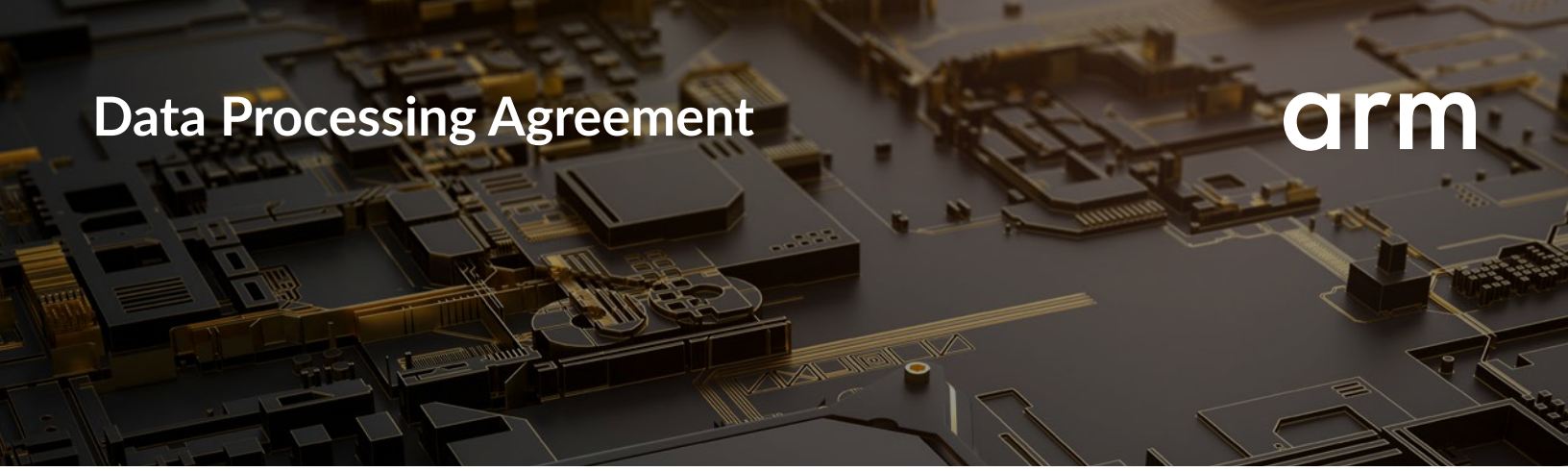

Data Processing Agreement

1. Scope

1.1 This Annex, including its Schedules, ("DPA") applies to Supplier's Processing of Personal Data as part of Supplier's provision of the Services.

1.2 This DPA is effective as long as Supplier Processes Personal Data.

1.3 Except as expressly stated otherwise in this DPA, in the event of any conflict or inconsistency between the terms of the Agreement and the terms of this DPA, the relevant terms of the DPA will prevail to the extent of the conflict or inconsistency.

2. Definitions

2.1 Capitalised terms have the meaning given to them in the Agreement unless otherwise defined in this DPA.

2.2 The following terms have the meanings set out below for this DPA:

"Affiliate" shall have the meaning set out in section 1159 of the Companies Act 2006;

"Data Protection Laws" means the GDPR, the UK Data Protection Act 2018, Directive 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them, and all other applicable laws relating to Processing of Personal Data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities.

"Europe" means the European Economic Area, Switzerland and the United Kingdom.

"GDPR" means, in each case to the extent applicable to the processing activities: (i) Regulation (EU) 2016/679; and (ii) Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the United Kingdom from the European Union;

"Losses" means all losses, liabilities, fines, charges, damages, actions, costs and expenses, professional fees (including legal fees actually incurred) and disbursements and costs of investigation, litigation, settlement, judgment, interest and penalties.

"Personal Data," "Data Controller," "Data Processor," "Data Subject," "Processing," (and **"Process"** and **"Processing"** shall be construed accordingly) and **"appropriate technical and organisational measures"** shall be interpreted in accordance with the GDPR; and

"Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data that Supplier Processes in the course of providing the Services.

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission decision of 5 February 2010, published under document number C(2010) 593 2010/87/EU.

3. Roles of the parties

3.1 The parties agree the following:

(a) Arm is the Data Controller or a Data Processor acting on behalf of Arm's customers who act as Data Controllers; and

(b) Supplier is the Data Processor, or as a sub-processor of Arm's customers, in respect of Personal Data Processed by Supplier for the provision of the Services.

3.2 Arm as the Data Controller, or as the Data Processor acting on behalf of its customers, shall be solely responsible for determining the purposes for which and the manner in which Personal Data are, or are to be, Processed.

4. Supplier's obligation

4.1 Where Supplier Processes Personal Data on behalf of Arm or of Arm's customers, Supplier shall, in respect of such Personal Data:

(a) act only on written instructions and directions from Arm and comply promptly with all such instructions and directions received from Arm from time to time;

(b) immediately notify Arm if, in Supplier's opinion, any instruction or direction from Arm infringes applicable Data Protection Law. Following such notification, Arm shall be entitled to suspend the Processing of Personal Data by Supplier, and to terminate any further Personal Data Processing and the Agreement;

(c) not Process Personal Data for any purpose other than for the provision of the Services and only to the extent reasonably necessary for the performance of this Agreement. Schedule 1 to this DPA sets out the nature, duration and purpose of the Processing, the types of Personal Data Supplier Processes and the categories of Data Subjects whose Personal Data are Processed;

(d) not disclose, publish or divulge Personal Data to any employee, director, agent, contractor or affiliate of Supplier or any third party except as necessary for the performance of the Services, to comply with applicable laws or with Arm's prior written consent; and

(e) cooperate with Arm and provide such reasonable assistance as Arm requires to comply with Data Protection Laws, this DPA, Arm's customers' instructions when Arm acts as a Data Processor, including complying with any complaints made by Data Subjects or investigations or enquiries made by any supervisory authority or any other regulator relating to Arm's or Supplier's obligations under applicable Data Protection Laws.

4.2 Supplier shall immediately and in writing inform Arm of:

(a) any request made by Data Subjects under Data Protection Laws;

(b) any request or complaint received from Arm's customers, consumers, employees or from any other individual;

(c) any question, complaint, investigation or other inquiry from a supervisory authority; and

(d) any request from a regulator or other public authority of whatever jurisdiction requiring the disclosure of Personal Data Processed by Supplier on behalf of Arm,

and Supplier shall provide a copy of any such request within 2 (two) business days. Supplier agrees that it will only respond to such request as instructed by Arm or as otherwise required by applicable law. Supplier shall assist Arm to fulfil its obligations to respond to requests made by Data Subjects in accordance with Data Protection Laws.

4.3 If (1) Arm receives approval for its binding corporate rules from a supervisory authority, and (2) Arm notifies Supplier of such approval, then Supplier will be subject to the following requirements:

(a) EU Data Subjects can enforce their rights as third party beneficiaries in relation to a breach by Supplier of this DPA or applicable Data Protection Laws in the event that EU Data Subjects are unable to bring a claim against Arm; and

(b) Supplier shall co-operate fully and accept to be audited by a competent supervisory authority and to comply with the advice of such supervisory authority.

4.4 Upon termination of the Agreement or upon request from Arm to securely delete or return Personal Data, Supplier shall comply with Arm's request to securely delete existing copies of such Personal Data unless Data Protection Laws require storage of the Personal Data, in which case Supplier shall protect the confidentiality of the Personal Data and shall not actively Process the Personal Data.

5. Security, Confidentiality and Breach Notification

5.1 Supplier agrees and warrants that it has implemented and maintains a comprehensive written information security program that complies with Data Protection Laws by applying all necessary and appropriate technical and organisational measures designed to:

(a) protect the security and confidentiality of Personal Data Processed by Supplier in providing the Services; and

(b) protect Personal Data against a Security Breach, having regard to the nature of the Personal Data which is to be protected.

As a minimum, the appropriate technical and organisational measures should include the requirements set out in Schedule 2.

5.2 Supplier agrees to notify Arm by emailing **privacy@arm.com** of any technical, operational, organisational or other change having a material impact on the security, confidentiality or protection of Personal Data, no less than 10 (ten) working days prior to implementing any such change. Supplier agrees to submit its information security program to an audit as provided by clause 8.

5.3 Supplier shall ensure that any Supplier personnel with access to Personal Data are bound by confidentiality obligations in respect of access, use or Processing of such Personal Data, and take reasonable steps to ensure the reliability and competence of Supplier's personnel who have access to the Personal Data. Without limiting the foregoing, Supplier undertakes to provide training as necessary from time to time to Supplier's personnel with respect to Supplier's obligations in this DPA and to ensure that Supplier's personnel are aware of and comply with such obligations.

5.4 In the event of a suspected Security Breach, Supplier shall, at Supplier's own expense:

(a) immediately take action to investigate any suspected Security Breach, and to identify, prevent and mitigate the effects of the suspected Security Breach and to remedy the Security Breach;

(b) notify Arm by emailing **privacy@arm.com** without undue delay Arm without undue delay and provide Arm with a detailed description of the Security Breach including:

(i) the likely impact of the Security Breach;

(ii) the categories and approximate number of Data Subjects affected and their country of residence and the categories and approximate number of records affected;

(iii) the risk posed by the Security Breach to individuals; and

(iv) the measures taken or proposed to be taken by Supplier to address the Security Breach and to mitigate its adverse effects.

and provide timely updates to this information and any other information Arm may reasonably request relating to the Security Breach; and

(c) not release or publish any filing, communication, notice, press release or report concerning the Security Breach without Arm's prior written approval (except where required to do so by applicable law). Supplier acknowledges and agrees that a violation of this clause, or the occurrence of any Security Breach, may cause immediate and irreparable harm to Arm for which monetary damages may not constitute an adequate remedy.

6. Sub-processing

6.1 Supplier shall not give access to or transfer any Personal Data to any third party (including any Supplier Affiliates, group companies or sub-processors) without the prior written permission of Arm. Where Arm gives permission to Supplier engaging sub-processors to carry out any part of the Services involving the Processing of Personal Data, Supplier shall include in any contract with such third party provisions in favour of Arm which are equivalent to those in this DPA and as are required by applicable Data Protection Laws. For the avoidance of doubt, where a sub-processor fails to fulfil its obligations under any sub-processing agreement or any applicable Data Protection Laws, Supplier will remain fully liable to Arm for the fulfilment of Supplier's obligations under this DPA.

6.2 Subject to compliance with clause 6.1, Arm agrees that Supplier may engage third-party sub-processors for the purposes of Processing Personal Data under the Agreement. A list of sub-processors approved by Arm as at the date of this Agreement is set out at Schedule 3. Supplier can at any time appoint a new sub-processor provided that Arm is given 15 (fifteen) business days' prior notice by emailing privacy@arm.com and Arm does not object to such changes within that timeframe. If Arm objects to the appointment of a new sub-processor within such period Supplier shall use reasonable efforts to make available to Arm a change in the Services or recommend a change to Arm's configuration or use of the Services, in each case to avoid the processing of Arm Personal Data by the objected-to sub-processor for Arm's consideration and approval. If Supplier is unable to make available such change within a reasonable period of time, which shall not exceed 10 (ten) business days or Arm does not approve any such changes proposed by Supplier, Arm may, by providing written notice to Supplier, terminate the Service or part thereof which cannot be provided by Supplier without the use of the objected-to sub-processor. In such case, termination will result in no further liability between the parties, except as otherwise provided in the Agreement.

7. International data transfers

7.1 Except where Supplier has obtained the prior explicit written permission from Arm, Supplier shall not Process Personal Data outside of Europe.

7.2 Where Arm gives permission, it shall be subject to the condition that Supplier Processes Personal Data either in a country which has been considered to provide an adequate level of protection under Data Protection Laws ("Adequate Country") or by a data recipient which has implemented adequate safeguards under Data Protection Laws, including binding corporate rules, Standard Contractual Clauses or the EU-U.S./ Swiss-U.S. Privacy Shield Framework (each an "Adequate Safeguard") which shall be made available to Arm on request.

7.3 To the extent that Supplier is located outside an Adequate Country and where no Adequate Safeguard is in place, the parties shall be deemed to have executed the Standard Contractual Clauses set out in Schedule 4 to this DPA. For the avoidance of doubt, the Standard Contractual Clauses apply to Personal Data Processed by Supplier in the context of the Services that are transferred outside of Europe, either directly or via an onward transfer, to any non-Adequate Country or to any recipient which has not implemented an Adequate Safeguard. For the purposes of this DPA, when the parties execute the Standard Contractual Clauses, they acknowledge that:

(a) Arm is the "data exporter" and Supplier is the "data importer";

(b) the law applicable to the Standard Contractual Clauses is the law applicable to this DPA;

(c) for the purposes of clauses 5(h) and 11 of the Standard Contractual Clauses, Arm consents to Supplier subcontracting processing operations in accordance with the provisions set out at clause 6 of this DPA;

(d) any rights to audit, pursuant to clauses 5(f) and 12(2) of the Standard Contractual Clauses, will be exercised in accordance with clause 8 of this DPA;

(e) in the event of any conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail to the extent of any conflict of inconsistency; and

(f) the information contained in Schedules 1 and 2 of this DPA form part of Appendices 1 and 2 of the Standard Contractual Clauses, respectively.

7.4 Where Arm gives permission and in the event that any of the conditions in 7.5 apply to the Processing of Personal Data by Supplier for the provision of the Services, Arm may, at its sole discretion, require Supplier to cease Processing Personal Data for the provision of the Services or co-operate with it and facilitate the use of an alternative Adequate Safeguard.

7.5 The conditions referred to in clause 7.4 are:

(a) an Adequate Country is held no longer to provide an adequate level of protection under Data Protection Laws;

(b) an Adequate Safeguard is held to be invalid; or

(c) a supervisory authority requires transfers to an Adequate Country or made pursuant to an Adequate Safeguard to be suspended.

8. Audit

8.1 Supplier shall:

(a) make available to Arm all information necessary to demonstrate Supplier's compliance with this DPA; and

(b) provide such co-operation as Arm considers to be necessary to enable Arm to audit and verify Supplier's and Supplier's sub-processors compliance with this DPA from time to time during the term of the Agreement and for 12 (twelve) months thereafter, which will include providing access to the premises, resources, and personnel of Supplier and Supplier's sub-processors use in connection with the provision of the Services. Such co-operation may include but shall not be limited to helping Arm to carry out risk assessments of Supplier's data processing operations, in particular providing information about, and permitting Arm to inspect, those operations.

9. Indemnity

9.1 Supplier shall not cause or permit to be done anything within its knowledge or control which may cause (or otherwise result in) Arm to be in breach of Data Protection Laws.

9.2 Supplier shall fully indemnify Arm from and against any and all Losses suffered or incurred by Arm arising from or in connection with breach by Supplier of any of its obligations under this DPA.

Schedule 1

Description of Data Processing Activities

Duration of Processing	From the date that Arm engages Supplier to provide Services until expiry or termination of the Agreement in accordance with the DPA
Nature/Purpose of Processing	
Retention	
Type of Personal Data (Include special category data if applicable)	
Categories of Data Subjects	
Third Countries or International Organisations Personal Data Will be Transferred to.	
Sub-processors	

Schedule 2

Security Measures

This appendix 2 sets out the description of types of technical and organisational security measures that may be implemented by the Data Importer in accordance clauses 4(c) and 5(c) of the Processor Clauses:

1. Access control to premises and facilities

1.1 Unauthorized access (in the physical sense) must be prevented.

1.2 Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

Examples:

- Access control system ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Security staff, janitors
- Surveillance facilities Alarm system, video/CCTV monitor

2. Access control to systems

2.1 Unauthorized access to IT systems must be prevented.

2.2 Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

Examples:

- Password procedures (incl. special characters, minimum length, change of password, the factor authentication)
- Automatic blocking (e.g., password or timeout)
- Creation of one master record per user
- Encryption of data media
- Two-factor authentication

3. Access control to data

3.1 Activities in IT systems not covered by the allocated access rights must be prevented.

3.2 Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

Examples:

- Differentiated access rights (profiles, roles, transactions and objects)
- Reports

- Use of professional and secure storage solutions
- Logging of access and (attempted) misuse

4. Disclosure control

4.1 Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

4.2 Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

Examples:

- Encryption/tunneling (VPN)
- Electronic signature
- Logging
- Transport security

5. Input control

5.1 Full documentation of data management and maintenance must be maintained.

5.2 Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

Example:

- Logging and reporting systems

6. Job control

6.1 Commissioned data processing must be carried out according to directions.

6.2 Measures (technical/organizational) to segregate the responsibilities between the Principal and the Agent:

Examples:

- Unambiguous wording of the contract
- Formal commissioning (request form)
- Criteria for selecting the Agent
- Monitoring of contract performance

7. Availability control

7.1 The data must be protected against accidental destruction or loss.

7.2 Measures to assure data security (physical/logical):

Examples:

- Backup procedures
- Mirroring of hard disks, e.g. RAID technology
- Uninterruptible power supply (UPS)
- Remote storage
- Anti-virus/firewall systems
- Disaster recovery plan

8. Segregation control

8.1 Data collected for different purposes must also be processed separately.

8.2 Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

Examples:

- “Internal client” concept / limitation of use
- Segregation of functions (production/testing)

Schedule 3

Approved Sub-Processors

Service Provider has appointed the following sub-processors to Process Personal Data in the context of the Services specified in the Agreement or in an individual statement of work; Arm's execution of this Agreement evidences Arm's written consent to the appointment of each sub-processor listed below.

Name	Location of Processing	Appropriate Safeguard (if applicable)	Processing Activities

Schedule 4

Standard Contractual Clauses

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.

The entity or entities identified as "Arm" in the Agreement are qualified as the "data exporter"

The entity or entities identified as "Supplier" in the Agreement are qualified 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.

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organisational security measures specified in Appendix 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 or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. 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.

Appendix 1 to the Standard Contractual Clauses

A description of the processing operations, data subjects, categories of data (including any special categories of data) is set out in Schedule 1 to the DPA.

Appendix 2 to the Standard Contractual Clauses

A description of the security measures is set out in Schedule 2 to the DPA.