

## F5 END USER SERVICES AGREEMENT

### DATA PROTECTION ADDENDUM

This Data Protection Addendum ("DPA") forms part of the End User Services Agreement (the "Agreement") applicable to certain SaaS Offerings to the extent set forth in the Service-Specific Terms for such SaaS Offerings. Additional detail for particular SaaS Offerings is available in the Service-Specific Terms, which take precedence over this DPA to the extent of any conflict.

#### 1. Definitions

##### 1.1 In this DPA:

- 1.1.1 "**Applicable Law**" means all laws, regulations and other legal requirements applicable to either (i) F5 in its role as provider of the SaaS Offerings or (ii) you. This may include, for example, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") and the California Consumer Privacy Act and associated regulations ("**CCPA**"). Each party is responsible only for the Applicable Law applicable to it.
- 1.1.2 "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- 1.1.3 "**Privacy Shield**" means the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks administered by the U.S. Department of Commerce.
- 1.1.4 "**Personal Data**" means any information relating to an identified or identifiable individual, within the meaning of the GDPR (regardless of whether the GDPR applies), and any other information constituting "personal information" as such term is defined in the CCPA (regardless of whether the CCPA applies).
- 1.1.5 "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- 1.1.6 "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1.1.7 "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
- 1.1.8 "**Standard Contractual Clauses**" means 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, attached hereto as Exhibit A and completed as described in the "Data Transfers" section below.
- 1.1.9 "**Subprocessor**" means any F5 affiliate or subcontractor engaged by F5 for the Processing of Personal Data.
- 1.1.10 "**Support Portal**" means support.f5.com and any similar online property that F5 operates for the purpose of providing support information or receiving support inquiries for the SaaS Offering.

1.2 Other capitalized terms have the meaning set forth in the Agreement.

#### 2. Scope and Relationship of the Parties

2.1 This DPA applies only to the Personal Data in Your Content as set forth in the Service-Specific Terms.

2.2 For such Personal Data, you are (or you represent that you are acting with full authority on behalf of) the Controller, and F5 is your Processor. If you are acting on behalf of a Controller (or on behalf of intermediaries such as other Processors of the Controller), then, to the extent legally permissible:

- 2.2.1 You will serve as the sole point of contact for F5 with regard to any such third parties;

- 2.2.2 F5 need not interact directly with any such third party in matters relating to this DPA; and
- 2.2.3 Where F5 would otherwise be required to provide information, assistance, cooperation, or anything else to such third party, F5 may provide it solely to you; but
- 2.2.4 F5 is entitled to follow the instructions of such third party with respect to such third party's Personal Data instead of your instructions if F5 reasonably believes this is legally required under the circumstances.

### **3. Your Instructions to F5**

- 3.1 F5 will Process the Personal Data only as described in the Agreement, unless obligated to do otherwise by Applicable Law. In such case, F5 shall inform you of that legal requirement before the Processing unless legally prohibited from doing so.
- 3.2 The details of the Processing are set forth in the Agreement.
- 3.3 The Agreement, including this DPA, along with your configuration of any settings or options in the SaaS Offering (as you may be permitted to modify from time to time, depending on the SaaS Offering), constitute your complete and final instructions to F5 regarding the Processing of Personal Data, including for purposes of the Standard Contractual Clauses, if they apply.
- 3.4 You shall not instruct F5 to Process Personal Data in violation of Applicable Law. F5 shall promptly inform you if, in F5's opinion, an instruction from you infringes Applicable Law.

### **4. Subprocessors**

- 4.1 F5 may subcontract the collection or other Processing of Personal Data in compliance with Applicable Law. Prior to a Subprocessor's Processing of Personal Data, F5 will impose contractual obligations on the Subprocessor that are substantially the same as those imposed on F5 under this DPA. New Subprocessors will be notified to you prior to their Processing of Personal Data by an update to the Service-Specific Terms posted at [f5.com/company/policies](https://f5.com/company/policies) (or a similarly accessible successor location that F5 specifies there or by notice to you under the Agreement), unless exigent circumstances require their earlier Processing of Personal Data, in which case the new Subprocessor will be notified to you as soon as practicable.
- 4.2 You may object to F5's use of a new Subprocessor by notifying F5 within ten (10) business days after receipt of an updated Subprocessor list. In the event you reasonably object to a new Subprocessor, as permitted in the preceding sentence, F5 will use reasonable efforts to make available to you a change in the SaaS Offering or recommend a commercially reasonable change to your use of the SaaS Offering to avoid Processing of Personal Data by the objected-to Subprocessor without unreasonably burdening you. If F5 is unable to make available such a change or recommendation within a reasonable period of time, not exceeding thirty (30) days, you may terminate the affected SaaS Offering that cannot be provided by F5 without the use of the objected-to Subprocessor by providing written notice to F5. F5 will refund to you any prepaid fees covering the remainder of the term of such SaaS Offering following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on you. If you do not object to use of the new Subprocessor and terminate as set forth above, the Subprocessor is deemed to be accepted by you. F5 remains liable for its Subprocessors' performance to the same extent F5 is liable for its own performance. This paragraph constitutes your consent to subprocessing under the Standard Contractual Clauses, if they apply.

### **5. Security**

- 5.1 F5 will assist you in your compliance with the security obligations of the GDPR and other Applicable Law, as relevant to F5's role in Processing the Personal Data, taking into account the nature of Processing and the information available to F5, by complying with the following paragraph, by making available the Support Portal subject to its terms, and, if available in the applicable SaaS Offering, by providing security options. You are solely responsible for determining whether and how to use such options within the scope of the Agreement, and F5 shall have no liability for damage arising from your failure to select the security options most appropriate to your use of the SaaS Offering.

- 5.2 To protect the Personal Data, F5 shall implement technical and organizational measures described in the applicable Service Specific Terms, without prejudice to F5's right to make future replacements or modifications to the measures that do not materially lower the level of security of the Personal Data.
- 5.3 You are solely responsible for reviewing any available security documentation and features and evaluating for yourself whether the SaaS Offering and related security meet your needs, including your security obligations under Applicable Law. You may use the Service Offering only if the security commitments in this DPA would provide a level of security appropriate to the risk in respect of the Personal Data.
- 5.4 F5 will ensure that the individuals F5 authorizes to Process the Personal Data (i) are subject to a written confidentiality agreement covering such data or are under an appropriate statutory obligation of confidentiality and (ii) receive training appropriate to their role in the Processing of the Personal Data.

## **6. Personal Data Breach Notification**

- 6.1 F5 will comply with the Personal Data Breach-related obligations directly applicable to it under the GDPR and other Applicable Law. Taking into account the nature of Processing and the information available to F5, F5 will assist you in complying with those applicable to you by informing you without undue delay after becoming aware of a confirmed Personal Data Breach. Such notification is not an acknowledgement of fault or responsibility. To the extent available, this notification will include F5's then-current assessment of the following, which may be based on incomplete information:
  - 6.1.1 The nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
  - 6.1.2 The likely consequences of the Personal Data Breach; and
  - 6.1.3 Measures taken or proposed to be taken by F5 to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

## **7. Assistance Responding to Data Subjects**

- 7.1 Taking into account the nature of the Processing, F5 will assist you with the fulfillment of your obligation to honor requests by individuals to exercise their rights under the GDPR and other Applicable Law (such as rights to access their Personal Data) by providing the SaaS Offering's admin capabilities and by forwarding to you any such requests or Personal Data-related complaints that F5 receives within a commercially reasonable timeframe. This timeframe will not exceed 5 business days if (i) the request or complaint is received through the privacy contact information specified in the F5 privacy notice that is hyperlinked from the home page of F5.com and (ii) the request or complaint identifies you as the F5 customer to whom it pertains. Additional support for such requests may be available and would require mutual agreement on fees, the scope of F5's involvement, and any other terms that the parties deem appropriate.

## **8. Assistance with DPIAs and Consultation with Supervisory Authorities**

- 8.1 Taking into account the nature of the Processing and the information available to F5, F5 will provide reasonable assistance to and cooperation with you for your performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving F5, and with related consultation with supervisory authorities, by providing you with the Documentation for the relevant Service Offerings, by making available the Support Portal subject to its terms, and by complying with the Audit section below. Additional support for data protection impact assessments or relations with regulators may be available and would require mutual agreement on fees, the scope of F5's involvement, and any other terms that the parties deem appropriate.

## **9. Data Transfers**

- 9.1 You will comply with Applicable Law relevant to your use of the SaaS Offering, including by obtaining any consents and providing any notices required under Applicable Law for F5 to provide the SaaS Offering. You will ensure that you are entitled to transfer the Personal Data to F5 so that F5 and its Subprocessors may lawfully Process the Personal Data in accordance with this DPA.

- 9.2 You authorize F5 and its Subprocessors to make international transfers of the Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected.
- 9.3 As of the effective date of this DPA, F5 maintains a Privacy Shield certification that covers certain SaaS Offerings, as indicated in their Service-Specific Terms.
- 9.4 To the extent legally required, taking into account F5's Privacy Shield certification, Brexit, and any other relevant factors, the Standard Contractual Clauses form part of this DPA and take precedence over the rest of this DPA to the extent of any conflict, taking into consideration their Clause 10. The Standard Contractual Clauses will be deemed completed as follows:
  - 9.4.1 The exporter is the "Organization" specified in your Account. The exporter's contact information is as set forth in your Account.
  - 9.4.2 The importer is F5 Networks, Inc., with the address set forth in the Notice section of the Agreement, and with email address [privacy@f5.com](mailto:privacy@f5.com), subject to an update by F5 of those addresses in accordance with the Agreement.
  - 9.4.3 For any particular SaaS Offering, Appendices 1 and 2 of the Standard Contractual Clauses are set forth in the Service-Specific Terms for that SaaS Offering.
  - 9.4.4 When you subscribe to a particular SaaS Offering, the parties are deemed to be signing the Standard Contractual Clauses and its applicable Appendices for that SaaS Offering.

## **10. Audits**

- 10.1 F5 will make available to you all information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits including inspections, conducted by you or another auditor mandated by you, as follows:
  - 10.1.1 If the requested audit scope is addressed in an ISO or other audit report issued by a third party auditor within the prior twelve (12) months and F5 provides such report to you and confirms that there are no known material changes in the controls audited, you agree to accept the findings presented in the report in lieu of requesting an audit of the same controls covered by the report. The report is Confidential Information of F5.
  - 10.1.2 If not covered by such report, F5 will provide a written description of its compliance measures for this DPA. This is Confidential Information of F5. You may also refer to the applicable Service Offering Documentation and the Support Portal, subject to its terms, as applicable.
  - 10.1.3 You agree to exercise any right you may have to conduct an audit or inspection, including under the Standard Contractual Clauses, if they apply, by instructing F5 to provide the report and/or information described above. If you wish to change this instruction regarding the audit, you may request a change to this instruction by sending F5 written notice as provided for in the Agreement. Such additional support may be available and would require mutual agreement on fees you would be charged, audit scope, the scope of F5's involvement, and any other terms that the parties deem appropriate.
  - 10.1.4 Nothing in this DPA will require F5 to disclose or make available:
    - 10.1.4.1 any data of any other customer of F5;
    - 10.1.4.2 access to systems;
    - 10.1.4.3 F5's accounting or financial information;
    - 10.1.4.4 any trade secret of F5;
    - 10.1.4.5 any information or access that, in F5's reasonable opinion, could (A) compromise the security of F5 systems or premises; or (B) cause F5 to breach its obligations under Applicable Law or applicable contracts; or
    - 10.1.4.6 any information sought for any reason other than the good faith fulfillment of your obligations under Applicable Law to audit compliance under this DPA.

**11. Return or Destruction**

- 11.1 F5 will, at your choice, return to you and/or destroy all Personal Data after the termination or expiration of your subscription to the relevant SaaS Offering except to the extent Applicable Law requires storage of the Personal Data. F5's return of Personal Data to you may be subject to reasonable fees for such return. If F5 has not received your election within 30 days of such termination or expiration, F5 may assume that you have selected deletion. The certification of deletion required by Clause 12 of the Standard Contractual Clauses (if they apply) will be provided only on written request.
- 11.2 Nothing will oblige F5 to delete Personal Data from files created for security, backup and business continuity purposes sooner than required by F5's reasonable data retention processes. If you require earlier deletion of such Personal Data, and such deletion is commercially feasible, you must first pay F5's reasonable fees for such deletion, which may include costs for business interruptions associated with such a request.

**Exhibit A**

**Commission Decision C(2010)593  
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<sup>1</sup>;
- (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

---

<sup>1</sup> 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.

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<sup>2</sup>***

The data importer agrees and warrants:

---

<sup>2</sup> 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.



- (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;
- (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 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 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

---

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.

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 or 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<sup>3</sup>. 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.
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.

**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)

---

<sup>3</sup> 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.

**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 in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

.....  
.....  
.....