Data Processor Agreement

25 MAY 2018

INTRODUCTION

For its Services, Meronimi crawls websites including social and web media platforms. In this context, Meronimi decides what data it collects and how and why this data is used in connection with the IntelligenceHub Platform. Our data collection and processing are not specific to any particular customer and is therefore not considered as being processed on the instructions of any customer.

Consequently for the data it processes independently of any customer instruction, Meronimi considers itself a *data controller* under the GDPR for personal data contained on its platform and undertakes that the features of the platform are compliant with GDPR principles.

For personal data input by customer or specific requests made by customer on the platform, Meronimi technically acts as *data processor* for the customer as it follows the instructions of the customer to input and process the data, of which some may be personal data.

As a data processor, Meronimi commits to appropriate technical and organizational security measures as required under the GDPR. Those measures are in place to protect customer data as set out in the below data processor agreement between Customer and Meronimi.

DATA PROCESSOR AGREEMENT

Controller and Processor have entered into a services agreement ("Terms of Service") regarding the provision of supplier monitoring services ("Services") by Processor to Controller.

Controller is the Customer of Meronimi, including Customer's Affiliates where relevant, as set out in the Terms of Service. Processor is the Meronimi entity contracting with Customer in the Terms of Service.

In order to provide the Services under the Terms of Service, Controller requires Processor to process, on its behalf, the personal data provided or input by customer or specific requests made by customer on the platform ("Customer Personal Data").

Controller has elected to appoint Processor to provide the Services and has determined the purposes and the essential means of the data processing to be carried out by Processor on behalf of Controller.

The Parties have decided to enter into this Data Processor Agreement ("DPA"), effective as of 25 May 2018, to set out their rights and obligations in relation to the processing of Personal Data by Processor in accordance with Article 28 of Regulation (EU) 2016/679 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 (hereinafter the "GDPR").

ARTICLE 1 – SUBJECT MATTER OF THE DPA AND DEFINITIONS

1.1. This DPA defines the respective rights and obligations of each Party in relation to the processing of Personal Data carried out by Processor on behalf of Controller.

1.2. Except as otherwise expressly provided or unless the context otherwise requires, the terms used in this DPA shall have the meaning attributed to them in the GDPR, in this DPA as well as in the Terms of Service.

ARTICLE 2 – DESCRIPTION OF THE DATA PROCESSING UNDERTAKEN BY PROCESSOR

2.1. Processor is instructed by Controller to process Customer Personal Data within the framework of the Services provided by Processor under the Terms of Service.

The categories of Personal Data and of data subjects concerned by the data processing are set out in Attachment 1.

2.2. Processor shall process the Personal Data only in accordance with the instructions of Controller. The instructions are provided within the framework of the Terms of Service between the parties.

2.3. Controller undertakes to confirm, in writing, all instructions given to Processor in relation to the processing of Personal Data, by the following means:

- the order form for the Services
- the written instructions given to the Support or Account team
- the confirmation of the Use Case by Controller through the execution of an order form or any equivalent contractual document, including by exchange of e-mails
- the set up and configuration of the IntelligenceHub Platform
- the specific searches made by Controller in the IntelligenceHub Platform

2.4. Processor undertakes to process Personal Data only as instructed by Controller through the provision of the Services.

ARTICLE 3 – DUTIES OF THE PARTIES

3.1. Controller has determined the purpose(s) of the data processing before engaging the Services of Processor. The nature of the data processing and the purpose(s) of the data processing are described in Attachment 1.

3.2. Controller has also defined the essential means of data processing, including:

- the Personal Data to be collected in relation to the specific searches of the Customer
- the categories of Personal Data to be processed on its behalf by determining the social media channels and other media types to be searched
- the identity of persons authorized to access Personal Data in the IntelligenceHub Platform
- the access rights of such users of the IntelligenceHub Platform
- the retention period of Personal Data.

The essential means of data processing as determined by Controller may be modified at any time by addressing a request, in writing, to the Support or Account team of Processor or by changing the appropriate settings in the IntelligenceHub Platform.

3.3. In regards to the purpose(s) of data processing, Controller represents and warrants that it shall not use or process, or request Processor to process, the Personal Data in any manner which infringes upon the rules laid out in the GDPR or in any other applicable law and that it will use relevant procedures and safeguards as required to protect such Personal Data.

3.4. Without prejudice to Controller's duties to ensure the lawfulness of data processing, Processor shall use its best commercially reasonable efforts to inform Controller if the latter's instructions may be deemed to infringe upon the provisions of the GDPR, including but not limited to taking into account the information made available by Controller. If the instructions of Controller are deemed unlawful by Processor, the latter is entitled to suspend the execution of such instructions until the lawfulness of such instructions is verified and confirmed in writing by Controller and, at the request of Processor, by outside counsel of Controller.

3.5. Taking into account the state of the art, the costs of implementation, the nature and the risks of Personal Data processing as well as appropriate industry standards, Processor undertakes to use its commercially reasonable efforts to implement appropriate technical and organizational measures in order to safeguard the protection of Personal Data and the processing of such Personal Data.

3.6. During the course of the DPA, Controller may request Processor to make an offer for the implementation of additional technical or organizational measures. In such case, Processor shall inform Controller, at its discretion, if such additional measures are feasible from a technical and organizational standpoint and, if it deems such measures feasible, Processor shall inform Controller of the costs involved with the implementation of such measures. If the offer is accepted by Controller, Processor shall implement the additional measures in accordance with the conditions agreed upon by the Parties.

3.7. Processor undertakes to monitor the adequacy of the protection of the technical and organizational measures at regular intervals.

3.8. Processor undertakes to process Personal Data as instructed by Controller, except if Processor is required to do so by law or in the context of a potential dispute concerning, for instance, the delivery of the Services to Controller.

ARTICLE 4 – RIGHTS OF THE DATA SUBJECTS

4.1. If a data subject addresses a request to Controller regarding data processing performed by Processor under the scope of this DPA, Controller shall redirect such request to Processor within a reasonable timeframe which must not exceed seven (7) business days. Processor shall use its commercially reasonable efforts to comply with such request within a reasonable timeframe.

ARTICLE 5 – PERSONAL DATA BREACH

5.1. Processor undertakes to notify Controller of a Personal Data breach compromising Controller's Personal Data without undue delay, and if possible within twenty-four (24) hours, after becoming aware of said breach.

5.2. In the context of the Personal Data breach notification to Controller, Processor shall provide the following information:

- description of the nature of the Personal Data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned
- description of the likely consequences of the Personal Data breach
- description of measures taken or proposed to be taken in order to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects
- the contact details of the Data Protection Officer or other contact person who can provide any additional information required

Where, and in so far as, it is not possible for Processor to provide the information at the same time, the information shall be provided to Controller in phases without undue further delay.

5.3. Controller undertakes to notify the competent data protection supervisory authority of the Personal Data breach without undue delay and, if applicable, to the data subjects concerned if such notification is required under the GDPR or any other applicable legislation. Controller shall inform Processor prior to any such notification taking place. Controller shall, to the maximum extent possible, take into account the observations presented by Processor in relation to the proposed draft of the Personal Data breach notification.

5.4. Upon request and written instruction of Controller, Processor may accept to handle, on behalf of Controller, the notification of a Personal Data breach to the competent data protection supervisory authority and to the data subjects concerned, as the case may be.

ARTICLE 6 – ASSISTANCE AND AUDIT

6.1. Processor shall use reasonable efforts to assist Controller to comply with the latter's duties in regards to data protection impact assessments required under the GDPR and/or by any competent authority and any related prior consultation processes with the relevant data protection supervisory authority.

6.2. Processor shall provide all reasonably required information and documents to Controller in order to prove compliance with its duties under this DPA. In this context and in order to confirm compliance, Controller shall be entitled to conduct an audit of the data processing undertaken by Processor on behalf of Controller.

Controller and Processor shall agree in writing on the reasonable conditions under which such audit may be carried out. In any case, any audit will have to comply with Processor's reasonable requirements, such as in terms of security, confidentiality, and the protection of intellectual property rights and business secrets. In particular, if the audit is carried out by a third party on behalf of Controller, such third party may not be a competitor of Processor and must sign a non-disclosure and confidentiality agreement, without prejudice to other conditions that may reasonably be imposed by Processor.

Any audit may not unduly interfere with the normal conduct of Processor's business. Controller will, in principle, provide at least two weeks' prior written notice of an audit request.

The findings of the audit will be evaluated and discussed by the Parties. As the case may be, the resulting additional measures agreed upon by the Parties shall be implemented by the relevant Party as soon as reasonably possible.

6.3. To the extent required and if Controller does not have direct access to the relevant information, Processor shall also endeavor to assist Controller to comply with the latter's duty to respond to legitimate requests of data subjects relating to their rights under the GDPR.

6.4. Reasonable costs relating to the audit and any other services rendered by Processor to assist Controller may be charged by Processor to Controller. Controller shall bear the costs of any external auditor appointed by it to perform an audit.

6.5. To the extent permitted, Controller may also request Processor to audit a Sub-Processor by complying with such Sub-Processor's reasonable requirements. Controller shall bear any reasonable costs charged by Processor and such Sub-Processor regarding such audit.

6.6. To the extent permitted, Controller undertakes to inform Processor without undue delay of any audits, inspections, or other measures taken by the data protection supervisory authority or by any other competent authority in relation to the processing of Personal Data relating to this DPA. Such notification shall be made free of charge and shall contain the essential elements describing the subject matter of the relevant authority's action. The Parties shall cooperate in good faith in responding to such enquiries.

ARTICLE 7 - TRANSFERS OF PERSONAL DATA OUTSIDE OF THE EU

7.1. Processor shall not transfer any Personal Data outside of the European Union ("EU"), unless instructed to do so by Controller or unless Personal Data is transferred to Sub-Processors approved by Controller in accordance with Article 9 of this DPA.

7.2. If Controller instructs Processor to export Personal Data outside of the EU, it shall ensure that such export complies with the conditions set out in the GDPR and in any other applicable data protection legislation.

7.3. If Processor is required to transfer Personal Data outside of the EU by virtue of law, by virtue of the order of a court or of any other competent authority, Processor shall endeavor to inform Controller prior to such transfer, except if such information is prohibited by law.

ARTICLE 8 – REPRESENTATIONS AND WARRANTIES, LIABILITY

8.1. Each Party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability section as agreed upon in the Terms of Service and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Terms of Service and all data processor agreements taken together.

8.2 Processor shall be solely responsible to use its best commercially reasonable efforts for the processing of Personal Data in accordance with this DPA. Even though Processor cannot guarantee that the technical and organizational security measures shall be effective under all circumstances, Processor will use its commercially reasonable efforts to ensure that the level of protection of Personal Data and of the processing of Personal Data is appropriate, as set out in Article 3 of this DPA.

8.3. Controller is responsible for ensuring that the data processing it instructs Processor to undertake is lawful and that it pursues legitimate and proportionate purposes. Moreover, Processor shall not be liable for the processing of Personal Data undertaken by Controller itself or by third parties acting under Controller's instructions.

ARTICLE 9 – SUBPROCESSING

9.1. As permitted by Article 28 3° of the GDPR, Controller hereby generally authorizes Processor to engage sub-processors for specific data processing operations ("Sub-Processor(s)") as deemed appropriate by Processor in the provision of the Services, without the prior specific approval of Controller being required to the extent the new Sub-Processor provides a level of protection for the Personal Data processing that is materially similar to the level of protection previously provided.

9.2. In case of engagement or replacement of a Sub-Processor, Processor shall need only to inform Controller in writing prior to any envisaged appointment or replacement of a Sub-Processor. This prior information notice shall contain a description of the nature of the Personal Data processing activities concerned as well as the designation of the Sub-Processor. Controller shall be entitled to formulate written objections to the appointment or replacement of a Sub-Processor within thirty (30) days of the receipt of the notice of information if it has a legitimate, material reason to object. If Controller objects to the use of the Sub-processor concerned, Processor shall have the right to cure the objection through one of the following options: (i) Processor will abort its plans to use the Sub- processor with regard to Controller's Personal Data; or (ii) Processor will take the corrective steps requested by Controller in its objection (which remove Controller's objection) and proceed to use the Sub-Processor with regard to Controller's Personal Data; or (iii) Processor may cease to provide or Controller may agree not to use (temporarily or permanently) the particular aspect of the service that would involve use of the Sub-Processor with regard to Controller's Personal Data.

In the absence of such objection, Processor shall be deemed to be fully entitled to appoint such Sub- Processor.

9.3. Controller acknowledges the Sub-Processors listed in Attachment 2 process Personal Data in the provision of the Services and agrees to such appointment by entering into this DPA.

9.4. The Parties agree that the term 'Sub-Processor(s)' refers only to service providers which provide data processing services in a capacity of processor. They further agree that this term shall not apply to the contractual service providers which provide ancillary services and which Processor may have recourse to in the provision of the Services under the Terms of Service, such as, without limitation, telecommunication services, postal services, office maintenance services, etc.

ARTICLE 10 - CONFIDENTIALITY

10.1. Processor confirms that all personnel who are processing Personal Data are subject to a confidentiality duty.

ARTICLE 11 - DURATION AND TERMINATION

11.1. This DPA is entered into for the duration of the Terms of Service. In the absence of a specified duration, this DPA shall be in force for the duration of the relationship between the Parties.

11.2. This DPA may be terminated by either Party, together with the Terms of Service, by giving appropriate notice for the termination of both agreements. In case of expiry or termination of the Terms of Service for any reason whatsoever, this DPA shall automatically terminate on the same date, and vice-versa.

11.3. After the provision of the Services related to Personal Data processing have come to an end, the Parties agree that Processor shall in principle delete Controller's Personal Data as soon as is reasonably possible and shall provide, upon Controller's request, a written confirmation of such deletion, the Personal Data processed on behalf of Controller. Alternatively, upon separate written agreement between the Parties, and in any case prior the expiry or termination date of the Terms of Service, Controller may request a copy of its Personal Data against payment of the reasonable costs incurred by Processor to render such service. It is understood by the Parties that the copy of the Personal Data may only contain data which Processor is legally and contractually permitted to provide, taking into account in particular the contractual provisions of third party content providers, social networks' terms of service and copyright laws.

Notwithstanding the foregoing, Processor shall be entitled to retain a copy of the Personal Data as long as required for evidentiary or statutory record retention purposes.

ARTICLE 12 – MISCELLANEOUS

12.1. This DPA together with its Attachments supersedes any and all other prior or contemporaneous understandings and agreements, either oral or in writing, between the Parties with respect to the subject matter hereof and constitutes the sole and only agreement between the Parties with respect to its subject matter. In particular, the provisions of the general terms and conditions of Processor relating to data protection and the storage of data are void and shall be replaced by the provisions of this DPA and its Attachments.

12.2. This DPA may be amended only by a written instrument which specifically refers to this DPA. Processor shall be entitled to amend this DPA by providing thirty (30) days' prior written notice to Controller.

12.3. Each Party shall give all notices and communications to the other Party in writing including by e-mail.

12.4. This Agreement shall be governed by English law.

ATTACHMENT 1

NATURE AND PURPOSES OF THE DATA PROCESSING

The nature of data processing consists of collecting, sorting, saving, transferring, restricting and deleting Personal Data in the context of Controller's use of the IntelligenceHub Platform and Services.

The purposes of the data processing concern:

A – Controller's users' access to the IntelligenceHub Platform and Services based on such Controller's users' personal data provided by Controller to Processor for the purpose of defining Controller's users' accesses the IntelligenceHub Platform (processed data includes identification, authentication, login, access and audit trial data)

B – Controller's supplier monitoring results processed on the basis of Controller's specific searches and, if applicable, the personal data input by the Customer in the IntelligenceHub Platform for the purposes of Controller's 360° internet media review, including supplier monitoring, social media and web media listening and analytics, customer care and support

CATEGORIES OF PERSONAL DATA AND OF DATA SUBJECTS

A – Data provided by the Controller to the Processor relating to users appointed by the Controller to access to the IntelligenceHub Platform

Data type	Personal Data	Purpose of use	Non-Personal Data
User settings	IP address, cookies	Keep login session, analytics	
IntelligenceHub service settings	First and last name, email address, role of employee	Politeness, security, authentication, subscription to marketing communications (possible to unsubscribe)	Company name, Industry sector, Field of expertise, Access right level, Meronimi settings (e.g. topics, queries), Time zone
IntelligenceHub service alerts and reports	Recipient email address	Necessary to establish communication	Meronimi stores a history of the last alerts/reports sent to Customers
Exchange of email communication and support requests	Sender email addresses (or telephone numbers)	Necessary to establish communication	Email server IP addresses
	Identification elements typically present in email footer/signatures	Optional	Description of the issue, requests
Webserver log files	IP address, username	Incident investigation (typically abuse), capacity planning	Resource accessed, timestamp
Meronimi service billing information	First and last name, email address, IP address when subscription was signed as part of signing proof (electronic signature), telephone number, history of bills	Compliance with legal and corporate governance obligations and good practice	Detailed information about the Customer (VAT information) service provided (start and end dates, fees, payment dates), complete billing address

B – Author data related to the Controller's monitoring of suppliers via the publications made in the internet, including social media users.

Results provided by the IntelligenceHub Platform or API to the Controller to match Controller's Queries in the IntelligenceHub Platform. Processor only processes information which has been made public by the data subject himself, such as:

- Identification data (name, username, user id, geographical area)
- Personal characteristics (age, gender, status)
- Consumer habits
- Hobbies and interests
- Professional and educational background
- Pictures and videos
- Any other supplier monitoring related information published by the data subject on a public Internet website or on a third-party platform that provides the Processor with data

ATTACHMENT 2

LIST OF SUB-PROCESSORS

Recipient	Country	Purpose/Activity	Guarantees/Notes
Trendiction SA	European Union (Luxembourg)	Hosting of IntelligenceHub Platform Search, crawling, indexing of public data for supplier monitoring purposes	DPA under GDPR Art 28
Campaign Monitor	United States	Sending of email alerts with information from or about the IntelligenceHub Platform	DPA under GDPR Art 28

RELEVANT ANCILLARY SUB-PROCESSORS

Recipient	Country	Purpose/Activity	Guarantees/Notes
Microsoft	United States	Email provider (Outlook) and file hosting (OneDrive)	DPA under GDPR Art 28 Privacy Shield certification
Freshworks	United States	Management of support requests sent by the customer	DPA under GDPR Art 28 Privacy Shield certification