IPREGISTRY DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") forms part of the Ipregistry Terms of Use (https://ipregistry.co/terms), or of any other agreement that governs your use of the Services (the "Agreement") between Ipregistry (a trademark of Elaunira SARL, a limited liability company with a share capital of €10,000, registered with the Antibes Trade and Companies Register (RCS) in France under company ID/SIREN: 983391012) and the customer ("you"). Accepting the Agreement also means accepting this Addendum and, where they apply, the Standard Contractual Clauses.

Ipregistry and you are each a "party" and together the "parties".

This Addendum applies to the processing of Personal Information in connection with your use of the Services. Unless this Addendum says otherwise, the terms of the Agreement apply to it. Terms not defined here have the meaning given in the Agreement. In this Addendum, "end users" includes your employees, customers, and their end users, as applicable. By agreeing to the Agreement, you acknowledge having read this Addendum and agree to be bound by its terms.

Ipregistry may revise this Addendum as necessary to address changes to Applicable Data Protection Law or Ipregistry policies. A revision applies to new customers when it is posted. For existing customers, it takes effect thirty (30) days after it is announced on the Ipregistry notices page (https://ipregistry.co/notices), unless they accept it earlier. Notices are also shown in the Ipregistry dashboard and sent by email to account holders who have not unsubscribed. Anyone can subscribe to them.

1. Definitions

a. "Applicable Data Protection Law" means any laws, rules, or regulations relating to privacy, security, or data protection applicable to a party's provision or use of the Services, including, as applicable (i) European Data Protection Law (ii) US Data Protection Law; (iii) the Brazilian Data Protection Law, Law N. 13.709 from August 14th, 2018 ("LGPD"); (iv) the People's Republic of China ("PRC") Personal Information Protection Law ("PIPL") and (v) any replacements, additions, successors, implementing requirements or legislation, or amendments to any of the foregoing.

b. "controller," "business," "processor," "service provider," "third party," "data subject," "consumer," "process," "personal data," "personal information," "sell," "share," "business purpose," "commercial purpose," "data protection impact assessment," and "supervisory authority" (or any equivalent terms) each has the meaning ascribed to them under Applicable Data Protection Law.

c. "Data Subject" means a data subject, consumer, or identified or identifiable natural person.

d. "European Data Protection Law" means those laws, rules, and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom relating to privacy, security, or data protection, including, as applicable (i) Regulation (EU) 2016/679 of the European Parliament and of the 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) ("GDPR"); (ii) the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("UK GDPR"); (iii) the EU ePrivacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Data Protection Act ("Swiss DPA").

e. "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject or household or that is "personal information," "personal data," or similarly protected data as ascribed under Applicable Data Protection Law.

f. "Restricted Transfer" means: (i) where the GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area that is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner, and (iv) where LGPD applies, a transfer of personal data from Brazil to a country outside of Brazil which does not provide an adequate level of protection within the meaning of LGPD.

g. "Services" refers to Ipregistry’s products and services, including the Ipregistry Datasets, the Ipregistry API & Data, the Ipregistry Web Services, and any other software, files, or data Ipregistry licenses to you.

h. "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

i. "Subprocessors" means the subcontractors of Ipregistry identified in Schedule 2, which process Personal Information that Ipregistry processes on your behalf.

j. "UK Addendum" means the "*UK Addendum to the EU Standard Contractual Clauses*" issued by the Information Commissioner's Office under s.119A(1) of the UK Data Protection Act 2018; as may be amended or superseded from time to time.

k. "US Data Protection Law" means those laws, rules, and regulations of the United States relating to privacy, security, or data protection, including, as applicable the California Consumer Privacy Act ("CCPA") as amended by the California Privacy Rights Act ("CPRA"), and the comparable privacy laws of other US states.

2. Processing of Personal Information You Provide

a. Acknowledgement. You acknowledge and agree that Ipregistry will process Personal Information you provide when you use the Services in the countries in which Ipregistry or its service providers maintain facilities, which may be outside the European Economic Area. Requests sent to the EU base URL of the Ipregistry API are answered by servers located in the European Union. They first pass through Ipregistry's network provider, whose point of entry depends on where the request comes from.

b. Ipregistry as a Processor or Service Provider. Subject to Section 2(c), Ipregistry processes Personal Information provided by you in connection with your use of the Services as a processor or service provider on your behalf. You are the controller or business (or act for one): you decide which Personal Information to provide and instruct Ipregistry on how to process it. Where Ipregistry acts as a processor or service provider on your behalf, Section 6 also applies.

c. Ipregistry as a Controller, Business, or Third Party. In some circumstances, Ipregistry processes Personal Information provided by you as an independent controller, business, or third party and you authorize this use. Ipregistry does so to operate, secure, and bill the Services, and to maintain and improve the Services and Ipregistry's data, including by using Personal Information in aggregated or de-identified form and together with data received from other sources. To maintain and improve the Services and Ipregistry's data, Ipregistry uses Personal Information sent through the API only in aggregated or de-identified form. Ipregistry does not sell the Personal Information you provide, does not use the Personal Information of your end users for advertising, and does not reveal to other customers or third parties that it originates from you or your end users. Even after you stop using the Services, Ipregistry will retain such Personal Information where it has a lawful basis to do so, for example to comply with its legal obligations, resolve disputes, and enforce its agreements. Where Ipregistry acts as an independent controller, business, or third party, each party shall be individually responsible for its own processing of the Personal Information and compliance with Applicable Data Protection Law.

d. Website. When you provide Personal Information through Ipregistry's website (including in correction requests), Ipregistry processes it in accordance with its Privacy Policy, available at https://ipregistry.co/privacy.

e. LIR Services. This Addendum does not apply to the registration, sponsorship, or lease of Internet number resources. Ipregistry processes the Personal Information collected for these

services as a controller, as described in its Privacy Policy and in the agreement signed for each resource.

3. Processing of Personal Information You Receive. You acknowledge and agree that you may receive Personal Information from Ipregistry in connection with your use of the Services, and that such information may relate to Data Subjects across jurisdictions (including from the European Economic Area, Switzerland, the United Kingdom, Brazil, and the PRC). For example, data licensed to you by Ipregistry may include Personal Information. Where you receive Personal Information from Ipregistry, you agree that (i) you will only process the Personal Information for the limited and specified purposes set forth in the Agreement and in accordance with Applicable Data Protection Law; (ii) you will provide to the Personal Information the same level of privacy protection as is required by Applicable Data Protection Law; (iii) Ipregistry has the right to take reasonable and appropriate steps to help ensure that you use the Personal Information in a manner consistent with Ipregistry's obligations under Applicable Data Protection Law; (iv) you shall notify Ipregistry if you make a determination that you can no longer meet your obligations under Applicable Data Protection Law; and (v) Ipregistry has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of the Personal Information. Ipregistry and you are each an independent controller or business with respect to the Personal Information, and each party shall be individually responsible for its own processing of the Personal Information and compliance with Applicable Data Protection Law. If you receive a Data Subject request about the Personal Information (directly or through Ipregistry), you will promptly comply with it as required by Applicable Data Protection Law. You shall give Ipregistry the assistance it needs to address any Data Subject rights or regulatory requests under Applicable Data Protection Law.

4. Your Obligations. Ipregistry requires, and you hereby represent and warrant, that (i) you have provided any legally required notices and choice, and have a lawful basis for the disclosure, transmission, and processing of Personal Information from, with, to, and by Ipregistry; (ii) you have complied with all data transfer requirements of any applicable jurisdictions, and any data transfers pursuant to this Addendum will not cause Ipregistry to be in breach of Applicable Data Protection Law; and (iii) any Personal Information provided by you has not been collected, stored, or transferred to Ipregistry in violation of any law, regulation, or contractual obligation applicable to you. You agree to maintain a privacy policy that complies with Applicable Data Protection Law and disclose your data practices relating to your use of the Services, provided that you shall not be required to expressly identify Ipregistry unless otherwise required by Applicable Data Protection Law. You shall not make any representations or warranties to your end users contrary to the terms and conditions in the Agreement. If you do, you are solely responsible for that representation or warranty to the extent it differs from the Agreement, and Ipregistry has no liability for it. As between Ipregistry and you, you are responsible for all acts and omissions of your end users in connection with their processing of Personal Information, and you will reasonably cooperate with Ipregistry in connection with any prohibited activities of any end user in connection with the Services. You will promptly notify Ipregistry if you become aware of any such prohibited activities. If the Standard Contractual Clauses are invalidated by a competent authority, you will work with Ipregistry to find an alternative legal basis for the transfer and continued processing of Personal Information in compliance with Applicable Data Protection Law, and you will cease processing Personal Information in the event no such basis is found or agreed upon by Ipregistry.

5. Liability. To the maximum extent permitted by applicable law, each party's liability is subject to the disclaimers, limitations of liability, and indemnification obligations in the Agreement.

6. Terms Applicable to Ipregistry as a Processor or Service Provider

a. Application. This Section 6 applies when Ipregistry processes Personal Information you provide as a processor or service provider on your behalf, and not when it acts as a controller, business, or third party.

b. Instructions. You instruct Ipregistry to process Personal Information for the following purposes: (i) processing in accordance with the Agreement; (ii) processing initiated by your end users in their use of the Services; and (iii) processing to comply with other documented reasonable instructions provided by you (*e.g.*, via email) where such instructions are consistent with the terms of the Agreement. Ipregistry shall process the Personal Information only on documented instructions from you, unless required to do otherwise by the applicable law to which Ipregistry is subject; in such a case, Ipregistry shall inform you of that legal requirement before processing the Personal Information, unless that law prohibits such disclosure on important grounds of public interest. The Agreement constitutes your complete and final documented instructions, and any additional or alternate instructions must be agreed upon separately. You will ensure that your instructions do not cause Ipregistry to violate any applicable law or contractual obligation. Ipregistry shall immediately inform you if, in its opinion, an instruction infringes Applicable Data Protection Law.

c. Subject Matter, Duration, Data Subjects, and Types.

   i. The subject matter of the processing is the performance of the Services to you pursuant to the Agreement.

   ii. The duration of the processing is the duration of the Agreement, except where applicable law requires otherwise.

   iii. The categories of data subjects or consumers about whom Ipregistry processes Personal Information are determined and controlled by you and may include your end users.

   iv. The types of Personal Information are determined and controlled by you and may include IP addresses, postal code level or less precise geolocation data, and user-agents.

d. CCPA/CPRA. For any Personal Information subject to CCPA/CPRA, Ipregistry agrees and certifies that it shall not: (i) sell or share the Personal Information; (ii) retain, use, or disclose the Personal Information for any purpose, including a commercial purpose, other than for the specific purpose of performing the Services or as otherwise permitted of a service provider by CCPA/CPRA; (iii) retain, use, or disclose the Personal Information outside of the direct business relationship between Ipregistry and you or (iv) combine the Personal Information with personal information that Ipregistry receives from or on behalf of another person, or

collects from its own interaction with the Data Subject, provided that Ipregistry may combine personal information to perform any business purpose as otherwise permitted of a service provider by CCPA/CPRA. If Ipregistry engages any other person to assist it in processing Personal Information for a business purpose on behalf of you, or if any other person engaged by Ipregistry engages another person to assist in processing Personal Information for such business purpose, it shall notify you in accordance with Section 6(e) below of such engagement, and the engagement shall be pursuant to a written contract binding the other person to observe requirements at least as protective as those set forth in this Section 6(d).

e. Subprocessors.

   i. You give Ipregistry general written authorization to engage the Subprocessors listed in Schedule 2 to help provide the Services. The list may change as described in Section 6(e)(ii). Ipregistry shall enter into an agreement with each Subprocessor containing data protection obligations no less protective than those in this Addendum with respect to the protection of Personal Information to the extent applicable to the services provided by the Subprocessor. Ipregistry shall be liable for the acts and omissions of its Subprocessors to the same extent Ipregistry would be liable if performing the services of each Subprocessor directly under the terms of the Agreement. Where a Subprocessor processes Personal Information outside the European Economic Area, Ipregistry ensures that the transfer relies on appropriate safeguards, such as the Standard Contractual Clauses, or on an adequacy decision.

   ii. Ipregistry shall announce any new Subprocessor on its notices page (https://ipregistry.co/notices) at least fifteen (15) business days before it processes Personal Information for the Services provided to you. These notices are also shown in the Ipregistry dashboard and sent by email to account holders who have not unsubscribed. Anyone can subscribe to them. You may object to Ipregistry's use of a new Subprocessor, on reasonable grounds relating to the protection of Personal Information, by notifying Ipregistry promptly in writing within ten (10) business days after the announcement. If you object to a new Subprocessor, Ipregistry will use reasonable efforts to make available to you a change in the Services or recommend a commercially reasonable change to your configuration or use of the Services to avoid processing of the Personal Information by the objected-to new Subprocessors without unreasonably burdening you. If Ipregistry is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, you may terminate the applicable Services which cannot be provided by Ipregistry without the use of the objected-to new Subprocessor by providing written notice to Ipregistry. Ipregistry will refund you the fees prepaid for the unused part of the current subscription period of such terminated Services, counted from the effective date of termination, without imposing a penalty for such termination on you.

f. Requests. Ipregistry shall, to the extent legally permitted, promptly notify you if Ipregistry receives a request from a Data Subject to exercise their rights under Applicable Data Protection Law ("Request"). Taking into account the nature of the processing, Ipregistry shall use commercially reasonable efforts to assist you in the fulfillment of your obligation to

respond to the Request. To the extent legally permitted, you shall be responsible for any costs arising from Ipregistry's provision of such assistance. You acknowledge and agree that Ipregistry may not be able to fulfill a Request where to do so would violate laws applicable to Ipregistry, or would interfere with Ipregistry's ability to meet legal obligations or protect its rights or those of a third party.

g. Data Protection Impact Assessments. Ipregistry shall provide you with reasonable cooperation and assistance as needed and appropriate to fulfill your obligations under the Applicable Data Protection Law to carry out a data protection impact assessment related to your use of the Services, to the extent you do not otherwise have access to the relevant information, and to the extent such information is available to Ipregistry. Ipregistry shall provide reasonable assistance to you in the cooperation or prior consultation with the supervisory authority in the performance of its tasks relating to the data protection impact assessment, to the extent required under Applicable Data Protection Law. To the extent legally permitted, you shall be responsible for any costs arising from Ipregistry's provision of such assistance.

h. Audit. Subject to a confidentiality undertaking, you may make a written request at reasonable intervals that Ipregistry make available to you the information necessary to demonstrate its compliance with this Section 6, including a summary of its technical and organizational security measures and the certifications or audit reports of its hosting providers that are available to it. If, after receiving this information, you need further information to demonstrate Ipregistry's compliance with its obligations as a processor or service provider, then Ipregistry agrees at the written request from you to submit, to the extent reasonably possible, any facilities where it processes Personal Information on behalf of you for audit to ascertain compliance. Such audit shall be carried out upon the reasonable request of you, with reasonable notice, at reasonable intervals (no greater than once per year), during normal business hours, under confidentiality terms agreed in advance, and without requiring Ipregistry to provide access to information relating to its other customers. You are responsible for and shall reimburse Ipregistry for the reasonable expenses associated with the audit. You must receive written approval from Ipregistry, which Ipregistry will not unreasonably withhold, before using any third party auditor, and such third party auditor must submit to a duty of confidentiality with respect to the audit, and must not be a competitor of Ipregistry, affiliated with one, acting at the request of one, or otherwise manifestly unsuitable.

i. Security. Ipregistry shall maintain appropriate technical and organizational measures for the protection of the security, confidentiality, and integrity of Personal Information (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss, alteration or damage, unauthorized disclosure of, or access to, Personal Information), including as further set out in Schedule 3 hereto. Ipregistry regularly monitors compliance with these measures and may update such measures from time to time, so long as such updates will not materially decrease the overall security of the Services during the provision of the Services pursuant to the Agreement. Ipregistry shall ensure that persons authorized to carry out processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality.

j. Incident Management and Notification. Ipregistry shall notify you without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information transmitted, stored, or otherwise processed by Ipregistry on behalf of you (a "Data Incident"). Ipregistry shall provide you with the information reasonably available to it about the Data Incident, to help you meet your own notification obligations. Ipregistry shall make reasonable efforts to identify the cause of such Data Incident and take steps as Ipregistry deems necessary and reasonable in order to remediate the cause of such a Data Incident to the extent the remediation is within Ipregistry's reasonable control. Ipregistry shall have no responsibility to you for Data Incidents caused by you or your end users.

k. Return and Deletion. Upon your written request or after the end of the Services, Ipregistry will, at your choice, return or delete Personal Information processed by Ipregistry on behalf of you. Ipregistry may retain Personal Information where applicable law requires it, and in backups, which are kept for up to one year, are used only to restore data, and are then deleted.

l. Government Requests. If a public authority requests access to Personal Information that Ipregistry processes on your behalf, Ipregistry shall notify you without undue delay unless the law prohibits it, shall challenge any request it considers unlawful, and shall disclose only what the request strictly requires.

7. International Transfers of Personal Information

a. The parties agree that in the event any transfer of Personal Information from you (as "data exporter") to Ipregistry (as "data importer") is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this Addendum, as follows:

   i. In relation to transfers of Personal Information that is protected by the GDPR and processed in accordance with Section 2(b) of this Addendum, the SCCs shall apply, completed as follows:

      A. Module Two (Transfer controller to processor) or Module Three (Transfer processor to processor) will apply (as applicable);

      B. in Clause 7, the optional docking clause will apply;

      C. in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 6(e)(ii) of this Addendum;

      D. in Clause 11, the optional language will not apply;

      E. in Clause 17, Option 1 will apply, and the SCCs will be governed by French law;

      F. in Clause 18(b), disputes shall be resolved before the courts of France;

G. Annex I of the SCCs shall be deemed completed with the information set out in Schedule 1.1 to this Addendum; and

H. Subject to section 6(i) of this Addendum, Annex II of the SCCs shall be deemed completed with the information set out in Schedule 3 to this Addendum;

ii. In relation to transfers of Personal Information protected by the GDPR and processed in accordance with Section 2(c) of this Addendum, the SCCs shall apply, completed as follows:

A. Module One (Transfer controller to controller) will apply;

B. in Clause 7, the optional docking clause will apply;

C. in Clause 11, the optional language will not apply;

D. in Clause 17, Option 1 will apply, and the SCCs will be governed by French law;

E. in Clause 18(b), disputes shall be resolved before the courts of France;

F. Annex I of the SCCs shall be deemed completed with the information set out in Schedule 1.2 to this Addendum; and

G. Annex II of the SCCs shall be deemed completed with the information set out in Schedule 3 to this Addendum;

iii. In relation to transfers of Personal Information protected by the UK GDPR, the SCCs as implemented under sub-paragraphs (i) and (ii) above will apply with the following modifications:

A. the SCCs shall be deemed amended as specified by Part 2 of the UK Addendum;

B. tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed respectively with the information set out in Schedules 1.1, 1.2 and 3 of this Addendum (as applicable); and

C. table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

iv. In relation to transfers of Personal Information protected by the Swiss DPA or LGPD, the SCCs will also apply in accordance with paragraphs (i) and (ii) above, with the following modifications:

A. references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA or LGPD (as applicable);

B. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA or LGPD (as applicable);

C. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Brazil", or "Swiss law" or "Brazilian law" (as applicable);

D. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland or Brazil from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland or Brazil);

E. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection and Information Commissioner or Brazil Data Protection Authority (as applicable);

F. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "applicable courts of Switzerland" or the "Brazil Data Protection Authority" and "courts of Brazil" (as applicable);

G. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland or Brazil (as applicable);

H. with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland; and

I. where LGPD requires the standard contractual clauses approved by the Brazilian data protection authority (ANPD), those clauses apply in place of the SCCs, and Ipregistry will sign them with you on request.

v. The parties agree that the retention periods set forth in Schedules 1.1 and 1.2 shall apply to all Personal Information transferred by you to Ipregistry under the Agreement, including without limitation Personal Information transferred from outside the EU, UK, Brazil and Switzerland and including all Personal Information submitted by you to Ipregistry prior to the effective date of this Addendum.

b. The parties agree that in the event any transfer of Personal Information from Ipregistry (as "data exporter") to you (as "data importer") is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this Addendum, as follows:

i. In relation to transfers of Personal Information protected by the GDPR and processed in accordance with Section 3 of this Addendum, the SCCs shall apply, completed as follows:

A. Module One (Transfer controller to controller) will apply;

B. in Clause 7, the optional docking clause will apply;

C. in Clause 11, the optional language will not apply;

D. in Clause 17, Option 1 will apply, and the SCCs will be governed by French law;

E. in Clause 18(b), disputes shall be resolved before the courts of France;

F. Annex I of the SCCs shall be deemed completed with the information set out in Schedule 4 to this Addendum; and

G. Annex II of the SCCs shall be deemed completed with the information set out in Schedule 5 to this Addendum;

ii. In relation to transfers of Personal Information protected by the UK GDPR, the SCCs as implemented under sub-paragraph (i) above will apply with the following modifications:

A. the SCCs shall be deemed amended as specified by Part 2 of the UK Addendum;

B. tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed respectively with the information set out in Schedules 4 and 5 of this Addendum (as applicable); and

C. table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

iii. In relation to transfers of Personal Information protected by the Swiss DPA or LGPD, the SCCs will also apply in accordance with paragraph (i) above, subject to the same modifications as described in Section 7(a)(iv).

c. If the Standard Contractual Clauses conflict with any provision of the Agreement (including this Addendum), the Standard Contractual Clauses prevail to the extent of the conflict.

d. The parties agree that in the event that any transfer of Personal Information from you to Ipregistry is subject to PIPL or other PRC laws and standards, you shall secure separate consent and/or comply with the other requirements under PIPL and other PRC laws and standards that may apply. To the extent that any transfer of Personal Information from you to Ipregistry is subject to PIPL, the purpose, period and processing method are as set forth in Schedules 1.1 and 1.2, and the security protection measures to be taken by Ipregistry are set forth in Schedule 3.

8. Execution and Entry into Force. The parties agree that this Addendum (and the Standard Contractual Clauses, as applicable) are referenced in and form an integral part of the Agreement, and execution of the Agreement shall be deemed to include execution of this Addendum and the Standard Contractual Clauses (as applicable), to the extent required by applicable law. If this Addendum conflicts with the rest of the Agreement on the processing of Personal Information, this Addendum prevails.

Schedule 1.1

Description of Processing / Transfer

Modules 2 and 3 (controller/processor to processor transfers)

A. LIST OF PARTIES

Data exporter(s):

Name:	Party identified as "you" in the Addendum
Address:	The notice address provided by you to Ipregistry
Contact person's name, position and contact details:	The contact person, their position and contact details provided by you to Ipregistry.
Activities relevant to the data transferred under these Clauses:	Providing data for the purpose of utilizing the Services.
Role:	Controller / Processor

Data importer:

Name:	Elaunira SARL
Address:	1 Chemin des Rosiers, 06800 Cagnes-sur-Mer, France
Contact person's name, position and contact details:	Laurent PELLEGRINO Managing Director legal@ipregistry.co
Activities relevant to the data transferred under these Clauses:	Providing the Services described in the Agreement. For example: ● Ipregistry API ○ Providing data relating to IP addresses and threat intelligence. ○ Providing data relating to user-agents. ○ Providing technical support for the Services, logging and backup.
Role:	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	End-users of the data exporter and those of its customers, business partners, and other third parties.
Categories of personal data transferred:	The personal data transferred is based on the products or services used pursuant to the Agreement, which may include, but are not limited to the following categories of personal data: ● Ipregistry API: IP addresses, Postal code level or less precise level geolocation data, User-agents.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	No sensitive data will be transferred.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous - the data will be transferred periodically over the term of the Agreement.
Nature of the processing:	The personal data transferred will be subject to the following basic processing activities (as applicable): ● Providing threat analysis and Internet Protocol intelligence services and products. ● Providing technical support for Ipregistry services and products. ● Providing licensed data. ● Providing support. ● Logging and backup.

Purpose(s) of the data transfer and further processing:	For purposes based on the Services used pursuant to the Agreement, including providing IP Geolocation services, threat detection, and related services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Personal data is retained only for as long as necessary to provide the Services, as described in the Ipregistry Privacy Policy (https://ipregistry.co/privacy), unless otherwise required by law. Backups are retained as set out in Section 6(k) of the Addendum.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	The Subprocessors listed in Schedule 2 process personal data to host, deliver, secure, and support the Services, for the duration of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the SCCs (where applicable):	For transfers to which the GDPR applies the competent supervisory authority will be determined in accordance with the criteria set forth in Clause 13 of the SCCs, provided that if the data exporter is not established in an EU Member State and has not appointed a representative, the French Supervisory Authority shall act as the competent supervisory authority. For transfers to which LGPD applies the competent supervisory authority is the Brazil Data Protection Authority. For transfers to which the UK GDPR applies the competent supervisory authority is the UK Information Commissioner's Office. For transfers to which the Swiss DPA applies the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

Schedule 1.2

Description of Processing / Transfer

Module 1 (controller to controller transfers)

A. LIST OF PARTIES

Data exporter(s):

Name:	Party identified as "you" in the Addendum
Address:	The notice address provided by you to Ipregistry.
Contact person's name, position and contact details:	The contact person, position, and contact details provided by you to Ipregistry.
Activities relevant to the data transferred under these Clauses:	Providing data for the purpose of utilizing the Services and allowing service improvement.
Role:	Controller

Data importer:

Name:	Elaunira SARL
Address:	1 Chemin des Rosiers, 06800 Cagnes-sur-Mer, France
Contact person's name, position and contact details:	Laurent PELLEGRINO Managing Director legal@ipregistry.co
Activities relevant to the data transferred under these Clauses:	Operation, security, billing, maintenance, and improvement of the Services
Role:	Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	End-users of the data exporter and those of its customers, business partners, and other third parties.
Categories of personal data transferred:	The personal data transferred is based on the products or services used pursuant to the Agreement, which may include, but is not limited to the following categories of personal data: ● Ipregistry API or Website: the IP address of the system calling the API; IP addresses, user-agents, and other request data in aggregated or de-identified form; account, billing, and usage data; content you send to Ipregistry.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	No sensitive data will be transferred.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous - the data will be transferred periodically over the term of the Agreement.
Nature of the processing:	Ipregistry processes personal data provided by you, including in aggregated or de-identified form and together with data received from other sources, to operate, secure, and bill the Services and to maintain and improve the Services and Ipregistry's data.
Purpose(s) of the data transfer and further processing:	For the purposes of operating, securing, billing, maintaining, and improving the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Personal data is retained for the periods described in the Ipregistry Privacy Policy (https://ipregistry.co/privacy), and for longer only where the law requires it.
For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing:	The service providers listed at https://ipregistry.co/service-providers host, secure and support Ipregistry's infrastructure, payments, communications and backups, for so long as Ipregistry retains the data.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the SCCs (where applicable):	For transfers to which the GDPR applies, the competent supervisory authority will be determined in accordance with the criteria set forth in Clause 13 of the SCCs, provided that if the data exporter is not established in an EU Member State and has not appointed a representative, the French Supervisory Authority shall act as the competent supervisory authority. For transfers to which LGPD applies the competent supervisory authority is the Brazil Data Protection Authority. For transfers to which the UK GDPR applies the competent supervisory authority is the UK Information Commissioner's Office. For transfers to which the Swiss DPA applies the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

Schedule 2

Subprocessors

The Subprocessors are the service providers shown as involved in API requests in the following list, which also gives the data they handle and the purpose of the processing:
https://ipregistry.co/service-providers

Schedule 3

Minimum Technical and Organizational Measures

Description of the technical and organizational security measures implemented by Ipregistry:

- Ipregistry maintains commercially reasonable technical and organizational measures to prevent unauthorized access, use, alteration, or disclosure of Personal Information.
- Data processing and storage services are accessible only to authorized personnel, using multi-factor authentication.
- Anyone given access to Personal Information, whether an employee or a contractor, is bound by a written confidentiality obligation.
- Access to the different environments is also controlled with SSH keys and IP-based restrictions.
- Data is backed up regularly.
- Backups of data are available for the past several days, weeks, and months.
- Backups are transferred over encrypted connections and stored encrypted at rest.
- All services have uptime monitoring to ensure availability.
- Downtime and critical issues are addressed via a prompt review that includes not just solving the issue, but also prevention of future-related issues.
- Application source code is stored in a central repository. Access to source code is limited to authorized individuals.
- All communications with the Ipregistry website and dashboard use HTTPS. The Ipregistry API supports HTTPS with TLS 1.2 or higher, and Ipregistry recommends it for all requests.

Ipregistry may update or modify such security measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

Schedule 4

Description of Processing / Transfer

Module 1 (controller to controller transfers)

A. LIST OF PARTIES

Data exporter(s):

Name:	Elaunira SARL
Address:	1 Chemin des Rosiers, 06800 Cagnes-sur-Mer, France
Contact person's name, position and contact details:	Laurent PELLEGRINO Managing Director legal@ipregistry.co
Activities relevant to the data transferred under these Clauses:	Providing the Services described in the Agreement.
Role:	Controller

Data importer(s):

Name:	Party identified as "you" in the Addendum
Address:	The notice address provided by you to Ipregistry
Contact person's name, position and contact details:	The contact person, position and contact details provided by you to Ipregistry.

Activities relevant to the data transferred under these Clauses:	Utilizing the Services described in the Agreement for the purposes described in the Agreement.
Role:	Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Individuals associated with IP Addresses supplied by Ipregistry
Categories of personal data transferred:	IP addresses, user-agents, and associated data.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	No sensitive data will be transferred.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous - the data will be transferred periodically over the term of the Agreement.
Nature of the processing:	Transmission of data to you for your purposes as permitted in the Agreement.
Purpose(s) of the data transfer and further processing:	For purposes based on the Services used pursuant to the Agreement, including providing IP Address intelligence services, fraud detection, and related services.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Data may be retained for the periods specified in the Agreement.
For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing:	N/A

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the SCCs (where applicable):	French Supervisory Authority

Schedule 5

Technical and Organizational Security Measures

Measure	Description
Measures of pseudonymisation and encryption of personal data	You will ensure that you support the following encryption measures when utilizing Ipregistry's Services: ● HTTPS encryption for data in transit, using TLS 1.2 or higher, when calling the Services and on every login interface. ● When possible, encryption of data at rest, using an industry standard algorithm such as AES-256.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	● Ensure that all account users have strong, secure passwords that are updated in line with industry standards such as NIST, or that passwordless authentication is used. ● Do not share user passwords, and deactivate any user accounts if no longer used. ● Treat your API keys like passwords, and store them securely (e.g. in a password manager) ● Logging in place for all information systems to record sufficient information to serve the operational needs, preserve accountability, and detect malicious activity.

Measures for the protection of data during transmission	● HTTPS encryption for data in transit using TLS 1.2 or higher.
Measures for the protection of data during storage	● System inputs recorded via log files ● Access Control Lists defining users who have access and what level of access, following need-to-know and least privilege principles.

Signature Page

This page is used when a signed copy of this Addendum is requested. The Addendum applies without it, as set out in Section 8. Signing this page also counts as signing the Standard Contractual Clauses, where they apply. A later revision of this Addendum applies as set out in its preamble, whether or not this page was signed.

Accepted and agreed, as of the dates below:

	Customer	**Ipregistry**
Company	_____	Elaunira SARL
Address	_____	1 Chemin des Rosiers, 06800 Cagnes-sur-Mer, France
Name	_____	Laurent Pellegrino
Title	_____	Managing Director
Date	_____	_____
Signature	_____	_____