Data Processing Agreement Addendum

Note that Appendix A is only relevant where non-EU data transfers are given

Agreement on contract data processing on behalf according to Art. 28 General Data Protection Regulation (GDPR)

Agreement entered into by and between

Customer
– Controller – referred to hereinafter as "Controller" –

and

A2 Hosting, Inc.
PO BOX 2998
Ann Arbor, MI, 48106, USA
– Processor – referred to hereinafter as "Processor" –

Preamble

This agreement defines and sets out in detail the data protection obligations of the contracting parties arising under the contract data processing on behalf as described in the reseller agreement ("Main Contract") with us. It applies to all activities relating to the said Main Contract where employees of the Processor or other persons or parties engaged by the Processor may encounter personal data of the Controller.

§ 1 Subject matter, term and specification of the contract data processing on behalf

(1) The aforesaid Main Contract specifies the subject matter and the term of the agreed contract data processing on behalf as well as the scope and nature of data collection, data processing and use of data. In particular, the following data will be processed:

Kind of data	**Purpose of the collection, processing and use of the data**	**Data subjects**

Registration data, e.g. data on the Registrant, Admin-C, Tech-C and Billing-C,Admin-C, Tech-C and Billing-C, Customer data, Traffic and communication data, billing and payment data	Registration of domain names and maintaining the registrations, hosting services, SSL certificates, hosting related services	Customers, Employee data

The term and termination of this agreement is dependent on the term and termination agreed in the main contract. Termination of the main contract automatically brings about the termination of the present agreement. It is not possible to terminate the present agreement separately.

(2) Where personal data is transferred to a third country or an international organisation where the adequacy requirement is not fulfilled (Art. 45 (3) GDPR) the transfer of personal data according to this agreement takes place based on standard clauses as attached in **Appendix A**. Where there are inconsistencies between this agreement and the standard clauses, the standard clauses shall prevail. Should the European Commission issue new standard clauses, the parties are obliged to make these part of this agreement.

§ 2 Scope of application and responsibility

(1) The Processor processes personal data on behalf of the Controller. This includes all activities specified in the contract and in the performance specifications. The Controller is solely responsible under this agreement for compliance with the statutory provisions in the applicable data protection and data privacy laws, in particular for ensuring the lawfulness of any disclosure or passing on of data to the Processor as well as for the lawfulness of data processing ("controller" within the meaning of Art. 4 no. 7 GDPR).

(2) The instructions are initially fixed in the contract and may subsequently be changed or modified or amended or replaced by specific individual instructions (individual instruction) in writing or in text form. Instructions which go beyond the contractually agreed services are treated as requests for a change of performance. Oral instructions must be confirmed in writing or in text form without undue delay.

(3) If the Processor is of the opinion that a permissible individual instruction is contrary to the applicable data protection or privacy law, it will inform the Controller to that effect as soon as possible. The Processor is entitled to suspend the implementation of the appropriate instruction until it is confirmed or adjusted by the Controller.

§ 3 Processor's duties

(1) The Processor may correct, adjust, cancel or restrict the processing of data that is processed under the contract only on, and in accordance with, a properly documented instruction given by the Controller. If and to the extent that, in this respect, a data subject contacts the Processor directly, the Processor will pass this request on to the Controller without undue delay.

(2) The Processor represents and warrants that it will comply with its duties under Art. 28 to 33 GDPR including but not limited to

a. the duty to appoint a data protection officer where prescribed by law.

b. Confidentiality according to Art. 28 subs. 3 b), 29, 32 subs.4 GDPR

The Processor will only engage employees in the performance of the services who have been committed to confidentiality and had been made familiar with the data protection and privacy regulations which are relevant for their work beforehand. The Processor as well as any person subordinated to it who has access to personal data may process this data exclusively in accordance with the instructions given by the Controller, including the powers and authorizations granted in this agreement, unless they are obliged by law to process the data. Data secrecy has to be maintained even after the termination of the contract.

c. Information on control measures and other measures taken by regulatory authorities must be given to the Controller without undue delay, if and to the extent such measures relate to this contract. This also applies if and to the extent that a competent authority conducts investigations in the context of proceedings for administrative or criminal offences regarding the processing of personal data in the context of contract data processing by the Processor on behalf of the Controller.

d. If and to the extent that the Controller itself is exposed to control measures by the regulatory authority or to proceedings for administrative or criminal offences or to a claim for information or a liability claim asserted against the Controller by a data subject or a third party or to any other claims relating to the contract data processing by the Processor on behalf of the Controller, the Processor will be obliged to use its best endeavours to support and assist the Controller.

e. Controller and Processor, upon request, will cooperate with the regulatory authority and help to perform the authority's responsibilities.

f. The Processor regularly controls the internal processes as well as the technical and organizational measures to ensure that the processing performed under its responsibility is in conformity with the requirements of the applicable data protection and privacy law and that the rights of the data subject are protected.

(3) The Processor will correct, adjust, cancel or block the data to be processed under the contract upon appropriate request by the Controller. The Processor will destroy data media, data carriers and other material in accordance with data protection and privacy law upon an appropriate specific

request by the Controller unless the parties have already agreed to that effect in the contract. In special cases to be specified by the Controller, the said material will be retained or handed over to the Controller.

(4) Upon request by the Controller, data, data media or carriers and any other material must be either returned or deleted after the termination of the contract.

§ 4 Technical and organizational measures

(1) The Processor, prior to the commencement of the data processing, is obliged to document the implementation of the required technical and organizational measures which have been defined and specified in the run-up to the contract award, in particular as regards the details of the specific contract execution, and is obliged to hand over such documentation to the Controller for inspection/ audit, see **Annex B**. If the Controller accepts the documentation, the documented measures will be treated and considered as the basis for the contract (**Annex B**). If and to the extent the inspection/ audit by the Controller reveals the need for adjustment, such an adjustment will be implemented by mutual agreement.

(2) The Processor is obliged to ensure the security of processing according to Art. 28 subs. 3 c), 32 GDPR, especially in combination with Art. 5 GDPR. All in all, the measures to be taken are data security measures and measures to ensure a security level appropriate to the existing risks as regards confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the varying likelihood of realization of the risk and the severity of the risk endangering the natural persons' rights and freedoms within the meaning of Art. 32 subs. 1 GDPR must be taken into account [for details see **Annex B**].

(3) The technical and organizational measures are subject to technical progress and further development. With regard to this, the Processor is allowed to implement alternative appropriate measures. The Processor is however not allowed to fall below the security level defined for the agreed measures. Essential changes must be documented.

§ 5 Controller's duties

(1) The Controller is responsible for the lawfulness of the collection, processing and use of the Controller's data as well as for the protection of the rights of the data subjects.

(2) The Controller is the owner of the Controller's data and the owner of the rights, if any, relating to the Controller's data.

(3) It is the responsibility of the Controller to provide the Processor with the Controller's data in due time to enable service provision as agreed in the main contract and the Controller is responsible for the quality of the Controller's data. The Controller is obliged to inform the Processor comprehensively and without undue delay of any failures, errors or irregularities which the Controller has found when auditing the Processor's work results as regards compliance with the data protection and privacy regulations or with the Controller's instructions.

§ 6 Control duties

(1) The Controller, prior to the commencement of data processing and at regular intervals thereafter, assures itself that the Processor complies with its duties under Art. 28 GDPR and in particular takes all required technical and organizational measures and documents the results.
- For such purpose, the Controller may – for instance – request information from the Processor,
- or, which may regularly only be done after mutual agreement with the Processor in due time and during usual business hours without causing an impairment of the Processor's business operations, conduct an audit either by itself or through an external expert provided the latter is not a competitor of the Processor.

(2) The Processor undertakes to provide the Controller, upon written request and within a reasonable period, with all information and evidence required for carrying out the control.

(3) The Processor is entitled, in its sole discretion and in consideration of the statutory obligations of the Controller, to refuse the disclosure of any information which is critical with regard to the Processor's business or where the disclosure of such information would constitute a violation of statutory or contractual regulations. The Controller must not be granted access to data or information about other customers of the Processor or access to information regarding the costs – unless such information constitutes the basis for the reimbursable or transitory expenses -, to quality assurance and contract management reports or to any other confidential data of the Processor which is not of direct relevance for the agreed control purposes.

(4) The Controller is obliged to inform the Processor in due time (as a rule at least two weeks in advance) of all circumstances related to the implementation of the control procedure. The Controller, as a rule, is not allowed to carry out more than one control per calendar year. This is without prejudice to the Controller's right to carry out additional controls in the case of special occurrences.

(5) If the Controller engages a third party to carry out the control, the Controller is obliged to create a commitment of such third party in writing which corresponds to the Controller's commitment to the Processor under this § 6. In addition, the Controller is obliged to commit the third party to confidentiality and secrecy unless the third party in question is bound to professional secrecy. The Controller, upon the Processor's request, is obliged to submit to the Processor the appropriate agreements concluded with the third party without undue delay. The Controller is not entitled to engage competitors of the Processor to carry out the controls.

(6) The Processor, at its choice and instead of an on-site control, may also evidence compliance with the technical and organizational measures according to **Annex B** by submitting proof of compliance with authorized rules of conduct according to Art. 40 GDPR or by submitting an appropriate current certificate or reports or extracts from reports issued by independent bodies (e.g. auditor, controller, data protection officer, IT security department, data protection auditors or quality auditors) or by submitting an appropriate certificate, such as a certificate according to Art. 42 GDPR, obtained in an IT security or data protection audit, provided that the audit report enables the Controller to reasonably satisfy itself that the technical and organizational measures according to **Annex B** to this agreement are duly implemented and complied with.

§ 7 Sub-Processors

(1) The Controller agrees that the Processor, for performing the contractually agreed services to be provided by it, involves companies affiliated with the Processor to perform the services resp. engages companies as Sub-Processors to perform the agreed services. The Processor will carefully select the Sub-Processors by their qualification and suitability.

(2) The Processor is allowed to engage Sub-Processors and/or change existing Sub-Processors if and to the extent that
- the Processor notifies the Controller of the intended sub-contracting/ outsourcing in writing or text form in due time before,
- the Controller does not object for good cause to the intended sub-contracting/ outsourcing by appropriate notice to the Processor issued in writing or in text form within a period of two weeks from receipt of the said notice;
- the sub-contracting is based on a contractual agreement according to Art. 28 subs. 2 – 4 GDPR.

(3) Only after all conditions for the sub-contracting have been fulfilled, the Processor will be allowed to disclose personal data of the Controller to the Sub-Processor and the Sub-Processor will be allowed to provide the agreed services for the first time.

(4) As of the time of conclusion of this agreement, the companies listed in **Annex C** are currently engaged by the Processor as Sub-Processors to perform parts of the services to be provided and, in this context, they also directly process and/or use the data of the Controller. The Controller hereby consents to the engagement of these Sub-Processors.

(5) Any further sub-contracting/ outsourcing by the Sub-Processor requires explicit consent by the Controller; all contractual regulations and obligations in the contract chain must also be imposed on any further Sub-Processors.

(6) If the Processor engages Sub-Processors, the Processor is responsible for imposing on the Sub-Processor the same duties which the Processor has under the present agreement with regard to data protection and privacy law.

(7) Sub-contracting does not require consent by the Controller if the Processor engages third parties for the purposes of ancillary services related to the main services such as in the case of external personnel, postal and dispatch services, maintenance or user service. The Processor will conclude agreements with such third parties to the extent required to ensure adequate data protection and privacy and data security and to enable control measures.

§ 8 Notification of breaches by the Processor

The Processor supports and assists the Controller in complying with the duties under Articles 32 to 36 GDPR to ensure the security of personal data, the duty to report any data breaches as well as in the data protection impact assessment and in prior consultations. This includes among other things

a. Ensuring adequate security standards by technical and organizational measures which take into account the circumstances and purposes of data processing as well as the anticipated likelihood and severity of a possible breach or violation of rights due to security holes and which enable immediate ascertainment of relevant breaches or violations;
b. Obligation to report any breach of personal data to the Controller without undue delay;
c. Obligation to support and assist the Controller as regards its duty to inform the data subjects and, in this context, provide the Controller with all relevant information with undue delay;
d. Supporting and assisting the Controller in assessing the data protection impact;
e. Supporting and assisting the Controller in prior consultations with the regulatory authority.

§ 9 Deletion and return of personal data

(1) No copies or duplicates will be generated without the knowledge or an appropriate instruction by the Controller. This does not apply to back-up copies if and to the extent they are required to

ensure proper data processing nor to data which is required for the purposes of compliance with statutory retention duties.

(2) The Processor, no later than upon termination of the Main Contract or, as the case may be, already upon completion of the contractually agreed services or upon request by the Controller, returns and hands over to the Controller all documents, results generated by the Processor in processing and/or using data as well as all data and databases relating to the contract which are in the Processor's possession. Alternatively, upon request by the Controller, the data may be destroyed in accordance with the applicable data protection requirements. The same applies to test material and rejects. The deletion report must be submitted to the Controller upon request.

(3) Any evidence and documentation which is meant to evidence proper data processing in accordance with the contractual and other applicable requirements must be retained by the Processor even beyond the end of the contract for the applicable retention period. The Processor, to relief itself, may hand over such evidence and documentation to the Controller upon termination of the contract.

§ 10 Information duties, written form clause, choice of law

(1) If the data of the Controller should be endangered by any seizure or attachment of the Processor's property or by insolvency or composition proceedings or other events or measures taken by third parties, the Processor will be obliged to inform the Controller without undue delay. The Processor will inform all responsible persons and bodies without undue delay to the effect that the Controller is the sole owner of and has exclusive responsibility for and control over the data.

(2) Changes and amendments to this Annex or any parts thereof – including any representations and warranties of the Processor – require an appropriate written agreement as well as explicit reference to the fact that the change or amendment in question refers to the present agreement. This also applies in the case of a waiver of this formal requirement.

(3) In the case of discrepancies or conflicts, the provisions contained in this Annex governing data protection and privacy take precedence over the provisions of the contract. If any individual parts of this Annex should be invalid, this will be without prejudice to the validity of the remaining provisions of the Annex.

ANNEX A - Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data importing organisation:

A2 Hosting, Inc.

PO BOX 2998

Ann Arbor, MI, 48106, USA

Address:

Tel.: +1 734 222 4678 ; e-mail: a2privacy@a2hosting.com

(the data **Importer**)

and the Customer

(the data **Exporter**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent,

unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in **Appendix B** before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by

contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses [1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely German law.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

---

[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data importer

The data exporter is (please specify briefly your activities relevant to the transfer):

Domain Name Registrar, SSL, Hosting Company and related services

Data exporter

The data importer is (please specify briefly activities relevant to the transfer):

Hosting Customer, Domain Name Registrant, SSL Registrant and related services customer

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Customers, Employees

Categories of data

The personal data transferred concern the following categories of data (please specify):

Registration data, e.g.. data on the Registrant, Admin-C, Tech-C and Billing-C,

Customer data, Traffic and communication data, billing and payment da, Website content

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Domain Name Registrations, Transmission of data to the Registry, Provision of related services, Publication of data via Whois services, Hosting, SSL certificates

Annex B – Technical and organizational measures

1. Confidentiality (Art. 32 subs. 1 b) GDPR)

- Physical access control

Office: Door Locking Devices, no unauthorized access to data processing systems, entry controls.
Data Center: Key-Cards with pin numbers, video surveillance, alarm systems

- Logical access control

Codes and passwords, automatic blocking systems, encryption of storage devices, firewalls, access control via certificates

- Data access control

Authorization concepts and data access authorization according to the actual needs, documentation of data accesses by logs, VPN access, encryption of backups

- Data separation control

Multi-tenancy systems, sand boxing, separation of test and production system

2. Integrity (Art. 32 subs. 1 b) GDPR)

- Data transfer control

Encryption, Virtual Private Networks (VPN), electronic signature.

- Data entry control

Logging, documents management.

3. Availability and resilience (Art. 32 subs. 1 b) GDPR)

- Availability control

Back-up strategy (online/ offline; on-site/ off-site), uninterruptible power supply (UPS), antivirus protection, firewall, report chains and emergency plans, redundant carriers in the data center.

- Quick restoration of availability (Art. 32 subs. 1 c) GDPR);
  Backups are stored in different locations and can be restored according to a recovery plan

4. Processes for regular testing, assessment and evaluation (Art. 32 subs. 1 d) GDPR; Art. 25 subs. 1 GDPR)

- Data protection management;
- Incident Response Management;

- Implementation of presettings which enable effective data protection (Art. 25 subs. 2 GDPR);
- Contract execution control

No contract data processing on behalf within the meaning of Art. 28 GDPR without appropriate instructions by the Controller, e.g. unambiguously drafted contracts, formalized contract management, strict selection of the service provider, duty to check proper execution in advance, subsequent controls.

Annex C – Sub-Processors engaged by the Processor

2Checkout

Automattic JetPack

Basekit

CCAvenue

CloudFlare

eNom

GetResponse

Global Sign

Google Analytics

Hotjar

MailChannnels

MaxMind

PayPal

PayU

Skrill

Stripe

Sucuri

SurveyMonkey

The SSL Store

Zapier