Appendix 6

Data Processing Agreement

Global version – April 2021

Data Processing Agreement

This Data Processing Agreement is an integral part of the agreements between the Customer (hereinafter ‘the Controller’) and i3D.net (hereinafter ‘the Processor’).

Article 1. Definitions
1.1 In this Data Processing Agreement, the following definitions are used, both singular and plural.
Controller: a natural or legal person, public authority, agency or other body that, alone or together with others, determines the purposes and means of the processing of Personal Data.
Personal Data: Personal Data (as defined by the GDPR) relating to the Controller or its staff, clients and/or other contacts.
Processor: the legal entity that processes Personal Data on behalf of the Controller.
Subprocessor: a legal entity or person, not being a member of the Processor’s staff, who is or will be engaged by the Processor for the purpose of providing products or services to the Controller on the Processor’s behalf, for which purpose the engaged person or entity may receive or have access to Personal Data.
Standard Contractual Clauses” or sometimes also referred to the “EU Model Clauses” means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix C.

Article 2. Purposes of data processing operations
2.1. The Processor commits to the processing of Personal Data on the instructions of the Controller, subject to the conditions of this Data Processing Agreement. The data will only be processed for the purpose of storing data of the Controller in the 'cloud', the related online services, network services, colocation and those purposes that can be reasonably associated with it or will be determined by mutual agreement.
2.2. The Controller will decide which types of Personal Data it requires the Processor to process and therefore also to which (categories of) data subjects the Personal Data relate. The Processor exerts no influence on this decision. This relates in any case to Personal Data of customers of the Controller, and staff of the Controller, that are stored by the Controller at the Processor. The Processor will refrain from using the Personal Data for any purpose other than that determined by the Controller. The Controller will inform the Processor of the purposes of the processing where these are not already stated in this Data Processing Agreement.
2.3. The Personal Data to be processed on the instruction of the Controller will remain the property of the Controller and/or the data subjects concerned.

Article 3. Obligations of the Processor
3.1. In respect of the processing referred to in article 2, the Processor will ensure compliance with applicable legislation and regulations, including in any event the legislation and regulations in the field of the protection of Personal Data, such as the General Data Protection Regulation.
3.2. All subsidiaries, sister companies and parent companies in the Processor's Group have the same rights and associated obligations under this Data Processing Agreement as the Processor.
3.3. The Processors obligations arising from this Data Processing Agreement also apply to any party processing Personal Data under the authority of the Processor, including, but not confined to, employees, in the broadest sense.

Article 4. Transfer of Personal Data
4.1. The Processor is allowed to process the Personal Data inside of the European Economic Area. In addition, the Processor is allowed to transfer the Personal Data to a country outside the European Economic Area, provided the Processor ensures an adequate level of protection and agree to be bound by the “standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council” (hereinafter “Standard Contractual Clauses”) attached in Appendix C “Standard Contractual Clauses” hereinafter..
4.2. Upon request, the Processor will inform the Controller of the country or countries involved.
4.3. In particular, the Processor will, in determining an adequate level of protection, take account of the duration of the intended processing, the country of origin and the country of destination, the general and sectoral rules of law that apply in the country concerned, as well as the professional rules and the security measures complied with in those countries.

Article 5. Division of responsibility
5.1. The Processor will make IT means available for the processing that can be used by the Controller for the purposes stated in article 2. The Processor will itself only perform processing based on agreements with the Controller.
5.2. With respect to all Personal Data and instructions issued by the Controller to the Processor, the Controller guarantees that it has the necessary authority. The Controller will indemnify the Processor against any form of harm and/or third-party claims that may arise from, or be related to or based on, an assertion that the Controller was not authorized to issue certain Personal Data or a certain instruction to the Processor.

Article 6. Subprocessors

6.1. The Processor engages Subprocessors, which are available on request and for which the Controller hereby provides authorization. In the case of new Subprocessors, the Processor will inform the Controller thereof. If the Controller has well-founded objections to the engagement of the Subprocessors, a suitable solution must be sought in consultation. If the parties are unable to reach a suitable solution, the Controller may give notice to terminate the Agreement if the use of a specific Subprocessor of which it has been notified is unacceptable to it.

6.2. All the companies within the Processor's Group, are part of the Subprocessors which the Processor engages.

6.3. The Processor will in any case ensure that these Subprocessors assume similar obligations in writing as those agreed between the Controller and Processor.

6.4. The Processor warrants correct compliance with the obligations in this Data Processing Agreement by such Subprocessors and, in the event of errors committed by such Subprocessors, is liable itself for any and all damage or loss as if it had committed the error(s) itself.

Article 7. Security

7.1. The Processor will put in place appropriate technical and organizational measures to secure the Personal Data against loss or any form of unlawful processing, including unnecessary collection or further processing.

7.2. The Processor will ensure that the security measures as described in Annex A or otherwise agreed in writing are always in place.

Article 8. Notification obligation

8.1. The Processor will inform the Controller, without unreasonable delay and if possible, within twenty-four (24) hours, if the Processor discovers or has reasonable grounds to suspect that unauthorized access to or unauthorized obtaining, use, loss, theft, destruction or disclosure of the Personal Data ('a data breach') is occurring or has occurred.

8.2. In case of a data breach the Processor will complete the form in Annex B as complete and accurate as possible and send it to the Controller.

Article 9. Handling requests and complaints from data subjects

9.1 If a data subject sends the Processor a request to access, improve, supplement, change or block their data, or submits a complaint to the Processor, the Processor will forward the request or complaint to the Controller and the Controller will follow up on the request or complaint. The Processor may inform the data subject that it has done so.

Article 10. Confidentiality

10.1. The Processor will keep secret all Personal Data which it receives from the Controller, or to which it is given access by the Controller, and the Processor will not disclose or make this data accessible to third parties (other than permitted Subprocessors) without prior written permission from the Controller, unless the Personal Data must be disclosed to a party authorized to receive such data (such as a supervisory authority, investigating officer or court) pursuant to a written obligation.

Article 11. Compliance check (audit)

11.1. The Controller is entitled to arrange that a suitable external party who is accepted by the Processor performs an audit in order to determine whether the Processor complies fully and correctly with this Data Processing Agreement. This party will be bound by confidentiality towards third parties.

11.2. In conducting the audit, an attempt will be made to minimize any impact on the Processor's business operations. Audits will be performed once per year at most and will be announced at least fourteen (14) days in advance.

11.3. The Processor will cooperate in the audit and will make available any information and employees that may reasonably be relevant to the audit (including supporting information such as system logs) as soon as possible.

11.4. If the audit shows that the Processor has materially failed to comply with this Data Processing Agreement, the Processor will put in place at its own expense all measures necessary to remedy any observed breach as quickly as possible. The Controller will bear the costs of the external party who performs the audit.

11.5 If the audit shows that the Processor has not failed to comply with this Data Processing Agreement, the Controller will bear the costs of the audit (including the reasonable costs incurred by the Processor through cooperating in the audit).

Article 12. Duration and termination

12.1. This Data Processing Agreement will remain in effect for the term specified in the agreement between the Parties, in the absence of which it will at least apply for the duration of the collaboration.

12.2. Upon termination of the services by the Processor, the Controller is itself responsible for making copies of, exporting or otherwise returning, in good time, the Personal Data that the Processor processes on behalf of the Controller. After termination of the Data Processing Agreement, the Processor will remove or destroy the (Personal Data) data of the Controller.

12.3. The Processor is entitled to revise this Data Processing Agreement and any of its annexes from time to time. It will inform the Controller of the changes at least one (1) month in advance. The Controller may lodge a notice of objection by the end of this one (1) month if it does not agree to the changes. If the Processor does not receive a notice of objection within this period, the changes will be deemed to have been accepted by the Controller.

Article 13. Applicable law and settlement of disputes

13.1. The Data Processing Agreement and its execution are governed by Dutch law.

13.2. Any disputes that may arise between the Controller and the Processor in connection with this Data Processing Agreement will be submitted to the competent court in Rotterdam.

Annex A. Security measures

#	Subject	Measure
1	Information security policy	An information security policy is in place which complies with the GDPR and any guidelines from the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), and which is aligned with the ISO/IEC 27001 standard. This policy has been communicated internally and implemented in practice through documented procedures.
2	Access management	The principles of 'least privilege' and 'need-to-know' are applied to staff and permitted Subprocessors. User access will be revoked or amended in a timely manner if there is any change to the status of staff members, suppliers, clients, business partners or third parties. Up-to-date forms of encoding and encryption that are generally regarded as safe will be used for identification, authentication and authorization.
3	Staff	Employees have been informed of their responsibilities regarding information security and there is a procedure for verifying that employees comply with their obligations.
4	Subprocessor contract management	A Data Processing Agreement for Subprocessors will be signed with every permitted Subprocessor, which will contractually oblige the Subprocessor to comply with the same obligations to processing as are contained in this Data Processing.
5	Security incident response	A documented security incident response plan is in place that is suitable for detecting, resolving and reporting data breaches, in accordance with the requirements of Article 8.
6	Vulnerability/ patch management	Periodic scans are conducted to detect vulnerabilities in the systems and network equipment used. Security patches are installed or implemented immediately or promptly after they become available.
7	Network and system security	Measures have been put in place to combat and detect malware as well as misuse of the network and systems (such as firewalls and antivirus software).
8	Physical access security	Suitable measures (such as locks, cameras and alarm systems) have been put in place to secure against unauthorized access the rooms where the Personal Data may be processed.
9	Logging	Through logging, it can be shown that only legitimate users are using or processing the Personal Data. When non-legitimate users are detected, suitable action is taken.
11	Business continuity and disaster recovery	Policy, processes and procedures have been implemented to ensure that the products or services provided, and the processed Personal Data remain available in case of unforeseen circumstances and disasters or can be recovered as quickly as possible.
12	Independent audits	Independent external audits are periodically performed to uncover non-compliances with defined security measures.

Annex B Data breach notification form

1. What kind of incident occurred?

2. What kind of data were involved?

3. In what way were the data compromised?

4. When did the incident occur?

5. What kind of consequences might the incident have for the Controller?

6. What measures have been taken to end the incident and/or limit the consequences?

7. What measures will be taken to end the incident and/or limit the consequences?

8. On what date are these measures expected to be implemented?

APPENDIX C –STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

(Pursuant to Commission Decision of 5 February 2010 (2010/87/EU))

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer also on behalf of the other Controllers
(in the Clauses hereinafter referred to as the 'data exporter')

and

i3D.net
(in the Clauses hereinafter referred to as the 'data importer')
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.

COMMISSION DECISION

of 5 February 2010

on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

(notified under document C(2010) 593)

(Text with EEA relevance)

(2010/87/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 [1], and in particular Article 26(4) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Pursuant to Directive 95/46/EC Member States are required to provide that a transfer of personal data toa third country may only take place if the third country in question ensures an adequate level of data protection and the Member States' laws, which comply with the other provisions of the Directive, are respected prior to the transfer.

(2) However, Article 26(2) of Directive 95/46/EC provides that Member States may authorise, subject to certainsafeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation

(4) Standard contractual clauses should relate only to data protection. Therefore, the data exporter and the data importer are free to include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses.

(5) This Decision should be without prejudice to national authorisations Member States may grant in accordance with national provisions implementing Article 26(2) of Directive 95/46/EC. This Decision should only have the effect of requiring the Member States not to refuse to recognise, as providing adequate safeguards, the standard contractual clauses set out in it and should not therefore have any effect on other contractual clauses.

(6) Commission Decision 2002/16/EC of 27 December2001 on standard contractual clauses for the transfer of or set of data transfer operations. The Working Party

on the protection of individuals with regard to the processing of personal data established under that Directive has issued guidelines to aid with the assessment.

personal data to processors established in third countries, under Directive 95/46/EC [2] was adopted in order to facilitate the transfer of personal data from a data controller established in the European Union to a processor established in a third country which does not offer adequate level of protection.

(7) Much experience has been gained since the adoption of Decision 2002/16/EC. In addition, the report on the implementation of Decisions on standard contractual clauses for the transfers of personal data to third countries [3] has shown that there is an increasing interest in promoting the use of the standard contractual clauses for international transfers of personal data to third countries not providing an adequate level of protection. In addition, stakeholders have submitted proposals with a view to updating the standard contractual clauses set out in Decision 2002/16/EC in order to take account of the rapidly expanding scopeof data-processing activities in the world and to address some issues that were not covered by that Decision [4].

[1] OJ L 281, 23.11.1995, p. 31.

[2] OJ L 6, 10.1.2002, p. 52.

[3] SEC(2006) 95, 20.1.2006.

[4] The International Chamber of Commerce (ICC), Japan Business Council in Europe (JBCE), EU Committee of the American Chamber of Commerce in Belgium (Amcham), and the Federationof European Direct Marketing Associations (FEDMA).

(8) The scope of this Decision should be limited to establishing that the clauses which it sets out may be used by a data controller established in the European Union in order to adduce adequate safeguards within the meaning of Article 26(2) of Directive 95/46/EC for the transfer of personal data to a processor established in a third country.

(9) This Decision should not apply to the transfer of personal data by controllers established in the European Union to controllers established outside the European Union which fall within the scope of Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [1].

(10) This Decision should implement the obligation provided for in Article 17(3) of Directive 95/46/EC and should not prejudice the content of the contracts or legal acts established pursuant to that provision. However, some of the standard contractual clauses, in particular as regards the data exporter's obligations, should be included in order to increase clarity as to the provisions which may be contained in a contract between a controller and a processor.

(11) Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should havethe power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.

(12) Standard contractual clauses should provide for the technical and organisational security measures to be applied by data processors established in a third country not providing adequate protection, in order to ensure a level of security appropriate to the risks repre- sented by the processing and the nature of the data to be protected. Parties should make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.

(13) In order to facilitate data flows from the European Union, it is desirable for processors providing data- processing services to several data controllers in the European Union to be allowed to apply the same technical and organisational security measures irre- spective of the Member State from which the datatransfer originates, in particular in those cases where the data importer receives data for further processing from different establishments of the data exporter inthe European Union, in which case the law of the designated Member State of establishment should apply.

(14) It is appropriate to lay down the minimum information that the parties should specify in the contract dealing with the transfer. Member States should retain the power to particularise the information the parties are required to provide. The operation of this Decision should be reviewed in the light of experience.

(15) The data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses. In particular the data importer should not disclose the personal data to a third party without the prior written consent of the data exporter. The data exporter should instruct the data importer throughout the duration of the data-processing services to process the data in accordance with his instructions, the applicable data protection laws and the obligations contained in the clauses.

(16) The report on the implementation of Decisions on standard contractual clauses for the transfers of personal data to third countries recommended the establishment of appropriate standard contractual clauses on subsequent onwards transfers from a data processor established in a third country to another data processor (sub-processing), in order to take account of business trends and practices for more and more globalised processing activity.

[1] OJ L 181, 4.7.2001, p. 19.

(17) This Decision should contain specific standard contractual clauses on the sub-processing by a data processor established in a third country (the data importer) of his processing services to other processors (sub-processors) established in third countries. In addition, this Decision should set out the conditions that the sub-processing should fulfil to ensure that the personal data being transferred continue to be protected notwithstanding the subsequent transfer to a sub-processor.

(18) In addition, the sub-processing should only consist of the operations agreed in the contract between the data exporter and the data importer incorporating the standard contractual clauses provided for in this Decision and should not refer to different processing operations or purposes so that the purpose limitation principle set out by Directive 95/46/EC is respected. Moreover, where the sub-processor fails to fulfil his own data-processing obligations under the contract, the data importer should remain liable toward the data exporter. The transfer of personal data to processorsestablished outside the European Union should not prejudice the fact that the processing activities shouldbe governed by the applicable data protection law.

(19) Standard contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular where the data subjects suffer damage as a consequence of a breach of the contract.

(20) The data subject should be entitled to take action and, where appropriate, receive compensation from the data exporter who is the data controller of the personal data transferred. Exceptionally, the data subject should also be entitled to take action, and, where appropriate, receive compensation from the data importer in those cases, arising out of a breach by the data importer or any sub-processor under it of any of its obligations referred to in the paragraph 2 of Clause 3, where the data exporter has factually disappeared or has ceased to exist in law or has become insolvent. Exceptionally, the data subject should be also entitled to take action, and, where appropriate, receive compensation from a sub- processor in those situations where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent. Such third-party liability of the sub-processor should be limited to its own processing operations under the contractual clauses.

(21) In the event of a dispute between a data subject, who invokes the third-party beneficiary clause, and the data importer, which is not amicably resolved, the data importer should offer the data subject a choice between mediation or litigation. The extent to which the data subject will have an effective choice will depend on the availability of reliable and recognised systems of mediation. Mediation by the data protection supervisory authorities of the Member State in which the data exporter is established should be an option where they provide such a service.

(22) The contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law. The same law should also govern the provisions on data protection of any contract with a sub-processor for the sub-processing of the processing activities of the personal data transferredby the data exporter to the data importer under the contractual clauses.

(23) Since this Decision applies only to subcontracting by a data processor established in a third country of his processing services to a sub-processor established in a third country, it should not apply to the situation by which a processor established in the European Union and performing the processing of personal data on behalf of a controller established in the European Union subcontracts his processing operations to a sub- processor established in a third country. In such situations, Member States are free whether to take account of the fact that the principles and safeguardsof the standard contractual clauses set out in this Decision have been used to subcontract to a sub-processor established in a third country with the intention of providing adequate protection for the rights of data subjects whose personal data are being transferred for sub-processing operations.

(24) The Working Party on the protection of individuals with regard to the processing of personal data established under Article 29 of Directive 95/46/EC has delivered an opinion on the level of protection provided underthe standard contractual clauses annexed to this Decision, which has been taken into account in the preparation of this Decision.

(25) Decision 2002/16/EC should be repealed.

(26) The measures provided for in this Decision are in accordance with the opinion of the Committee estab-lished under Article 31 of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

Article 1

The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedomsof individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive 95/46/EC.

Article 2

This Decision concerns only the adequacy of protection provided by the standard contractual clauses set out in the Annex for the transfer of personal data to processors. It does not affect the application of other national provisions implementing Directive 95/46/EC that pertain to the processing of personal data within the Member States.

This Decision shall apply to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as processors.

Article 3

For the purposes of this Decision the following definitions shall apply:

(a) 'special categories of data' means the data referred to in Article 8 of Directive 95/46/EC;

(b) 'supervisory authority' means the authority referred to in Article 28 of Directive 95/46/EC;

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

(d) 'data importer' means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision 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;

(e) 'sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer and who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for the processing activities to be carried out on behalf of the data exporter after the transfer in accordance with the data exporter's instructions, the standard contractual clauses set out in the Annex, and the terms of the written contract for sub-processing;

(f) '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;

(g) '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.

Article 4

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer or asub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC wherethose requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;

(b) a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.

3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.

Article 5

The Commission shall evaluate the operation of this Decision on the basis of available information three years after its adoption. It shall submit a report on the findings to the Committee established under Article 31 of Directive 95/46/EC. It shall include any evidence that could affect the evaluation concerning the adequacy of the standard contractual clauses in the Annex and any evidence that this Decision is being applied in a discriminatory way.

Article 6

This Decision shall apply from 15 May 2010.

Article 7

1. Decision 2002/16/EC is repealed with effect from 15 May 2010.

2. A contract concluded between a data exporter and a data importer pursuant to Decision 2002/16/EC before 15 May 2010 shall remain in force and effect for as long as the transfers and data-processing operations that are the subject matter of the contract remain unchanged and personal data covered by this Decision continue to be transferred between the parties. Where contracting parties decide to make changes in this regard or subcontract the processing operations that are the subject matter of the contract they shall be required to enter into a new contract which shall comply with the standard contractual clauses set out in the Annex.

Article 8

This Decision is addressed to the Member States.

Done at Brussels, 5 February 2010.

For the Commission

Jacques BARROT

Vice-President

ANNEX

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 exporting organisation: ....

Address: ....

Tel. ....;. fax ....;. e-mail: ....

Other information needed to identify the organisation

....

(the data **exporter**)

And

Name of the data importing organisation: ....

Address: ....

Tel. ....;. fax ....;. e-mail: ....

Other information needed to identify the organisation:

....

(the data **importer**)

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 [1];

(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;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 indi- viduals 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 sub-processor 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 dataexporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor 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 tothe 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor 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 [1]

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 2 before processing the personal data transferred;

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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 sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard toits 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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, namely ....

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

Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses [1]. Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 ....

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

4. The data exporter shall keep a list of sub-processing 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 sub-processor 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 sub-processor 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.

On behalf of the data exporter:

Name (written out in full): ……………………………………………………

Position: ……………………………………………………

Address: ……………………………………………………

Other information necessary in order for the contract to be binding (if any):

Signature ……………………………………

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): ……………………………………………………

Position: ……………………………………………………

Address: ……………………………………………………

Other information necessary in order for the contract to be binding (if any):

Signature ……………………………………

(stamp of organisation)

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 exporter

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

....

....

....

Data importer

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

....

....

....

Data subjects

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

....

....

....

Categories of data

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

....

....

....

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):

....

....

....

DATA EXPORTER

Name: ....

Authorised Signature ....

DATA IMPORTER

Name: ....

Authorised Signature ....

Appendix 2

to the Standard Contractual Clauses

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

Description of the technical and organisational security measures implemented by the data importer inaccordance with Clauses 4(d) and 5(c) (or document/legislation attached):

....
....

....
....

....
....

....
....

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim [1].

[1] Paragraph on liabilities is optional.