controller and its Authorized Users in order to continuously improve the services in order to provide Customer with the best possible support including the most accurate insights and recommendations for Controller.

1.3 Data Processor also uses the Personal Data provided by Controller in order to generate insights for Controller on its commercial performance. The processing on behalf of Controller will continue until such time as the Services Agreement is terminated.

2. TYPE OF PERSONAL DATA

2.1 The Personal Data that Customer imports to the Uncover Platform.

3. CATEGORIES OF DATA SUBJECTS

The below list is an indication of possible Data Subjects and is not intended to be complete.

- Controller's clients
- Directors and employees of Controller's Clients
- Other natural persons whose Personal Data is processed by using the services due to the nature of these persons' relationship with the Controller's clients or other Data Subjects

4. SUB PROCESSOR(S)

Data Processor has engaged the following Sub-Processors:

- Amazon Web Services, Inc. for cloud infrastructure services.
- Microsoft Azure for artificial intelligence services.

Appendix 2 – Security measures

1. Organizational security

1.1 Uncover maintains the level of maturity required to achieve the ISO 27001 certification. In practice this means:

a. Authorizations are explicitly documented as a matter of procedure;
b. Authorizations are reviewed periodically;
c. All changes to the application, systems and networks are tracked in an auditable way and attributable to individuals;

1.2 Access to Client data or systems is awarded to a strictly limited number of staff that have committed to confidentiality

1.3 A threat model/risk assessment for the Services is performed by an independent third party organization on a yearly basis

2. Data security

2.1 Customer data is classified by Uncover as the highest level of sensitivity and treated accordingly.

3. Network security

3.1 All servers are protected with firewalls.

4. Validation

4.1 Yearly, Uncover has an independent, adequate third party specialized in security testing perform an external and internal security test to validate security measures, in the scope of the penetration test.

4.2 Critical and high severity findings are resolved in a timely manner. A retest is performed to confirm the resolution of the findings.