**DATA PROCESSING AGREEMENT**

**BETWEEN**

**Opinum NV**, incorporated and registered under Belgian law, with company number 0561.807.172 and registered office at Rue Emile Francqui 9 à 1435 Mont-Saint-Guibert, Belgium (**Processor**)

acting in the capacity of Processor

**AND**

**Client**, any company and legal entity, natural or legal person acting on its behalf, in a non-private on its behalf, other than in a private capacity (B2B), which has registered for the use of the Services in accordance with the Terms of Sale each a **Party** and collectively the **Parties**.

**This DPA is an integral part of Opinum’s terms of sale. Adherence to these terms therefore implies acceptance by the Customer of the following provisions regarding to the processing of personal data.**

**AGREED TERMS**

# Definitions and Interpretation

The following definitions and rules of interpretation apply in this DPA.

## Definitions:

**Business Purposes** means the services described in the Master Agreement and/or any other purpose specifically identified in Annex A.

**Data Protection Legislation** means the GDPR and the applicable implementation legislation under Belgian law.

**GDPR** means Regulation (EU) 2016/679 of the European Parliament and of 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 (General Data Protection Regulation).

**Controller**, **Data Protection Impact Assessment**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **process(ing**) and **Processor** shall have the same meaning as in the GDPR.

## This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement.

## In the case of conflict or ambiguity between:

### any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail; and

### any of the provisions of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail.

# Personal Data types and processing purposes

## The Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Processor. The Controller shall inform the Processor of any additional national and/or sector-specific mandatory legislation that applies to the processing by the Processor as a result of the processing by the Controller.

## Annex A describes the nature and purpose of processing, the retention term(s) and the Personal Data categories and Data Subject types in respect of which the Processor may process to fulfil the Business Purposes.

# Processor's obligations

## The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Controller's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. The Processor must promptly notify the Controller if, in its opinion, the Controller's instruction would not comply with the Data Protection Legislation.

## The Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Controller or this DPA specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Processor to process or disclose Personal Data, the Processor must first inform the Controller of the legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

## The Processor will reasonably assist the Controller with meeting the Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, Data Protection Impact Assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

# Processor's employees

## The Processor will ensure that all employees:

### are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data; and

### are aware of the Processor's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

# Security

## The Processor must implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data, as further described in Annex B.

## The Processor must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

### the pseudonymisation and encryption of personal data;

### the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

### the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

### a process for regularly testing, assessing and evaluating the effectiveness of security measures.

# Personal Data Breach

## The Processor will without undue delay and in any case within 24 hours notify the Controller in writing if it becomes aware of a Personal Data Breach.

## Where the Processor becomes aware of a Personal Data Breach, it shall, without undue delay, also provide the Controller in writing with the following information:

### description of the nature thereof, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

### the likely consequences; and

### description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

## Immediately following a Personal Data Breach, the Parties will co-ordinate with each other to investigate the matter. The Processor will reasonably co-operate with the Controller in the Controller's handling of the matter, including:

### assisting with any investigation;

### taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach.

## The Processor will not inform any third party of any Personal Data Breach without first obtaining the Controller's prior written consent, except when required to do so by law.

# Cross-border transfers of Personal Data

## The Processor (or any Sub-Processor) shall not transfer or otherwise process Personal Data outside the European Economic Area (**EEA**) without obtaining the Controller's prior written consent.

## Such consent of Controller is not required when the transfer of Personal Data to countries outside the EEA is mandatory under EU or EU member state provisions.

# Subcontractors

## The Processor may only authorise a third party (**Sub-Processor**) to process the Personal Data if:

### the Controller is provided with an opportunity to object to the appointment of each Sub-Processor within 14 days after the Processor has notified in writing the Controller of its intention to appoint such Sub-Processor, it being understood that the Controller shall only object to such appointment in writing and on reasonable and evidenced grounds; and

### the Processor enters into a written contract with the Sub-Processor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Controller's written request, provides the Controller with copies of such contracts.

## Those Sub-Processors approved at the commencement of this DPA are as set out in Annex A. The Processor must list all approved subcontractors in Annex A and include any Sub-Processor's name, location and contact information for the person responsible for data protection compliance.

## Without prejudice to Clause 13.1, the Processor shall remain fully liable to the Controller for any failure by a Sub-Processor to fulfil its obligations in relation to the processing of the Personal Data.

# Complaints, Data Subject requests and third-party rights

## The Processor must take such technical and organisational measures as agreed in writing between the Parties, and promptly provide such information to the Controller as the Controller may reasonably require, to enable the Controller to comply with:

### the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

### information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

## The Processor must notify the Controller immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either Party's compliance with the Data Protection Legislation.

## The Processor must notify the Controller within 5 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

## The Processor will reasonably cooperate with, and assist, the Controller in responding to any complaint, notice, communication or Data Subject request.

## The Processor must not disclose the Personal Data to any Data Subject or to a third party other than at the Controller's request or instruction, as provided for in this DPA or as required by law.

# Term and termination

## This DPA will remain in full force and effect so long as:

### the Master Agreement remains in effect; or

### the Processor retains any Personal Data related to the Master Agreement in its possession or control (**Term**).

## Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement (including, but not limited to, Clause 13.1) will remain in full force and effect.

# Data return and destruction

## On termination of the Master Agreement for any reason or expiry of its term, the Processor will securely delete or destroy or, if directed in writing by the Controller, return and not retain, all or any Personal Data related to this DPA in its possession or control.

## If any law, regulation, or government or regulatory body requires the Processor to retain any documents or materials that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

## The Processor will certify in writing that it has destroyed the Personal Data within 14 days after it completes the destruction.

# Audit

## The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations under this DPA and the Data Protection Legislation and allow the Controller and its authorized auditors to perform audits regarding the compliance by the Processor with its obligations under this DPA and the Data Protection Legislation.

## Any such audit may not take place more than once every contract year, shall be at the sole expense of the Controller and shall be subject to the Controller providing the Processor with at least thirty (30) days prior written notice of its intention to perform an audit. The audit shall take place during the normal business hours and shall not unreasonably interfere with the Processor’s business activities. The Processor shall have the right to require Controller and any third-party auditor to enter into a non-disclosure agreement prior to performing the audit.

# Miscellaneous

## To the extent permitted under applicable law, any limitations and/or exclusions of liability in the Master Agreement are applicable to this DPA.

## If at any time during the Term, one of the provisions of this DPA, is determined to be or to have become invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions of the DPA shall not in any way be affected or impaired. The Parties shall negotiate in good faith to replace such invalid, illegal or unenforceable provision with a valid, legal and enforceable provision the effect of which comes as close as possible to that of the invalid, illegal or unenforceable provision.

## This DPA will be governed by, and construed in accordance with, the laws applicable to the Master Agreement. The same court as stated in the Master Agreement shall have exclusive jurisdiction for any disputes arising from or in connection with this DPA.

**Annexes:**

- ANNEX A Description of processing and contact information

- ANNEX B Technical and organisational measures

**ANNEXE A Description of processing and contact information**

**Other business purposes and specific processing instructions**

**Nature of the treatment**

|  |  |
| --- | --- |
| collect  registration  organisation  structuration  conservation  adaptation or modification  extraction  consultation | use  communication by transmission, broadcast or any other form of making available  reconciliation or interconnection  limitation, deletion or destruction of data (whether or not by automated means)  Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Catégories de Personnes concernées**

|  |  |
| --- | --- |
| Employees and/or consultants of the Contractor  Clients of the Data Controller  Users of the following service/website/application:  Data Hub Opinum | Other : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Catégories de Données à caractère personnel**

|  |  |
| --- | --- |
| Personal identification data (*name, address, telephone number, etc*.)  Electronic identification data (*IP address, MAC asdress, cookies, etc*.)  Financial data (*bank account numbers, insurance, salary, etc.*)  Personal characteristics (*age, gender, date of birth, place of birth, citizenship, visas, etc.)*  Psychological data (opinions on personality, etc.)  Family *(marital status, cohabitation, name of spouse/partner, children, parents, etc.)*  Affiliations *(membership of professional and non-professional organisations, clubs, groups, associations, etc.)*  Judicial data *(data on convictions and offences, suspicions, indictments and administrative sanctions)* | Characteristics of the accommodation (*address, type of dwelling, length of stay, etc.)*  Health data *(physical health, mental health, genetic data, treatments, prescriptions, etc.)*  Education *(curriculum, study funding, qualifications, work experience, publications, etc.)*  Profession and job *(current job, job description, application data, career, salary, computer equipment data, passwords and codes, etc.)*  Photos or videos  Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Retention period**

During the Application Period

Specific retention periods: \_\_\_\_\_\_\_.

**Contact details for the person responsible for data protection compliance**

|  |  |  |
| --- | --- | --- |
|  | **Data controller** | **Subcontractor** |
| **Name** |  | FABIEN TRAMASURE |
| **Title** |  | DPO |
| **Email** |  | [dpo@opinum.com](mailto:dpo@opinum.com) |
| **Telephone number** |  |  |

**List of EU SaaS Subcontractors**

|  |  |  |
| --- | --- | --- |
| **Company name** | **Place of treatment** | **Nature of subsequent subcontracting** |
| Microsoft NV/SA | Data centre West Europe (Netherlands) | Opinum Data Hub Saas EU hosting |
| Claranet | EU | Cassandra cluster provider (database of measurement data) |
| 84 codes AB (CloudAMQP) | EU | Tools for queues in which messages are passed. |
| MongoDB Cloud | EU | Database of site and source metadata. |
| Splunk | US | Centralized logging tool |
| Paddle | UK | Matomo analytical tool |
| Exavault | US | FTP (optional) |
| Altova | EU | EU MapForce tool used to transform data files into the standard Opinum format (optional) |
| Aspose Pty Ltd | BE | Generates reports containing customer data, as requested by customers in Excel or PS (optional) |
| Plivo Inc. | US | SMS sending tools (optional) |
| SendGrid | US | Emailing platform (optional) |
| Schneider electric industries sas | FR | Algorithm (optional) |
| Highsoft | EU | HighChart library |
| Syncfusion | US | Flutter (optional sitecare) |
| HATCH Group | BE | Development Agency (optional sitecare) |
| Microsoft Bing | US | Bing converts addresses into geopoints for display on maps |

**ANNEXE B Technical and organisational measures**

## Organisational measures

* ***Physical security of buildings (alarm, access badge, cameras)***
* ***Employee computers are password protected and all employee computers are equipped with anti-virus software.***
* ***Appointment of a DPO and CISO***
* ***Information security policy***
* ***Internal RGPD compliance policy***
* ***Contractual privacy clauses***
* ***Data protection and information security awareness***
* ***Data processing contract with subcontractors***
* ***Logging***

## Technical measures

**API (Opinum)**

Access to the REST API is secured by authentication. To connect to the REST API, a unique client ID/secret pair must be requested and generated by Opinum. This authorization information only gives the right to access the REST API.

A user must still authenticate before they can access the account they are bound to exclusively.

**STORAGE (Opinum)**

Files uploaded directly to Opinum Data Hub Storage are effectively secured by the HTTPS connection. More details in the Data Access chapter.

**DATA ENCRYPTION**

All data is encrypted between the platform and the browser.

**DATA STORAGE**

Opinum uses several types of database, all of which have a high level of security and availability.

Opinum uses the Microsoft data centre called Western Europe, based in the Netherlands.

Microsoft™ Azure runs in data centres managed and operated by Microsoft™. These data centres in various locations comply with leading industry standards for security and reliability, such as ISO/IEC 27001:2013 and NIST SP 800-53.

Microsoft™ Azure SQL databases automatically create database backups that are retained for 35 days and use Azure Geo-Redundant Read Access Storage (RA-GRS) to ensure their preservation even if the data centre is unavailable.

​**USER MANAGEMENT**

* ***User access***

Each Opinum Data Hub user has strict access to the account to which they belong. Each user is identified by a unique identifier, their email address. Each email address, and therefore each user, can only have access to one account. It is not possible for a user to log into another account.

Each user has permissions on sites and sources according to their role.

Users in the Manager role have access to all sites and sources in their account.

Users in the User role only have access to sites and sources for which they have been given permission. These permissions are set by a user in that account with the Manager role. Under no circumstances can a user access data from a site or source to which they do not have permission.

* ***User authentification***

Opinum uses Oauth v2, JWS (JSON Web Signature) and Open ID Connect authentication standards.

Only a hash of the passwords is stored. Opinum has no way of accessing the decrypted passwords.

* ***Session Management***

Each session per user is limited to one hour. After one hour the user is disconnected and must reconnect.

**OTHER MEASURES**

* ***Anti-virus and malware***
* ***Firewalls***
* ***Network segregation***
* ***Remote access security***
* ***Test protocol***

Each year Opinum has a penetration test carried out by an independent and certified organisation. The results of the latest penetration test are available on request via our ticketing tool : <https://help.opinum.com/tickets>

* https://identity.opinum.com
* https://datahub.opinum.com
* https://api.opinum.com
* https://push.opinum.com
* FTP

The methodology used covers industry standards:

The Technical Guide to Information Security Testing and Assessment (SP 800-115) produced by the National Institute of Standards and Technology (NIST)

The Penetration Testing Execution Standard (PTES), created by security professionals to provide a detailed framework for conducting penetration tests.

The key elements of the Open Web Application Security Project (OWASP) testing guide.