Data Processing Agreement

Controller: [name controller]

Processor: Crowdtech

Crowdtech B.V.
Generaal Vetterstraat 82
1059 BW Amsterdam
+3120 - 412 0812
crowdtech.com

The undersigned:

1. [Controller], having its registered office at the address xxx, xxx in xxx, duly represented in this matter by Mr/Ms [name], hereinafter referred to as: "**Controller**"

   and

2. The private company with limited liability Crowdtech B.V., having its registered office at the address Generaal Vetterstraat 82, 1059 BW in Amsterdam, duly represented in this matter by Mr. D. Nokes, hereinafter referred to as: "**Processor**".

Collectively referred to as Parties

Parties take the following into account:

a) Controller is obliged to enter into a data processing agreement with Processor for the processing of its (Sensitive) Personal Data under the GDPR.
b) In the context of the activities agreed between the parties as stated in a main agreement, for which this agreement is the written data processing agreement, Processor will process Personal Data for and on behalf of Controller without being subject to the direct authority of Controller.
c) Processor will process Personal Data in the performance of the activities in accordance with the instructions and under the responsibility of Controller.
d) In addition, Controller may instruct Processor in writing to perform other processing activities, which will be added as an appendix to this processing agreement.
e) Processor will only perform data processing that has been instructed in writing by Controller.

Declare that they have agreed the following

Article 1: Assignment

1.1 The Controller issues an order to the Processor, which is accepted by the Processor, to process Personal Data in accordance with this agreement.
1.2 The Processor has no independent authority over the data that is processed for the Controller in accordance with this processing agreement.
1.3 The Processor will only process the Personal Data listed in appendix 1 and provided by the Controller as strictly necessary for the work described therein. If applicable, additional security measures may also be included in this appendix that the Processor will comply with.
1.4 After the assigned tasks have been carried out, the Processor will, at the first written request of the Controller, return files with (Personal) Data that the Controller has made available in the context of this agreement and immediately destroy the copies of these files made by the Controller, unless the Controller disputes the services provided and/or

(Personal) Data. Copies of Personal Data that are part of the Processor's backup routine must be deleted by the Processor as soon as possible.

1.5 If Processor receives requests for access to the data from data subjects, Processor will forward these to Controller without delay. Processor will support Controller in complying with these requests within the period set by law.

1.6 Processor will refrain from performing other processing operations referred to in Article 1, unless otherwise agreed in Appendix 1.

Article 2: Compliance with laws and regulations

2.1 Processor will act in accordance with the GDPR and other applicable laws and regulations regarding data protection when processing Personal Data as described in Article 1.

2.2 Processor will process Personal Data under this agreement exclusively within the European Union/European Economic Area.

Article 3: Indemnification and liability

3.1 If Processor is liable for damage caused by its activities as Processor for Controller, the following provisions apply:

3.1.1 If the damage is covered by the professional and business liability insurance or cyber and data risks insurance of Processor, liability is limited to the amount paid out in that case by the insurer, plus the applicable deductible.

3.1.2 If the damage is not covered by the liability insurance or cyber and data risks insurance, liability is limited to 100% of the annual amount of the compensation that Processor has received for its activities in the context of the assignment.

3.2 Any liability of Processor for any consequential damage suffered by Controller is excluded. Consequential damage includes, among other things, lost income, lost profit, reduced goodwill and/or lost savings.

3.3 Any limitation of liability shall lapse in the event of intent and/or gross negligence by the Processor.

Article 4: Security measures, compliance and incidents

4.1 Processor shall, like Controller, take, maintain, evaluate and, if necessary, adjust and update appropriate technical and organizational measures to protect Personal Data against loss, theft or any form of unlawful processing. These measures shall ensure, taking into account the nature, scope, context and purpose of the processing, the state of the art and the costs of implementation, an appropriate level of security, taking into account the likelihood and severity of the various risks that the processing and the data to be protected entail and shall comply with the provisions of the guidelines and Article 32 GDPR.

4.2 Processor shall, at the request of Controller, provide all information necessary to demonstrate compliance with the provisions of paragraph 1.

4.3 Processor shall enable Controller to inspect the measures taken at its first written request, with the aim of verifying what is stipulated in this agreement.

4.4 Processor will cooperate in this and provide all information relevant to the audit in a timely manner that is necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

4.5 Controller will in principle not conduct an audit of Subprocessors because Processor is fully responsible and liable for this.

4.6 Persons conducting an audit will comply with the security procedures in force at Processor. The costs of an audit will be borne by Controller, unless the audit shows that Processor has acted in breach of this agreement or has failed to take sufficient appropriate measures, taking into account the state of the art and the costs of implementation, given the risks associated with the processing, the nature, scope, context and purpose of the data to be protected.

4.7 Controller will limit the audit to what is established in this agreement, for the data processing and the Personal Data of Controller. Data processing that Processor carries out for other Clients is excluded from this audit. All information that Controller becomes aware of during the audit and that does not relate to Controller will be kept confidential by Controller.

4.8 If Processor, when processing Personal Data, becomes aware of a security breach/data leak that leads to the destruction, loss, modification or unauthorized disclosure of, or unauthorized access to, transmitted, stored or otherwise processed data, which is likely to pose a risk to the rights and freedoms of the data subject, Processor will inform Controller thereof without delay, but no later than within 24 hours of discovery. Processor will take all possible technical and organizational measures in the meantime to stop, prevent and/or repair the security incident. Processor will provide information with the notification regarding the nature of the breach, the nature of the leaked Personal Data, the technical protection measures and other relevant facts and circumstances that are important to determine whether the supervisory authority and/or the data subject should be informed.

4.9 Processor will immediately complete Appendix 2 in full and send it digitally to the contact person of the Controller.

4.10 If there is reasonable doubt as to whether the breach poses a likely risk to the rights and freedoms of the data subject, the Processor will report the breach to the Controller, in order to enable the Controller to form its own opinion as to whether a report is necessary.

4.11 If there is an obligation to report to the supervisory authority or to inform the data subjects, this will be done exclusively by the Controller. Processor will provide its full cooperation and assistance in this regard in order to be able to meet these obligations.

Article 5: Engagement of Subprocessors

5.1 Processor is not permitted to outsource its obligations under the Data Processing Agreement to a Subprocessor without prior general or specific written consent from Controller, whereby Controller may not unreasonably refuse or delay its consent. Consent is hereby granted for the Subprocessors listed in Appendix 1.

5.2 Processor is only permitted to engage a Subprocessor on the basis of a written agreement with the relevant Subprocessor, in which at least the same obligations are imposed on the Subprocessor as are imposed on Processor under this Data Processing Agreement.

5.3 Processor remains responsible for compliance with its obligations under the Agreement and this Data Processing Agreement, as well as for any act or omission on the part of the Subprocessor that causes Processor to breach its obligations under the Agreement or this Data Processing Agreement.

Article 6: Confidentiality

6.1 Processor, its personnel and third parties engaged by it are obliged to maintain confidentiality with regard to the Personal Data of which they become aware or could have become aware, on the basis of article 28 paragraph 3 under b GDPR.

6.2 Processor shall only provide access to the Personal Data to its employees and third parties engaged by it to the extent necessary for the performance of the data processing assigned by the Controller.

6.3 Processor shall oblige the persons employed by it or performing work on its behalf to maintain confidentiality with regard to the Personal Data of which they can become aware.

6.4 Processor's duty of confidentiality may only be breached if a statutory provision requires the provision of data or the official appointed by the Controller has indicated to Processor the need for disclosure.

6.5 If a supervisor of the Controller requests access to the data processing, the Processor must provide all necessary cooperation to enable the Controller to comply with its obligations imposed by supervisors.

6.6 The confidentiality obligation applies both during and after the work has been completed and will continue to exist after termination of this agreement.

6.7 The Processor will inform the Controller of any request for access, provision or other form of retrieval and communication of the Personal Data, unless legislation prohibits this notification for important reasons of general interest.

Article 7: Rights of data subjects

7.1 If a data subject invokes one of his rights under art. 15 to 22 GDPR with the Processor, the Processor will forward this request to the Controller without delay.

7.2 The Processor will provide the Controller with full and timely assistance in the exercise of its obligation to respond to requests regarding the exercise of the rights referred to in paragraph 1.

Article 8: Other provisions

8.1 No general terms and conditions apply to this agreement. Dutch law applies. The competent court is the court that has jurisdiction on the basis of the main agreement.

8.2 If another agreement between the Controller and the Processor contains provisions that deviate from the provisions of this agreement, the provisions of this agreement prevail.

8.3 Amendments to this agreement are only valid if they have been agreed in writing between the parties.

8.4 This agreement enters into force at the time the main agreement enters into force and has a term that is equal to that of the main agreement. This agreement cannot be terminated prematurely.

Signed in duplicate:

Processor:	Crowdtech
Name:	Daniel Nokes
Function:	Managing Director
Date:	[DATE]

Signature

Controller:
Name:
Function:
Date:

Signature

Annex 1: independent use of Crowdtech Insights by Controller

In this agreement, "actions" are understood to mean every act or collection of acts relating to personal information as part of Controller's remit to the Processor, in any case including:

- Provision of the Crowdtech Research Platform as a SaaS service, on the platform of the Processor.
- Storage of (personal) data that Controller saves via the SaaS service, on the platform of the Processor.
- Provision of technical support to Controller for the SaaS service on the platform of the Processor.
- Creation of back-ups of the (personal) data of Controller that have been saved via the SaaS service on the platform of the Processor.

Subprocessors

Crowdtech engages the following subprocessors:

Subprocessor	Services
1. Microsoft Ireland Operations Ltd. Atrium Block B Carmenhall Road Sandyford Industrial Estate, Dublin 18 Ireland	Microsoft provides software that processes research data (such as Excel) and storage space for the files (OneDrive). The data of the users of Crowdtech Insights is stored in Azure. Crowdtech uses Azure AI Language for its AI functionality Cai to detect and remove personally identifiable information (PII) before the text is sent to Mistral's LLM.
2. Spotler Papendorpseweg 91 3528 BJ Utrecht CoC: 09103500 LEI: 724500PKRXW8AGOPUH50	Spotler handles the sending of emails from Crowdtech Insights (SMTP provider). They only process the data required to send the email, such as the email address and, if applicable, details like salutation and (last) name.
3. Cyberlab Philitelaan 57 5617 AK Eindhoven CoC: 52474925	Cyberlab provides our SIEM system (Rapid7), including SOC support. Through this, they have visibility into incoming IP addresses.

Optional subprocessors

The following subprocessors are only applicable if the specific add-on is purchased:

Subprocessor	Services
1. Embite Kleterstraat 11a 3862 CA Nijkerk The Netherlands CoC: 60683988	Embite provides the Crowdtech Personal Insight add-on, which enables survey responses to be shared with individual respondents. When a personal report is accessed, survey responses and any additional enrichment data are temporarily processed through Embite's servers. This data is used exclusively to generate the report and is not permanently stored or cached. The original research data remains stored at Crowdtech. Embite does not have access to respondents' email addresses or to the Crowdtech Survey research environment. Embite's application is hosted on a dedicated Virtual Private Server (VPS) at Hetzner in Germany.

Data center

Crowdtech's data is hosted at Equinix's AM5 and AM8 data centres in Amsterdam, the Netherlands. Equinix provides rack space for Crowdtech's own servers, on which the Crowdtech Insights platform runs. As Equinix does not have access to the data, it is not considered a subprocessor.

Equinix B.V. Rembrandt Tower Amstelplein 1 1096 HA Amsterdam CoC: 63332248

Annex 2: report of data breach

If the Contractor or Client suspects or has become aware of a data breach as referred to in the GDPR, one party will immediately inform the other party - but no later than within 24 hours - of the other party. When reporting, the reporter is requested to provide the information below. The notification must also be sent to so@crowdtech.com

1. **Contact person(s)**
    a. name
    b. Position
    c. Mobile phnoe
    d. E-mail address
2. **Report**
    a. Date and time of the report
    b. Resume
3. **Size**
    a. Minimum number of people involved
    b. Maximum number of people involved
4. **Infringement**
    a. Date, time and / or period of the infringement
    b. Date and time of discovery of infringement
    c. The nature of the infringement (read / copy / change / delete / theft / etc.)
5. **Personal data**
    a. Type of data, for example:
        i. Name, address, city
        ii. Gender, date of birth and / or age
        iii. Phone numbers
        iv. E-mail addresses or other addresses for electronic communication
        v. Access or identification data
        vi. Financial details
        vii. Citizen service numbers
        viii. (Copies of) proof of identity
        ix. Special personal data
    b. Consequences of the infringement for the parties involved, for example:
        i. Stigmatization or exclusion
        ii. Damage to health
        iii. Exposure to (identity) fraud
        iv. Exposure to spam or phishing
6. **Measures**
    a. The technical and organizational measures taken by the reporter
7. **Encryption**
    a. Is the data in its entirety or partially encrypted, hashed or otherwise made incomprehensible or inaccessible to unauthorized persons
    b. How have the data been made incomprehensible or inaccessible?
8. **Completion**
    a. Is the report complete, or will additional information follow?