DATA PROCESSING AGREEMENT

This Data Processing Agreement, including any schedules attached to it (hereinafter, the "**DPA**"), supplements the Terms of Service (hereinafter, the "**Agreement**"), entered into by and between the Customer, as defined in the Agreement, hereinafter, the "**Controller**") and **Marker.io SRL** (hereinafter, the "**Processor**"), a Belgian company registered at the Crossroads Bank for Enterprises under the number 0556.685.968, having its registered office at Quai Paul Verlaine 2/2, 6000 Charleroi. By executing the Agreement, the Controller enters into this DPA on behalf itself and, to the extend required under applicable Data Protection Legislation (as defined below).

Controller and Processor are hereinafter individually referred to as a "**Party**" and collectively referred to as the "**Parties**".

WHEREAS:

1. Controller and Processor have exchanged the necessary documentation, including without limitation privacy policies, terms of service, records of processing activities, and information and security policies, in order for the Parties to be able to frame the actions to be undertaken under the present DPA; and

2. Controller and Processor wish to lay down in this DPA the assignment for and further agreements concerning the processing of these Personal Data by Processor under or in connection with the Agreement.

IT IS AGREED AS FOLLOWS:

1. INTERPRETATION

1.1 In this DPA, the following words shall have the hereinafter stated meaning when written with a capital letter:

Agreement has the meaning given to that term in recital 1 of this DPA;

Approved Sub-Processors means the Sub-Processors that have been approved by Controller in accordance with article 5;

Data Protection Legislation means any law, enactment, regulation, regulatory policy, by law, ordinance, or subordinate legislation relating to the processing, privacy, and use of Personal Data, as applicable to Controller, Processor, and/or the Services, including:

(a) in Belgium:

(i) the Regulation of the European Parliament and of the Council 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) (GDPR), and any corresponding or equivalent national laws or regulations; and

(ii) the Data Protection Act of 30 July 2018 and any other national laws or regulations implementing the GDPR;

(iii) the Electronic Communications Act of 13 June 2005 and any other national laws or regulations implementing EU Directive 2002/58/EC (ePrivacy Directive)

(b) in other EU countries: the ePrivacy Directive and the GDPR, and all relevant Member State laws or regulations giving effect to this Directive or corresponding with this Regulation; and

(c) any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant supervisory authority;

in each case, as in force and applicable, and as may be amended, supplemented, or replaced from time to time;

Data Security Incident has the meaning given to that term in article 4.1;

Data Subject means the individual to whom Personal Data pertains;

Personal Data means the personal data that Processor or any Approved Sub-Processor will process when providing the Services to the Controller. For the purpose of this definition, "processing" of personal data and "personal data" will have the meaning given to those terms under the applicable Data Protection Legislation. A description of Personal Data is set out in schedule 2 and its sub-schedules relating to specific projects (schedule 2.1 and following);

Privacy Manager Means the contact person appointed by the Processor for all data protection matters;

Relevant Records has the meaning given to that term in article 7.1;

Services means the services that Processor will provide to Controller under or in connection with the Agreement;

Third Country has the meaning given to that term in article 6.1.

1.2 If there is any conflict or inconsistency between any:

1.2.1 term in the main part of this DPA;

1.2.2 term in any of the schedules to this DPA; and

1.2.3 term in the Agreement and its schedules and annexes;

the term falling into the category first appearing in the list above shall take precedence.

2. General obligations

2.1 When processing Personal Data, the Parties will at all times comply with their obligations under all applicable Data Protection Legislation.

2.2 Processor will agree to comply with any security policies and standards that may be made available by the Controller to Processor from time to time.

2.3 Processor will (and will ensure that the Approved Sub-Processors will) only process Personal Data on behalf of the Controller:

2.3.1 in the manner and for the purposes set out in schedule 2, including any of its sub-schedules; and

2.3.2 upon the written instruction of the Controller.

2.4 In addition to the foregoing, the Controller hereby:

2.4.1 instructs Processor to take such steps in the processing of Personal Data on behalf of the Controller as are reasonably necessary for the provision of the Services under or in connection with the Agreement; and

2.4.2 authorises Processor to provide to the Approved Sub-Processors and on behalf of Controller instructions that are equivalent to the instructions set out in article 2.4.1.

2.5 The Controller represents and warrants that the documentation it provides to Processor in connection to this DPA for the delineation of its tasks under same agreement, therein included, without limitation its privacy policies and its safety and security policies, are true and accurate on the date as of which such information is provided to Processor in the light of the circumstances and purposes for which such documentation has been provided.

2.6 If in Processor' reasonable opinion, compliance with Controller's instructions would constitute a breach of the applicable Data Protection Legislation, Processor will promptly notify Controller thereon in writing within a reasonable delay.

1. If the Controller does not answer to Processor' reasonable opinion referred above, within a delay of fourteen (14) calendar days of receiving it, Processor will be free to put the particular instruction aside, without incurring any penalty or liability in that regard. If the Controller should persist in its instruction, and Processor remains unsatisfied, the Parties agree to address a joint request to the Belgian Data Protection Authority or another independent third-party expert, appointed by a common decision of both Parties.

3. CONFIDENTIALITY AND SECURITY

3.1 Processor undertakes to treat all Personal Data strictly confidential. Unless Controller requires otherwise in writing, Processor will not disclose Personal Data to any third party other than:

3.2 to those of its employees, Approved Sub-Processors, and employees of the Approved Sub-Processors to whom such disclosure is strictly necessary for the provision of the Services, provided that:

(i) any disclosure under this article 3.1 is made subject to strict obligations of confidentiality and data protection no less onerous than those imposed upon Processor under this DPA, under the Agreement, and consistent with any procedures specified by Controller from time to time;

(ii) the persons to whom Personal Data may be disclosed pursuant to article 3.1.1 will have received appropriate training regarding the data protection obligations that Processor and the Approved Sub-Processors must comply with under applicable Data Protection Legislation and under this DPA;

(iii) Processor will implement measures to ensure that any persons to whom Personal Data may be disclosed pursuant to article 3.1.1 will not process Personal Data except on instruction from the Controller; or

3.2.2 to the extent required by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction, provided that Processor will:

(i) give written notice to Controller of any disclosure of Personal Data that Processor or any Approved Sub-Processor is required to make under article 3.1.2, promptly after it becomes aware of that requirement (unless such notice is prohibited by applicable legislation); and

(ii) co-operate with Controller regarding the timing and content of such disclosure and any action which Controller may wish to take to challenge the validity of such requirement.

3.3 In regard to the Controller, Processor will (and will ensure that the Approved Sub-Processors will) implement the security measures set out in schedule 1 and will keep these measures in place for the entire term of this DPA. Processor will consider these measures as minimum standards imposed on it by the Controller and may make the appropriate changes in order to complement those minimum security measures in schedule 1.

4. Reporting Data Security Incidents

4.1 Processor will provide Controller with written notice, promptly, but in any event without undue delay of becoming aware of any actual or potential:

4.1.1 breach of security that leads (or may lead) to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Personal Data (or any media or carrier containing the same) held by Processor or Approved Sub-Processors;

4.1.2 unauthorized processing of any Personal Data held by Processor or the Approved Sub-Processors;

4.1.3 breach by Processor or by any Approved Sub-Processor of the obligations of this DPA or under applicable Data Protection Legislation; or

4.1.4 enforcement proceeding, action, lawsuit, or any pending or threatened enforcement proceeding, action, lawsuit, brought or threatened against Processor or Approved Sub-Processors relating in any way to Personal Data;

(each a "**Data Security Incident**").

4.2 After the receipt of the notice referred under article 4.1, the Parties will further coordinate on in common accord on the provision by Processor to the Controller of a written notice containing at least the following information, as may be required for notification to the competent Data Protection Authority and the completion of each Party's internal registers:

4.2.1 a reasonably detailed description of the nature of the Data Security Incident including (without limitation):

(i) the categories and number (including the minimum and maximum number) of affected Data Subjects; and

(ii) the categories and number (including the minimum and maximum number) of affected data records concerned;

4.2.2 the name and contact details of the Privacy Manager or other representatives of Processor who may provide additional information about the Data Security Incident to Controller;

4.2.3 when the Data Security Incident took place (date or time period);

4.2.4 the type of Personal Data that are affected by the Data Security Incident, such as (non-exhaustively) name and address details; telephone numbers; email addresses; login details; government-issued unique identifiers (including (without limitation) tax and social insurance numbers); copies of identity documents (such as passports); gender, date of birth and/or age and other details;

4.2.5 whether the affected Personal Data had been encrypted, hashed, or otherwise rendered incomprehensible, inaccessible, or unintelligible for unauthorized persons and how this took place;

4.2.6 the (suspected) cause of the Data Security Incident;

4.2.7 relationship with any earlier Data Security Incidents;

4.2.8 the likely consequences of the Data Security Incident;

4.2.9 the measures taken and proposed to be taken by Processor and the Approved Sub-Processors pursuant to article 4.5; and

4.2.10 any additional information as may be requested by Controller in relation to the data breach.

4.3 In addition to the coordination referred under article 4.2, the Parties will coordinate with each other to further investigate the Data Security Incident. Processor will (and will ensure that the Approved Sub-Processors will) fully cooperate with Controller, in handling of the Data Security Incident, including, without limitation, by:

4.3.1 assisting with any investigation (including any investigation conducted by or on behalf of a competent public authority);

4.3.2 providing an external auditor mandated by the Controller with physical access to the facilities and operations affected;

4.3.3 facilitating interviews with employees of Processor or of any Approved Sub-Processor and others involved in the matter; and

4.3.4 making available all Relevant Records, logs, files, data reporting, and other materials that may be useful for the investigation of the Data Security Incident or for allowing Controller to notify the Data Security Incident to a competent public authority or to the affected Data Subjects.

4.4 Processor will duly document any Data Security Incident. Such documentation must contain at least the information set out in paragraphs 4.2.1 through 4.2.10 as well the results of the investigation referred to in article 4.3.

4.5 Processor will not release or publish any filing, communication, notice, press release, or report concerning any Data Security Incident without Controller's prior written approval unless Processor is required to do so pursuant to applicable law. In the latter case, Processor will provide the Controller with reasonable prior written notice where lawful to do so in order to provide Controller with the reasonable opportunity to object to such disclosure.

4.6 Processor will take the measures that are reasonably necessary:

4.6.1 to remedy any Data Security Incident;

4.6.2 prevent any re-occurrence of the Data Security Incident or any further Data Security Incidents;

4.6.3 to mitigate the impact of the Data Security Incident on the privacy of the Data Subjects; and

4.6.4 to mitigate any adverse impact of the Data Security Incident on the Controller.

5. SUBCONTRACTING AND SUB-PROCESSING

5.1 Processor may subcontract all or part of the processing of Personal Data if Processor provides the Controller, prior to any intended changes concerning the addition or replacement of a sub-processor, with a notification on it intend to subcontract. The Controller shall have a delay of seven (7) calendar days to reasonably object to such changes in the processing of the Personal Data. In the absence of such an objection, the sub-processor will be considered an Approved Sub-Processor.

5.2 Processor and the Sub-Processor will enter into a written data processing agreement setting out the same, considered functionally rather than formally, (or more onerous) obligations as those set out in this DPA.

5.3 For the purpose of article 5.1, the Controller hereby accepts the subcontracting of the processing of Personal Data to the Sub-Processors described in schedule 3. The Sub-Processors described in schedule 3 will be deemed to be the Approved Sub-Processors for the purpose of this DPA.

5.4 If Processor wishes to subcontract all or part of the processing of Personal Data, it will first provide to the Controller a prior written notice of its intention to engage any Sub-Processor setting out the following information in sufficient detail:

5.4.1 the name and address of the proposed Sub-Processor;

5.4.2 the subject matter of the proposed subcontract, including a description of the services to be provided by the proposed Sub-Processor, the proposed sub-processor's involvement in the processing of Personal Data;

5.4.3 the countr(y)(ies) where the proposed sub-processor intends to process Personal Data;

5.4.4 a description of the technical and organisational measures implemented by the proposed sub-processor to protect the security, confidentiality, and integrity of Personal Data that will be processed by the proposed sub-processor;

5.4.5 a written confirmation by Processor that the sub-processor agrees to be bound by a written data processing agreement setting out the same (or more onerous) obligations as those set out in this DPA;

5.4.6 any additional information that Controller may reasonably require; and

5.4.7 if the proposed sub-processor intends to further subcontract the processing of Personal Data, the information set out in paragraphs 5.3.1 through 5.3.6 in respect of each sub-processor to whom the proposed sub-processor intends to further subcontract the processing of Personal Data.

5.5 Processor will remain liable for all acts and omissions of the Approved Sub-Processors as fully as if they were the acts and omissions of Processor or its employees or agents.

6. Cross-border transfers of Personal Data

6.1 Processor will not (and Processor will ensure that the Approved Sub-Processors will not) transfer or permit access to Personal Data to a country or its agencies outside of the European Economic Area (“**EEA**”) (such other country being a “**Third Country**”), whatever the means unless Controller has approved such transfer in writing prior to such transfer taking place and:

6.1.1 there has been an **EU Commission finding of adequacy** in respect of that Third Country pursuant to applicable Data Protection Legislation, or

6.1.2 the Sub-Processor (and/or Agreed Sub-Processors) transfer the Personal Data in the framework of **binding corporate rules**; or

6.1.3 the transfer takes place within the context of **an approved certification mechanism**, in accordance with the applicable Data Protection Legislation; or

6.1.4 the Sub-Processor (or its Approved Sub-Processors) agrees to the application of the **standard contractual clauses** ("**SCCs**") approved by the EU Commission or another competent data protection authority, in the application of the applicable Data Protection Legislation.

2. Before proceeding to transfer Personal Data, except in the hypothesis of article 6.1.1., Processor agrees to verify the applicable data protection legislation in force in the Third Country to which the Personal Data would be transferred. Processor undertakes to evaluate the effectiveness of the protection afforded by such legislation, as compared to the applicable Data Protection Legislation. If Processor should find that the legislation in the Third Country does not guarantee an essentially equivalent level of data protection, compared to the applicable Data Protection Legislation, it undertakes to implement additional measures in order to achieve such essentially equivalent level of protection.

7. Audit

7.1 Processor will keep at its normal place of business detailed, accurate and up-to-date records describing in reasonable detail (such records hereafter referred to as "**Relevant Records**"):

7.1.1 the processing of Personal Data by Processor and the Approved Sub-Processors (including, without limitation, the nature and the purpose of the processing, the type of Personal Data and the categories of data subjects);

7.1.2 a list of all the Approved Sub-Processors;

7.1.3 for each Approved Sub-Processor:

(i) a description of the processing conducted by the Approved Sub-Processor (including, without limitation, the nature and the purpose of the processing, the type of Personal Data and the categories of data subjects); and

(ii) a copy of the data processing agreement entered into by the Approved Sub-Processor pursuant to article 5.1.2;

7.1.4 in the event described in article 6.1.4 an execution copy of the contract containing the approved model clauses;

7.1.5 a description of the measures taken pursuant to article 3;

7.1.6 if applicable, the information referred to in article 4.3; and

7.1.7 any other information that:

(i) Processor or the Approved Sub-Processors are required to document under or pursuant to applicable Data Protection Legislation; or

(ii) is necessary to demonstrate to Controller that Processor’s and the Approved Sub-Processors' compliance with this DPA and with applicable Data Protection Legislation.

7.2 Processor will permit the Controller’s third party representatives as well as any competent public authority to:

7.2.1 gain access to, and take copies of, the Relevant Records and any other information that is available to Processor; and

7.2.2 inspect all systems used by Processor for processing Personal Data;

during normal business hours for the purpose of auditing Processor' compliance with their obligations under this DPA and with the applicable Data Protection Legislation.

7.3 Processor will provide all reasonable assistance to the conduct of such audits.

7.4 Any such audit will be subject to the Controller’s representative agreeing to reasonable confidentiality obligations in respect of the information obtained, provided that all information obtained may be disclosed to Controller.

7.5 Following an audit, if Controller or any competent public authority in their reasonable opinion deems that Processor or any Approved Sub-Processor is failing to comply with any of its obligations under this DPA or under any applicable Data Protection Legislation:

7.5.1 Processor will provide to Controller an action plan to:

(i) remediate the deficiencies identified in the audit; and

(ii) ensure that such deficiencies or any similar deficiencies will not (re-)occur in the future (“**Remediation Plan**”);

7.5.2 promptly upon the validation of the Remediation Plan by Controller and/or the competent public authority, as the case may be, Processor will implement the Remediation Plan. Not less than once a month Processor will update Controller and/or the competent public authority, as the case may be, on the status of the implementation of the Remediation Plan;

7.5.3 upon completion of the Remediation Plan, Processor will notify Controller or the competent public authority, as the case may be, and Controller or the competent public authority will be entitled to conduct another audit in accordance with this article 7 in order to verify whether the Remediation Plan has been duly implemented; and

7.5.4 Processor will bear any costs and expenses resulting from:

(i) the conduct of such audit falling under the application of article 7.5;

(ii) the preparation, validation, and implementation of any Remediation Plan; and

(iii) any follow-up audit to verify due implementation and completion of any Remediation Plan.

8. Assistance when Handling requests from data subjects

8.1. Processor will (and will ensure that the Approved Sub-Processors will) fully cooperate with Controller when handling requests from Data Subjects exercising their rights, including (without limitation) their right to be informed about the processing of their Personal Data, under applicable Data Protection Legislation.

8.2. Processor shall:

8.1.1 without undue delay notify the Controller when Processor (or any Approved Sub-Processors) receives a request from a Data Subject under any of the applicable Data Protection Legislation in respect of the Personal Data; and

8.1.2 take all required actions and provide all required information, by e-mail to the Privacy Manager info@marker.io or by letter to the address of the Processor as indicated above within fifteen (15) days as of its receipt, unless otherwise instructed by the Controller; and

8.1.3 ensure that it (or any Approved Sub-Processor) does not respond to that request except on the documented instructions of Controller or as required by applicable Data Protection Legislation to which Processor is subject.

9. Assistance when Conducting piaS

Processor will (and will ensure that the Approved Sub-Processors will) fully cooperate with Controller when conducting any privacy impact assessments in connection with the provision of the Services.

10. Term and termination

10.1 This DPA enters into force on its signature and will remain in force for as long as Processor will provide the Services under the Agreement unless this DPA is terminated earlier in accordance with this article 10.

10.2 The Controller has the right, without prejudice to its other rights or remedies, to terminate this DPA immediately (without the necessity for judicial action) by written notice to Processor if the latter is in material breach of this DPA and either that breach is not capable of remedy or, if the breach is capable of remedy, Processor has failed to remedy the breach within thirty (30) days after receiving written notice of default from Controller requiring it to do so.

10.3 Notwithstanding any other breach which qualifies as material under article 10.2, any breaches by Processor of articles 2, 3, 4, 5, or 6 will be considered a material breach allowing Controller to terminate this DPA in accordance with article 10.2.

11. Transferability

Processor is not entitled to transfer the rights and/or obligations arising from this DPA to a third party without prior written approval from Controller.

12. Return/Destruction of Personal Data

12.1 Unless stated otherwise for a specific project, within ninety (90) days after expiration or termination of this DPA, Processor will (and will ensure that the Approved Sub-Processors will):

12.1.1 at the option of Controller:

(i) return to Controller in a then commonly used electronic format all Personal Data that, as of the termination date or expiration date, are in the possession or under the control of Processor and/or the Approved Sub-Processors; or

(ii) destroy or purge their computer systems and files of any Personal Data that, as of the termination date or expiration date, are in the possession or under the control of Processor and the Approved Sub-Processors; and

12.1.2 deliver to Controller a written notice in order to:

(i) confirm that such return, destruction, and purging have been carried out; and

(ii) identify in reasonable detail which Personal Data Processor and the Approved Sub-Processors are required by the applicable law to retain after termination or expiration of this DPA.

12.2 The provisions set out in article 12.1.1 will not apply to any Personal Data that Processor and the Approved Sub-Processors are required by the applicable law to retain after termination or expiration of this DPA, in which case:

12.2.1 the provisions of this DPA will survive the termination or expiration of this DPA and will continue to apply to these Personal Data; and

12.2.2 Processor will (and will ensure that the Approved Sub-Processors will) perform their obligations under article 12.1 promptly when Processor and the Approved Sub-Processors are no longer required to retain these Personal Data.

13. Indemnification

13.1 Each Party ("**Defaulting Party**") shall be liable in relation to the other Party ("**Non-defaulting Party**") for any material breach or infringement it commits against the provisions set out in this DPA and/or for any breach of the provisions of the applicable Data Protection Legislation, bringing harm to the Non-defaulting Party but excluding any harm arising from administrative fines or private damages which are compensated to the other Party in the manner set out under Section 13.2. The Parties' liability extends to the actions committed by their legal representatives, subcontractors, employees, or any other agents.

3. The liability of the Defaulting Party does not include any damages resulting from operational loss, profit loss, loss of goodwill, and any other indirect loss and consequential damage. Data loss shall not be considered falling under the scope of indirect loss.

4. Any damages owed by the Defaulting Party to the Non-defaulting Party shall be further limited in accordance with the provisions relating to the limitations of liability as set out under the Agreement concluded between the Parties, or any other applicable agreement between

the Parties setting out the main relationship between them and in reason of which this Agreement for the processing of personal data is constituted.

5. The previous limitations of liability do not apply in those circumstances where the Defaulting Party acted intentionally, or where the harm was caused by wilful misconduct or by gross negligence.

13.2 Nothing in this article 13 of the DPA will affect any Party's liability to the Data Subjects to the extent that the limitation of such rights is prohibited by the Data Protection Laws.

14. Applicable law and jurisdiction

This Agreement will be governed by the laws of Belgium. The courts of Hainaut, department of Charleroi will have exclusive jurisdiction for any dispute between the Parties arising out of or relating to this DPA.

Schedule 1: Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

Physical Access Control

No unauthorised access to Data Processing Facilities, (access control, intrusion detection, and video surveillance systems.)

Electronic Access Control

No unauthorised use of the Data Processing and Data Storage Systems (secure passwords, firewall, automatic blocking/locking mechanisms, encryption of data carriers/storage media).

Internal Access Control (permissions for user rights of access to and amendment of data)

No unauthorised Reading, Copying, Changes or Deletions of Data within the system (rights authorisation concept, need-based rights of access, logging of system access events).

Isolation Control

The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing

Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)

The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

Data Transfer Control

No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption over SSL/TLS 1.2, Virtual Private Networks (VPN), electronic signature

Data Entry Control

Verification, whether and by whom personal data is entered into a Data Processing System, is changed, or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

Availability Control

Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site and dual redundancy), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning

Rapid Recovery (Article 32 Paragraph 1 Point c GDPR)

4. Procedures for regular testing, assessment, and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

Data Protection Management

Incident Response Management

Data Protection by Design and Default (Article 25 Paragraph 2 GDPR)

Order or Contract Control

No third party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks

DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES TAKEN BY THE PROCESSOR AND DESCRIPTION OF THE LOCATION OF DATA PROCESSING

The data processing is based in Europe and the legal entity of the Processor incorporated in Belgium.

All of the personal data are store in Amazon (AWS) server in Ireland. For encryption, the Processor use https in transit and the hashing process at rest.

AWS data centers feature state of the art environmental security controls to safeguard against fires, power loss, and adverse weather conditions. Physical access to these facilities is highly restricted, and they are monitored by professional security personnel.

Processor’s offices are equipped with access control, intrusion detection, and video surveillance systems. All communications are encrypted over SSL/TLS 1.2, which cannot be viewed by a third party and is the same level of encryption used by banks and financial institutions.

Processor monitors documented threats from public security research databases (such as the Common Vulnerabilities and Exposures catalog), and its employees run automated vulnerability scanners, including retire.js and nsp, at regular intervals and before each deployment.

Processor’s developers receive training for secure software development, including Open Web Application Security Project guidelines.

All major code changes are subject to a multipoint code review, with specific attention paid to security.

Processor maintains firewalls on its edge servers and origin load balancers to protect against bandwidth and protocol-based attacks, and Processor uses intelligent web application firewalls and elastic scaling of its compute capacity to mitigate attacks at the application layer, including complex and evolving attacks. All personal data is stored with at least dual redundancy, and Processor have designed its storage solution for 99.999999999% long-term durability.

For Jira, when a user enters its authentication credentials in Processor’s solution, they are first ciphered using a highly secure algorithm (AES 256 bits) and then stored in Processor’s encrypted MongoDB database.

For all the other integrations, Processor uses OAuth2/OAuth3, which means Processor asks for certain permission to access user’s tool. The token Processor get from that connection is unique and stored securely in its encrypted database.

Processor's team access is controlled by a carefully managed and audited security policy. All team members sign non-disclosure agreements to protect user’s personal data. All employees receive tools and training for handling sensitive data (including credentials) and for avoiding social engineering and other non-technical attacks.

Processor's team log activity across its platform, from individual API requests to infrastructure configuration changes. Logs are aggregated for monitoring, analysis, and anomaly detection and archived in vaulted storage. Processor implements measures to detect and prevent log tampering or interruptions.

Processor conducts regular internal security audits and review its hardware, software, and physical security configurations. If the Processor discovers a vulnerability, a formal incident response framework will be followed to ensure rapid mitigation and transparent Controller communication.

Schedule 2: Description of data processing

1. Nature of the Data

The nature of the personal data used is precisely defined in the Agreement.

2. Categories of Data Subjects

The Categories of Data Subjects are precisely defined in the Agreement.

3. The purposes of the data processing

The personal data will be processed to perform the Services as agreed in the Agreement and to manage the contractual relationship between the Processor and the Controller.

4. The manner in which the data processing will be conducted

Personal data will be processed in accordance with the Controller's instructions. Controller shall without undue delay confirm oral instructions (at the minimum in electronic form).

5. The processing instructions

The processing instructions are set in the Agreement.

6. The data protection officer or other contact person at the Controller:

The contact details are set in the Controller’s privacy policy.

7. The Privacy Manager at the Processor:

Name: Olivier Kaisin

Contact details:

Address: Quai Paul Verlaine 2/2, 6000 Charleroi
Phone number: +32 494 73 16 46
Email: olivier@marker.io

Schedule 3: Approved Sub-Processors

Amazon Web Services, Inc	Infrastructure	https://aws.amazon.com/privacy/	- Contact details - Screen capture & issue details - Data that identifies you	This is a web hosting provider: we use it to store contracts and other data you generate by using the service securely in the cloud.	EU
MongoDB, Inc.	Infrastructure	https://www.mongodb.com/legal/privacy-policy	- Contact details - Screen capture & issue details - Data that identifies you - Data on how you use Marker.io	This is a hosted database provider: we use it to store data generated through your use of Marker.io	US
Cloudflare	Infrastructure	https://www.cloudflare.com/privacypolicy/	- your IP adress	We use this service to deliver the our serivce faster to you	US and EU
Google Analytics	Analytics	https://policies.google.com/privacy	- Contact details - How you use Marker.io - Data that identifies you - Cookies	GoogleAnalytics is a web analytics service: we use it to track your use of the service, and prepare reports on user activity.	US
Amplitude	Analytics	https://amplitude.com/privacy	- Data on how you use Marker.io - How you use Marker.io - Cookies	This is a web analytics service: we use it to track your use of the service, and prepare reports on user activity	US

				.	
Fullstory	Analytics	https://www.fullstory.com/legal/privacy/	- Contact details - How you use Marker.io - Data that identifies you - Cookies	This is a web analytics service: we use it to track your use of the service, and prepare reports on user activity .	US
Hotjar	Analytics	https://www.hotjar.com/legal/policies/privacy	- Contact details - How you use Marker.io - Data that identifies you - Cookies	This is a web analytics service: we use it to track your use of the service, and prepare reports on user activity .	EU
Clearbit	Analytics	https://clearbit.com/privacy	- Contact details - Data that identifies you - Cookies	This is a contact enrichement service: we use it to improve your registration and communication experience with us.	US
Segment	Analytics	https://segment.com/docs/legal/privacy/	- Contact details - How you use Marker.io - Data that identifies you - Cookies	This is a web analytics service: we use it to track your use of the service, and prepare reports on user activity .	US

Profitwell	Analytics	https://www.profitwell.com/privacy-policy	- Contact details - How you use Marker.io - Data that identifies you - Cookies	This is a web analytics service on top of payment provider stripe: we use to track financial metrics based on user activity	US
Plausible	Analytics	https://plausible.io/privacy	- How you use Marker.io (anonymously data)	This is a web analytics service: we use it to track your use of the service, and prepare reports on user and website visitor activity.	EU
Stripe	Payments	https://stripe.com/privacy	- Contact details - Financial information - Cookies	This service processes payments for us.	EU and US
Quaderno	Payments	https://quaderno.io/privacy/	- Contact details - Financial information - Cookies	This service processes tax calculation and invoicing for us.	EU
VatStack	Payments	https://vatstack.com/privacy	- Contact details - Financial information	This service processes tax calculation.	US
Close.com	Customer Communication	https://www.close.com/privacy	- Contact details	This is our CRM to help new sign ups become successfull with Marker.io	US
Sendgrid, Inc. (now twilio)	Customer Communication	https://sendgrid.com/policies/privacy/	- Contact details - How you use Marker.io	We use this service for sending, storing and tracking emails.	US

Intercom, Inc.	Customer Communication	https://www.intercom.com/terms-and-policies#terms	- Contact details - How you use Marker.io - Cookies	We use this service for customer communications, user interaction and helpdesk assistance.	US
Customer.io	Customer Communication	https://customer.io/legal/privacy-policy/	- Contact details - How you use Marker.io - Cookies	We use this service for sending, storing and tracking emails.	US
Jira	Integrations (by your request)	https://www.atlassian.com/legal/privacy-policy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Jira and facilitate how you're able to report and collect issues into these services	US
GitHub	Integrations (by your request)	https://help.github.com/articles/github-privacy-statement/	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with GitHub and facilitate how you're able to report and collect issues into GitHub	US
Asana	Integrations (by your request)	https://asana.com/terms#privacy-policy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Asana and facilitate how you're able to report and collect issues into Asana	US

GitLab	Integrations (by your request)	https://about.gitlab.com/privacy/	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with GitLab and facilitate how you're able to report and collect issues into GitLab	US
Slack	Integrations (by your request)	https://slack.com/privacy-policy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Slack and facilitate how you're able to report and collect issues into Slack	EU and US
Bitbucket	Integrations (by your request)	https://www.atlassian.com/legal/privacy-policy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Bitbucket and facilitate how you're able to report and collect issues into these services	US
Trello	Integrations (by your request)	https://www.atlassian.com/legal/privacy-policy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Trello and facilitate how you're able to report and collect issues into these services	US

Clickup	Integrations (by your request)	https://clickup.com/privacy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Clickup and facilitate how you're able to report and collect issues into these services	US
Teamwork	Integrations (by your request)	https://www.teamwork.com/legal/privacy-policy/	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Teamwork and facilitate how you're able to report and collect issues into these services	US
Wrike	Integrations (by your request)	https://www.wrike.com/security/privacy/	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Wrike and facilitate how you're able to report and collect issues into these services	US
Shortcut	Integrations (by your request)	https://shortcut.com/privacy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Shortcut and facilitate how you're able to report and collect issues into these services	US

Notion	Integrations (by your request)	https://www.notion.so/Terms-and-Privacy-28ffdd083dc3473e9c2da6ec011b58ac	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io Notion and facilitate how you're able to report and collect issues into these services	US
Monday.com	Integrations (by your request)	https://monday.com/trustcenter/privacy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Monday.com and facilitate how you're able to report and collect issues into these services	US
Linear	Integrations (by your request)	https://linear.app/privacy	- Contact details - Screen capture & issue details - Data that identifies you	This enables us to integrate Marker.io with Linear and facilitate how you're able to report and collect issues into these services	US