IPDATA: STANDARD CONTRACTUAL CLAUSES

Capitalized terms used but not defined in these Clauses (including the Appendix) have the meanings given to them in the agreement into which these Clauses are incorporated (the "Agreement") or in these recitals. For the purposes of these Clauses, "Customer" shall mean any person or entity that uses or retains the services of Ipdata LLC, which includes the provision of IP related information, as more specifically described in the Agreement (the "Services").

SECTION I

CLAUSE 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

CLAUSE 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

CLAUSE 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

CLAUSE 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

CLAUSE 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

CLAUSE 7 – *Not used*

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach').

In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

CLAUSE 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (14) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

CLAUSE 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

CLAUSE 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data

subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

CLAUSE 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

CLAUSE 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

CLAUSE 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

CLAUSE 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter: [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: Customer

Address: As specified in the Agreement

Contact person's name, position and contact details: Contact details for the data exporter and its/their data protection officer or representative in the European Union are specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement.

Signature and date: The parties agree that execution of the Agreement shall constitute execution of these Clauses by both parties.

Role: Controller

Data importer:

Name: Ipdata LLC

Address: 2035 Sunset Lake Road Suite B-2, Newark, Delaware 19702

Contact person’s name, position and contact details: Jonathan Kosgei, Owner; jonathan@ipdata.co

Activities relevant to the data transferred under these Clauses: The data importer processes data for the data exporter in order to perform the Services.

Signature and date: The parties agree that execution of the Agreement shall constitute execution of these Clauses by both parties.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Data subjects include the individuals about whom data is provided via the Services by (or at the direction of) the data exporter.

Categories of personal data transferred

- Contact information, including name, address, email address, and telephone number.
- Authentication information, including the user name and password used to register an account on ipdata.co.
- Financial information, including debit or credit card number, its expiration date, and its security code, for payment processing purposes
- Comments, reviews, and suggestions via customer surveys, Ipdata message platforms, or email.
- Online behavior information including online activity, preferences, and time spent viewing features.
- IP address and geolocation data, mobile network information, proxy and VPN related information, usage type data, or device information.

The frequency of the transfer

- To effectuate the Services, personal data may be transferred on a continuous basis until it is deleted.

Nature of the processing

- The data importer will process personal data to provide, secure, and manage the Services and, specifically, to provide Customers information related to IP addresses, including the approximate locations of said IP addresses.

Purpose(s) of the data transfer and further processing

- The data importer will process personal data to provide, secure, and manage the Services and, specifically, to provide Customers information related to IP addresses, including the approximate locations of said IP addresses.

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 shall be retained for the duration of the Agreement or until such data is deleted.

For transfers to sub-processors, also specify subject matter, nature, and duration of the processing

The subject matter and duration of transfers to sub-processors are as described above. The nature of such transfers are described below.

1. Amazon Simple Email Service (SES)

- Managing contacts and sending messages – SES makes it possible to manage a database of email contacts, phone contacts or any other contact information to communicate with users. These services may also collect data concerning the date and time when the message was viewed by a user, as well as when a user interacted with it, such as by clicking on links included in the message.

2. Amazon Web Services

- Hosting and backend infrastructure – AWS has the purpose of hosting data and files that enable ipdata.co to run and be distributed as well as to provide a ready-made infrastructure to run specific features or parts of ipdata.co. Some of these services work through geographically distributed servers, making it difficult to determine the actual location where personal data is stored.

3. Clearbit

- Customer Intelligence – Clearbit collects marketing data to enable ipdata.co to understand its customers and manage marketing and sales interactions.

4. Google Analytics

- Analytics – Google Analytics is a web analysis service provided by Google LLC ("Google"). Google utilizes the data collected to track and examine the use of ipdata.co to prepare reports on its activities and share them with other Google services. Google may use the data collected to contextualize and personalize the ads of its own advertising network.

5. Google Optimize

- Content performance and features testing – Google Optimize allows ipdata.co to track and analyze the user response concerning web traffic or behavior regarding changes to the structure, text or any other component of ipdata.co. Google may use the data collected to contextualize and personalize the ads of its own advertising network.

6. Google Tag Manager

- Tag management – Google Tag Manager helps the ipdata.co to manage the tags or scripts needed on ipdata.co in a centralized fashion. This results in users' data flowing through these services, potentially resulting in the retention of this data.

5. Intercom

- User database management – Intercom allows ipdata.co to build user profiles by starting from an email address, a personal name, or other information that a user provides to ipdata.co, as well as to track user activities through analytics features. This personal data may also be matched with publicly available information about the user (such as social networks' profiles) and used to build private profiles that ipdata.co can display and use for improving ipdata.co. Some of these services may also enable the sending of timed messages to the user, such as emails based on specific actions performed on ipdata.co.

6. Sentry

- Infrastructure monitoring – Sentry allows ipdata.co to monitor the use and behavior of its components so its performance, operation, maintenance and troubleshooting can be improved. Which personal data are processed depends on the characteristics and mode of implementation of these services, whose function is to filter the activities of ipdata.co.

7. Stripe

    - Payment processing – Stripe enables ipdata.co to process payments by credit card, bank transfer or other means. To ensure greater security, ipdata.co shares only the information necessary to execute the transaction with the financial intermediaries handling the transaction. Some of these services may also enable the sending of timed messages to users, such as emails containing invoices or notifications concerning the payment.

10. Sendgrid

    - Customer communications and engagement – Sendgrid enables ipdata.co to communicate with customers by email and manage marketing campaigns and other customer transactions.

11. ClickHouse

    - Analytics and monitoring – ClickHouse enables ipdata.co to monitor the use and behavior of its components so its performance, operation, maintenance and troubleshooting can be improved. Which personal data are processed depends on the characteristics and mode of implementation of these services, whose function is to filter the activities of ipdata.co.

12. ProfitWell

    - Subscription management – ProfitWell enables ipdata.co to measure and automate its subscription growth.

13. Cohere

    - Infrastructure management – Cohere enables ipdata.co to utilize artificial intelligence to manage and generate content, such as product descriptions, blog posts, articles, and marketing copies; extract concise, accurate summaries of articles, emails, and documents; build text searches; and run text classification for customer support routing, intent recognition, and sentiment analysis.

14. SatisMeter

    - Customer support – SatisMeter enables ipdata.co to survey customers and collect customer feedback in order to support said customers and ensure ipdata.co is providing its services satisfactorily.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority is the authority identified by the data exporter as its competent supervisory in the Agreement.

Examples of competent supervisory authorities include:

- Australia: Office of the Australian Information Commissioner
- Brazil: National Data Protection Authority (ANPD)
- Canada: Office of the Privacy Commissioner of Canada
- Germany: Federal Commissioner for Data Protection and Freedom of Information (BfDI)
- Korea: Personal Information Protection Commission
- Switzerland: Federal Data Protection and Information Commissioner (FDPIC)
- United Kingdom: Information Commissioner's Office

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

I. GENERAL SECURITY MEASURES

1. The data importer maintains security documentation and supervises compliance with the rules therein.

2. The data importer ensures that persons authorized to process personal data are familiar with data protection rules (e.g. by training).

3. Only persons who are granted authorization by applicable database managers shall be allowed to carry out data processing ("Authorized Person").

4. Database managers shall identify Authorized Persons upon granting access to a database.

5. The data importer shall ensure that Authorized Persons are obliged to keep personal data and the methods of their protection confidential.

II. DOCUMENTATION

1. The data importer shall keep and maintain written documentation regarding data security principles.

2. The documentation that is kept by the data importer consists of: (1) the Security Policy and (2) internal manuals setting out how to use the IT systems and how to secure data (the "IT Manuals").

III. SPECIFIC SECURITY MEASURES

1. The data importer shall ensure that:

    a. Buildings, premises, or parts comprising the area where data are processed are secured against access of unauthorized persons;

    b. Any unauthorized person may have access to the area where personal data is processed only with the data importer's consent, or in the presence of an Authorized Person;

    c. Access control principles are applied in the IT system used for personal data processing;

    d. A separate unique identifier (ID) is registered for each IT system user, so that an authentication procedure may be completed;

    e. The policies provided to the Authorized Persons shall instruct Authorized Persons to take such precautions as may be necessary to ensure that the confidential component(s) (including the login credentials (e.g. identifier/username)) are kept

secret and that the devices used and held exclusively by Authorized Persons are kept with due care;

f. Access to personal data is only be available after entering the Authorized Person's login credentials (e.g. identifier/username and password);

g. The IT system used for processing personal data is secured in particular against:

   i. software used for gaining unauthorized access to the IT system;

   ii. loss of data which may be caused by a failure of power supply or line interference.

h. Upon notification by a system or database manager that an Authorized Person no longer has a need to access the relevant data or system, authentication credentials for such Authorized Person shall be de-activated.

i. Passwords for user authentication are changed at least once every ninety (90) days and consist of at least eight characters, including small and capital letters, numbers and special characters;

j. Personal data being processed within the IT system are secured by making back-ups of the data filing systems, which ensures that:

   i. Data is kept secure against any unauthorized takeover, change, damage or destruction;

   ii. Data is deleted as soon as there is no business need to keep such data; and

   iii. back-ups are carried out at a frequency and complexity necessary to ensure the availability of such systems, including daily backups where appropriate.

k. Appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data importer can ensure that data or electronic equipment are available in case the Authorized Person is either absent or unavailable for a long time and it is not possible to carry out certain data processing activities without further delay.

l. The data importer shall take measures to ensure that personal data is encrypted per data importer policies and cannot be read, copied, modified or removed without authorization, and that it is possible to check and establish to which parties the transfer of personal data by means of electronic transmission is envisaged. Where data importer-issued laptops are used to process personal data, special care is taken when the device is transported, stored or used, including cryptographic protection measures (such as encryption);

m. The data importer shall take measures to ensure that unused removable media containing personal data are destroyed or made unusable; alternatively, they may be re-used for another purpose provided that the data contained in them is not intelligible and cannot be re-constructed by any technical means. In case of the event of repairs or servicing, the data should be protected or removed before such activity is carried out.

n. it supervises the implementation and maintenance of security measures within the IT system;

o. the IT system used for processing personal data is secured against any dangers originating from the Internet by physical and logical security measures protecting against any unauthorized access (e.g. firewalls). In particular, the data importer shall protect sensitive data or data related to criminal offense and proceedings against unauthorized access by implementing appropriate measures; and

p. Cryptographic protection measures (e.g. encryption) are applied per data importer policies.

2. Where personal data is intended to be made publicly available, the provisions concerning the authentication process (set out above) shall not apply to the processing of such personal data. In any case, the importer shall ensure that health data, where processed, will not be publicly disseminated.

3. The data importer shall take measures to review data processing activities and the access levels given to Authorized Persons.

4. The data importer shall protect personal data against the risk of intrusion and the effects of malware by implementing suitable security measures, updated at least every six months.

5. The data importer shall carry out, at least annually, the regular update of computer programs aimed at preventing vulnerability and removing flaws (e.g. bugs). If sensitive data or data related to criminal offenses and proceedings are processed, the data importer shall carry out such update out at least every six months.

6. If either the personal data or means of protecting the personal data have been damaged, the data importer shall adopt suitable measures to ensure that personal data access is restored within a specific period, which is compatible with data subjects' rights and not in excess of seven days.

7. Where the data importer provides or procures the provision of IT services to the Controller (which consists of managing the Controller's databases or IT systems), the data importer shall appoint, in writing, a system administrator who oversees such activities. A list of the system administrators shall be kept by the data importer for inspection by the Controller on request. The system administrators will be required to monitor access to the Controller's systems and keep a copy of log/access files for 6 months. The data importer shall, on (at least) an annual basis, conduct an assessment on the activities of the system administrator.

8. Where personal data may – in accordance with this agreement – be processed by a sub-processor, the data importer shall take reasonable measures to ensure that the data are processed strictly in accordance with its / the Controller's instructions.

9. The data importer shall take adequate measures to ensure that any personal data that have been collected for different purposes can be processed separately

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Amazon Simple Email Service (SES)

    i. Address:
    Amazon Web Service, Inc.
    410 Terry Ave N
    Seattle, Washington 98109

    ii. Contact person's name, position and contact details: The contact person is the Data Protection Officer of the sub-processor, who may be reached at the above address.

    iii. Description of processing: Managing contacts and sending messages – SES makes it possible to manage a database of email contacts, phone contacts or any other contact information to communicate with users. SES may also collect data concerning the date and time when the message was viewed by a user, as well as when a user interacted with it, such as by clicking on links included in the message.

2. Amazon Web Services (AWS)

    i. Address:
    Amazon Web Service, Inc.
    410 Terry Ave N
    Seattle, Washington 98109

    ii. Contact person's name, position and contact details: The contact person is the Data Protection Officer of the sub-processor, who may be reached at the above address.

    iii. Description of processing: Hosting and backend infrastructure – AWS has the purpose of hosting data and files that enable ipdata.co to run and be distributed as well as to provide a ready-made infrastructure to run specific features or parts of ipdata.co. Some of these services work through geographically distributed servers, making it difficult to determine the actual location where personal data is stored.

3. Clearbit

    i. Address:
    APIHub, Inc. d/b/a Clearbit

90 Sheridan St.
San Francisco, California 94103

ii. Contact person's name, position and contact details: The contact person is the Data Protection Officer of the sub-processor, who may be reached at the above address.

iii. Description of processing:
Clearbit collects marketing data to enable ipdata.co to understand its customers and manage marketing and sales interactions.

4. Google Analytics

i. Address:
Google LLC
1600 Amphitheatre Parkway
Mountain View, California 94043

ii. Contact person's name, position and contact details: Emil Ochotta, the Data Protection Officer of the sub-processor, may be reached at the address above.

iii. Description of processing: Google Analytics is a web analysis service provided by Google LLC ("Google"). Google utilizes the data collected to track and examine the use of ipdata.co to prepare reports on its activities and share them with other Google services. Google may use the data collected to contextualize and personalize the ads of its own advertising network.

5. Google Optimize

i. Address:
Google LLC
1600 Amphitheatre Parkway
Mountain View, California 94043

ii. Contact person's name, position and contact details: Emil Ochotta, the Data Protection Officer of the sub-processor, may be reached at the address above.

iii. Description of processing: Content performance and features testing – Google Optimize allows ipdata.co to track and analyze the user response concerning web traffic or behavior regarding changes to the structure, text or any other component of ipdata.co. Google may use the data collected to contextualize and personalize the ads of its own advertising network.

6. Google Tag Manager

i. Address:
Google LLC
1600 Amphitheatre Parkway
Mountain View, California 94043

ii. Contact person's name, position and contact details: Emil Ochotta, the Data Protection Officer of the sub-processor, may be reached at the address above.

iii. Description of processing: Tag management – Google Tag Manager helps the ipdata.co to manage the tags or scripts needed on ipdata.co in a centralized fashion. This results in users' data flowing through these services, potentially resulting in the retention of this data.

7. Intercom

i. Address:
Intercom Inc.
55 2nd Street, 4th Fl.
San Francisco, California 94105

ii. Contact person's name, position and contact details: The contact person is the Data Protection Officer of the sub-processor, who may be reached at legal@intercom.com

iii. Description of processing: User database management – Intercom allows ipdata.co to build user profiles by starting from an email address, a personal name, or other information that a user provides to ipdata.co, as well as to track user activities through analytics features. This personal data may also be matched with publicly available information about the user (such as social networks' profiles) and used to build private profiles that ipdata.co can display and use for improving ipdata.co. Some of these services may also enable the sending of timed messages to the user, such as emails based on specific actions performed on ipdata.co.

8. Sentry

i. Address:
Functional Software, Inc. d/b/a Sentry
45 Fremont Street, 8th Floor
San Francisco, CA 94105

ii. Contact person's name, position and contact details: The contact person is the Data Protection Officer of the sub-processor, who may be reached at compliance@sentry.io.

iii. Description of processing: Infrastructure monitoring: Sentry allows ipdata.co to monitor the use and behavior of its components so its performance, operation, maintenance and troubleshooting can be improved. Which personal data are processed depends on the characteristics and mode of implementation of these services, whose function is to filter the activities of ipdata.co.

9. Stripe

i. Address:
Stripe, Inc.
510 Townsend Street
San Francisco, CA 94103, USA
Attention: Stripe Legal

ii. Contact person's name, position and contact details: The contact person is the Data Protection Officer of the sub-processor, who may be reached at dpo@stripe.com.

iii. Description of processing: Payment processing – Stripe enables ipdata.co to process payments by credit card, bank transfer or other means. To ensure greater security, ipdata.co shares only the information necessary to execute the transaction with the financial intermediaries handling the transaction. Some of these services may also enable the sending of timed messages to users, such as emails containing invoices or notifications concerning the payment.

10. Sendgrid (owned by Twilio)

i. Address:
Twilio Inc.
801 California St., Suite 500
Denver, CO 80202, USA

ii. Contact person's name, position and contact details: The contact person is the Data Protection Officer of the sub-processor, who may be reached at dpo@sendgrid.com.

iii. Description of processing: Customer communications and engagement – Sendgrid enables ipdata.co to communicate with customers by email and manage marketing campaigns and other customer transactions.

11. ClickHouse

i. Address:
ClickHouse, Inc.
Attn: Privacy Practice Group

50 Castro St. Ste. 120 Unit 92426
Mountain View, CA 94041, USA

ii. Contact person's name, position and contact details: The Privacy Practice Group of the sub-processor may be reached at privacy@clickhouse.com.

iii. Description of processing: Analytics and monitoring – ClickHouse enables ipdata.co to monitor the use and behavior of its components so its performance, operation, maintenance and troubleshooting can be improved. Which personal data are processed depends on the characteristics and mode of implementation of these services, whose function is to filter the activities of ipdata.co.

12. ProfitWell (owned by Paddle)

i. Address:
Paddle.com Inc.
3811 Ditmars Blvd, #1071 Astoria
New York, 11105-1803, USA

ii. Contact person's name, position and contact details: The sub-processor contact may be reached at privacy@paddle.com.

iii. Description of processing: Subscription management – ProfitWell enables ipdata.co to measure and automate its subscription growth.

13. Cohere

i. Address:
Cohere Inc.
171 John Street, Suite 200
Toronto, Ontario M5T 1X3, Canada

ii. Contact person's name, position and contact details: The Privacy Officer of the sub-processor may be reached at privacy@cohere.ai.

iii. Description of processing: Infrastructure management – Cohere enables ipdata.co to utilize artificial intelligence to manage the generate content, such as product descriptions, blog posts, articles, and marketing copies; extract concise, accurate summaries of articles, emails, and documents; build text searches; and run text classification for customer support routing, intent recognition, and sentiment analysis.

14. SatisMeter

i. Address:
SatisMeter s.r.o.

Česká 1113/1, Prague 5, 158 00, Czech Republic

ii. Contact person's name, position and contact details: The Data Protection Officer of the sub-processor may be reached at support@SatisMeter.com or by mail to SatisMeter s.r.o., Data Protection Officer, Česká 1113/1, Prague 5, 158 00, Czech Republic.

iii. Customer support – SatisMeter enables ipdata.co to survey customers and collect customer feedback in order to support said customers and ensure ipdata.co is providing its services satisfactorily.