Undersigned:

This Data Processing Agreement is incorporated into the agreement(s) between CrowdSense and Customer and applicable for all current clients unless it is replaced by a valid Customer Processing Agreement

Taking into account that:

a) CrowdSense owns PublicSonar technology that enables users to collect and analyze open source reporting for real-time detection, early warning, and environmental imagery creation and maintenance.
b) The Controller wishes to use CrowdSense's PublicSonar and has concluded an agreement with the Processor for this purpose.
c) Processor is processing, in the context of the implementation of the Agreement, (personal) data of users of open sources and possibly others, in PublicSonar;
d) Controller also stores other important and sensitive information of Controller in PublicSonar;
e) The Processor undertakes careful processing, in the context of those activities;
f) The Controller has designated the purpose and means for this as set out in the Agreement and accompanying documents;
g) The Processor develops and manages the technology and files and the Processor thereby has access to and can influence the use of that data;
h) Processor and Controller are prepared to enter into obligations regarding information security and other aspects of the Personal Data Protection Act and the resulting standards frameworks;
i) Parties want to document agreements regarding the processing and security of this (personal) data in accordance with Article 14 paragraph 5 of the Wbp in this Processor Agreement;
j) The provisions of the agreement apply to this Processor Agreement insofar as this Processor Agreement does not deviate from it.

Declare to have agreed as follows:

Article 1. DEFINITIONS

1.1 *Personal data: any information concerning or traceable to an identified or identifiable natural person;*
1.2 *Data: all other data (data) not being personal data;*
1.3 *Processing: any action or set of actions with regard to personal data, including in any case collecting, recording, organizing, storing, editing, changing, retrieving, consulting, using, providing by means of forwarding, dissemination or any other form of making available, bringing together, linking, as well as shielding, erasing or destroying data, as referred to in Article 1 under b of the Personal Data Protection Act (Wbp).*
1.4 *Data subject: the person to whom the personal data relates.*
1.5 *PublicSonar: the service offered by the Supplier that enables users of the Controller to independently consult open sources with the aim of detection, early warning and the construction and maintenance of situational awareness by processing potentially relevant messages in real time.*
1.6 *Processor Agreement: this agreement between Responsible Party and Processor;*

1.7 *Agreement: Agreed agreements and conditions between the Processor and the Controller relating to the technology and service(s) provided by the Processor to the Controller*
1.8 *Wbp: Personal Data Protection Act.*
1.9 *Wpg: Police Data Act*

Article 2. Purposes of processing

2.1 Under the terms of this Processor Agreement, the Processor undertakes to 'process' personal data on behalf of the Controller or to enable processing by the Controller. Processing will only take place within the scope of the purpose determined by the Controller.
2.2 The Processor will not process the personal data for any purpose other than as determined by the Controller. The Controller will inform the Processor of the processing purposes insofar as these have not already been mentioned in the License Agreement or this Processor Agreement.
2.3 In this context, processing by the Processor means the automatic collection and partial analysis of messages from open sources at the request of the Controller, annotating messages from open sources and storing messages from open sources and other data from the Controller. Other forms of processing in the context of the Agreement are carried out by the Controller.
2.4 The Processor has no control over the personal data made available. For example, he does not make decisions about receipt and use of the data, the provision to third parties and the duration of the storage of data. The control over the personal data provided under this agreement will never rest with the Processor.
2.5 The personal data to be processed on the instructions of the Controller remain the property of the Controller and/or the relevant data subject.

Article 3. Responsibilities

3.1 With regard to the purposes and processing referred to in Article 2, the parties mutually undertake to act in accordance with the Personal Data Protection Act or any laws and regulations explicitly indicated by the Controller.
3.2 It is the responsibility of the Controller to ensure that the processing of personal data falls under one of the exemptions under the Personal Data Protection Act, and that no notification to the supervisory authority is therefore required.
3.3 Processor is solely responsible for the processing of personal data under this Processor Agreement as referred to in 2.3. The Processor is expressly not responsible for the other processing of personal data, including in any case but not limited to the collection of personal data by the Controller, processing for purposes that have not been reported to the Processor by the Controller, processing by third parties and/or for other purposes.
3.4 The Controller guarantees that the content, the use and the order to process the personal data as referred to in this Agreement are not unlawful and do not infringe any rights of third parties.

Article 4. Obligations Processor

4.1 Processor undertakes to take measures to guarantee the confidentiality, integrity and availability of the information provision.
4.2 Processor works in accordance with ISO 27001.

4.3 The Processor will inform the Controller, at its first request, about these measures it has taken and the measures regarding its obligations under this Processor Agreement.

4.4 The Processor will limit the distribution of personal data or other data of the Controller necessary for the functioning of PublicSonar and for the purposes and processing referred to in Article 2 to a minimum.

4.5 The obligations of the Processor arising from this Processor Agreement also apply to those who process personal data under the authority of the Processor, including but not limited to employees, in the broadest sense of the word.

Article 5. Security

5.1 The Processor takes all appropriate technical and organizational measures to secure personal data that is processed for the benefit of the Controller and to keep them secure against loss or against any form of unlawful processing (such as unauthorized access, damage, alteration or provision of personal data).

5.2 The Processor has in any case taken the following security measures:

a) Encryption (encryption) of digital files with personal data
b) Security of network connections via Secure Socket Layer (SSL) technology
c) Intelligent application firewall
d) Intrusion detection as an extra layer of protection against unauthorized access
e) Management activities take place via an encrypted VPN connection (L2TP--PSK) where the 'single point of access' principle is applied

5.3 The Processor does not guarantee that the security is effective under all circumstances. If an expressly described security is missing in the Processor Agreement, the Processor will make every effort to ensure that the security meets a level that is not unreasonable in view of the state of the art, the sensitivity of the personal data and the costs associated with taking the security into account.

Article 6. Reporting obligation

6.1 The Data Protection Officer (dpo@publicsonar.com), on behalf of the Processor, will inform the Customer as soon as possible - but no later than 24 hours after the first discovery - of all security breaches as well as other incidents that must be reported by law to a supervisor or data subject, without prejudice to the obligation to undo or limit the consequences of such breaches and incidents as quickly as possible.

6.2 The notification from the Processor to the Controller in any case includes reporting the fact that there has been a leak, as well as:

a) What the (alleged) cause of the leak is
b) What the possible (as yet known and/or expected) impact of the leak is
c) What are the possible solutions

6.3 The Controller is responsible for reporting to the supervisor(s) and any other authorities that the Controller must inform.

6.4 The Processor will provide all necessary cooperation in providing, if necessary, in the shortest possible term, additional additional information to the supervisor(s) and/or data subject(s).

6.5 The Processor keeps a detailed log of all security breaches, as well as the measures taken in response to such breaches, and provides access to this at the first request of the Controller.

Article 7. Handling request

7.1 Data subjects with requests regarding reporting of open sources directed to the Processor are referred to the Controller

7.2 Requests from data suppliers are processed and handled by the Processor, unless it is explicitly the responsibility of the Controller.

7.3 Handling of requests by the Processor towards suppliers never concerns Controller-specific information.

Article 8. Secrecy and Confidentiality

8.1 The Processor, including its employees, has a duty of confidentiality towards third parties on all personal data that the Controller collects in the context of this Processor Agreement. The Processor will not use this information for any other purpose than for which the Controller has obtained it.

8.2 This duty of confidentiality does not apply insofar as the Controller has given explicit permission to provide the information to third parties.

8.3 If the Processor is required to provide data on the basis of a legal obligation, the Processor will verify the basis of the request and the identity of the requester and the Processor will inform the Controller immediately prior to the provision. Unless legal provisions prohibit this.

Article 9 Audit

9.1 The Controller is permitted to carry out an audit (or have it carried out) on the security measures (both technical and organisational) of the Processor. Any form of audit, including pen tests, must be announced to the Processor in writing by the Controller in advance. The costs for conducting the audit are borne by the Controller.

9.2 The Controller is at all times entitled to check the processing of personal data (or have it checked). The Processor is obliged to admit the Controller or inspection body on the instructions of the Controller and to cooperate so that the inspection can actually be carried out.

9.3 The Controller will report in advance in which period these will be carried out. The costs of audits carried out at the initiative of the Controller are for the account of the Controller.

9.4 Processor is entitled to integral reporting of the outcome of the audit. The Processor will inform the Controller on request of the manner in which the Processor uses the results.

Article 10. Duration and Termination

10.1 This agreement takes effect at the time of signing and continues for the duration of the agreed cooperation, unless it is replaced by another valid processing agreement from Customer.

10.2 As soon as the Processor Agreement has been terminated, for any reason and in any way whatsoever, the Processor will remove and/or destroy all personal data and other data of the Processing Officer present and any copies thereof within two months after the end of the agreement.

Article 11. Liability

11.1 If the Processor fails to fulfill the obligation under this agreement can give him notice of default. However, the processor is immediately in default if the fulfillment of the relevant obligation is already permanently impossible, other than due to force

majeure within the agreed term. Notice of default is given in writing, whereby the Processor is granted a reasonable period of time to still fulfill its obligations. This term is a strict deadline. If compliance is not met within this period, the Processor is in default.

11.2 Processor is liable on the basis of the provisions of Article 49 of the Wbp, including damage or disadvantage resulting from non-compliance with this agreement

11.3 The Processor indemnifies the Controller against damage or disadvantage insofar as this arises from the activities of the Processor.

Article 12. Applicable law and dispute resolution

12.1 The Processing Agreement and its implementation are governed by Dutch law

12.2 All disputes that may arise between the Parties in connection with the Processor Agreement will be submitted to the competent court for the district in which the Processor is located.

Article 13. Signed version

13.1 In the case a Customer needs a signed version of this Processing Agreement, please reach out to the Data Protection Officer via dpa@publicsonar.com