FirstRand

FIRSTRAND GROUP DATA PROTECTION POLICY FOR SUPPLIERS AND BUSINESS PARTNERS

August 2021

TABLE OF CONTENTS

1 BACKGROUND AND PURPOSE

FirstRand Limited and its subsidiary companies, including divisions, segments and business units (referred to as **FirstRand** or **the group**) recognise that personal information (**PI**) and records are important assets that must be protected. This document establishes a governance framework that sets out ethical and sound PI protection practices that are to be followed by all suppliers and business partners appointed by the group. This policy sets out the minimum PI protection requirements applicable to suppliers and business partners to preserve the integrity, confidentiality and availability of PI or records furnished to suppliers and business partners during the course and scope of their engagement with the group.

This policy will set out the rules of engagement in relation to how PI is handled by suppliers and business partners on behalf of FirstRand, as well as the minimum legal requirements that FirstRand requires suppliers and business partners to adhere to, including compliance with the requirements of the Protection of Personal Information Act 4 of 2013 (**POPIA**), the General Data Privacy Regulation (**GDPR**) and other legislation, where applicable from time to time, in their capacity as service providers or business partners to the group. This policy is applicable to all suppliers and applicable business partners who engage with the group and handle PI as defined in applicable law.

All group suppliers and business partners are expected to comply with all local legislative requirements within the jurisdiction in which they operate.

This policy serves as an additional measure which specifies the requirements that FirstRand has in relation to how suppliers and business partners are required to organise themselves and provide goods and/or services, or collaborate in relation to agreements concluded with FirstRand and its affiliates.

FirstRand subscribes to the higher of the host-or-home principle when dealing with jurisdictions outside of South Africa. This means that where the supplier or business partner conducts business activities within a jurisdiction where the PI protection laws and regulations are of a higher standard than POPIA, then the provisions of those laws and regulations will take precedence over the provisions of POPIA, and vice versa.

2 DEFINITIONS

The following concepts will be used throughout this policy and are defined as follows:

Affiliate	Means (a) any subsidiary or a holding company or a subsidiary of the holding company of either party, or (b) any entity that controls, is controlled by or is under common control with either party. The terms “subsidiary” and “holding company” will have the meaning assigned thereto in Chapter 1 of the Companies Act, No. 71 of 2008 (the Companies Act). The term “control” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity through the ownership of voting securities representing 50% (fifty per cent) plus 1 (one) of the possible votes.
Agreement	Means the agreement entered into between the group and the supplier or business partner, as applicable.
Associate	Shall mean any entity or unincorporated joint venture in which FirstRand has the right to receive at least 20% (twenty per cent) of the profit share or similar benefit derived from such entity or unincorporated joint venture.

Business partner	A business partner, in the context of this policy, means a natural or juristic person (**person**) holding a business relationship with the group, where such relationship does not fall within the category of a supplier, employee or customer relationship, and which person processes PI for, on behalf of or together with FirstRand under the terms of the applicable agreement between the group and the person. (*For the avoidance of doubt, the term **business partner** is used for the sake of convenience and for descriptive purposes only and should not be construed to imply a partnership between the group and the business partner in a legal sense or as understood in law.)*
Child	A child is a natural person who is defined as a child by a country's legislation and who has not been recognised as an adult by the courts of a country.
Competent person	Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of PI.
Customer	A customer is a natural or legal person who is a group customer or a person who provided their PI/SPI to the group in the context of a sale of acquiring goods or services.
Data subject	Means the person to whom PI relates. In reference to the group, this primarily but without limitation means customers, employees and operators/suppliers, other persons and third parties.
Employee	Means a person employed for wages or a salary, including permanent employees, non-permanent employees, contractors, secondees and contingent workers.
FirstRand or the group	Means FirstRand Limited and its subsidiary companies, including divisions, segments and business units. Certain subsidiary companies may be excluded from the FirstRand group description for the purposes of this data protection policy such as where the FirstRand group is involved in private equity investments (**excluded subsidiaries**). A simplified legal entity structure for the group can be found on the FirstRand website.
Juristic person	Means an existing company, corporation, trust, not-for-profit organisation or other legal entity recognised by law as having rights and duties.
Legislation	Means relevant and applicable data privacy and protection legislation, including but not limited to: • the Protection of Personal Information Act 4 of 2013 (POPIA); • the General Data Protection Regulation (GDPR); • the Data Protection (Bailiwick of Guernsey) Law, 2017; • the Data Protection (Jersey) Law 2018; and • the UK's Data Protection Act 2018.
Natural person	Means an identifiable, living human being.
Operator	Means a person who processes PI for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. This means any party that processes information on behalf of FirstRand.
PAIA	The Promotion of Access to Information Act 2 of 2000.
PCI standard	Means Payment Card Industry standard.

Personal information (PI)	Means information relating to an identifiable, living, natural person and where it is applicable an identifiable, existing juristic person, including, but not limited to: (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other PI relating to the person or if the disclosure of the name itself would reveal information about the person. In reference to this policy, PI must be seen primarily but without limitation as PI of group customers, employees and suppliers, and other persons and third parties.
PIN	Means "personal identification number", which is a secret numeric password known only to the user and a system to authenticate the user to the system.
POPIA	Protection of Personal Information Act 4 of 2013.
Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning PI, including: (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
Public record	Means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
Record	Means any recorded information: (a) regardless of form or medium, including any of the following: (i) writing on any type of material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) a label, marking or other writing that identifies or describes anything of which it forms a part, or to which it is attached by any means; (iv) a book, map, plan, graph or drawing; (v) a photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) being in the possession of or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.

Responsible party/ies	Means a public or private body or any other person which/who, alone or in conjunction with others, determines the purpose of and means for processing PI. In reference to this policy, the responsible parties are the FirstRand entities as defined above.
Sensitive cardholder PI	This information includes but is not limited to card validation codes/values, full track PI (from the magnetic strip or equivalent on a chip), PINs and PIN blocks. Authentication must be against cardholders and/or authorised payment card transactions in terms of PCI.
Special personal information (SPI)	Means any PI of a data subject, concerning: (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to: (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Supplier	Means a natural or juristic person who provides a product or renders services to the group.
DEFINITIONS FROM THE GDPR	
Controller	Means a juristic person in the group, registered in the United Kingdom, Guernsey or Jersey who, alone or jointly with others, determines the purposes and means for processing PI. Such purposes and means will be determined by the GDPR or privacy laws in the United Kingdom, Guernsey or Jersey.
Processor	Means a juristic person who processes PI on behalf of the controller.
Sub-processor	Means a juristic person defined in Annexure A of this policy.

3 APPLICABILITY

This policy is applicable to all suppliers and business partners who collect and/or process PI and or/records for, on behalf of or together with the group. The group will at the time of the conclusion of any agreement, and regularly during the course and scope of its agreement with suppliers or business partners who collaborate with the group or provide goods and/or services which require the collection and/or processing of PI and/or records in accordance with this policy, provide them with a copy of this policy.

4 SCOPE OF APPLICATION

This policy is applicable to all PI, SPI and children's PI collected, retained, processed and disseminated by all suppliers and applicable business partners for, on behalf of, or together with the group in terms of an agreement between the group and the supplier or the business partner. This includes but is not limited to PI, SPI and/or children's PI of the employees of the group, group customers, employees of group customers, and third parties whose PI is in the possession of the group and subsequently processed on the group's behalf by the supplier or business partner.

This policy supports FirstRand's internal policies. Suppliers and business partners will be informed if they need to adhere to any other internal policy.

5 SUPPLIERS AND BUSINESS PARTNER OBLIGATIONS WHEN DEALING WITH PI AND RECORDS

5.1 Accountability

5.1.1 The supplier or business partner acknowledges and accepts that any PI and/or records received from the group and/or created by it for or on behalf of the group will not become the property of the supplier or business partner.

5.1.2 The supplier or business partner shall at all times be solely and fully responsible for all its employees, agents, subcontractors and other third parties who act on its behalf in the performance of their functions in terms of its relationship with the group.

5.1.3 The supplier or business partner may only make use of agents, subcontractors and third parties for the processing of the PI if:

- the group has been informed of the agent, subcontractor and third party used and such agent, subcontractor and third party has been approved by the group in writing;
- the supplier or business partner has conducted a privacy risk assessment of the agent, subcontractor and third party and the said agent, subcontractor and third party has passed the risk assessment and has the appropriate and necessary controls to mitigate any privacy risks; and
- the supplier or business partner concludes agreements with such agents, subcontractors and third parties on no less onerous terms than that which the supplier or business partner agreed on with the group.

5.1.4 By contracting with the group the supplier or business partner, in its performance of its mandate or the obligations under the applicable agreement, undertakes that its employees, agents, subcontractors and other third parties who act on its behalf in the performance of its functions in terms of its relationship with the group, and who shall have access to the group's PI and/or records, have signed the appropriate confidentiality undertakings; and that the supplier or business partner acknowledges and confirms that:

- it has appropriate internal policies dealing with privacy and security in place for purposes of compliance with privacy legislation;
- it has external privacy notices or policies which advise data subjects how it processes PI and which notices are aligned to the disclosure obligations of privacy legislation;
- its employees, agents, subcontractors and third parties have been provided with the appropriate training to ensure that they understand the provisions of privacy legislation and PI privacy principles in general, as well as their roles and responsibilities in relation to the provision of service to the group as a responsible party;
- it will at all times adhere to the provisions, updates and amendments of privacy legislation;
- when processing PI of children or SPI, it will at all times act in accordance with any special provisions provided for in privacy legislation and the provisions of the agreement with the group; and
- it will share PI with its agents, employees' subcontractors and other third parties only as strictly necessary, and to the extent necessary to process the PI in accordance with the agreement with the group.

The following policy statements relate only to the GDPR, where in scope:

5.1.5 Where the supplier or business partner is confirmed as a processor by the group, and where, as a result of providing the service to a controller and such a service requires the collection and/or processing of PI belonging to the controller, the controller and the supplier will conclude a PI transfer agreement on the terms outlined in Annexure A (which are not negotiable).

5.1.6 Where the supplier or business partner is confirmed as a sub-processor by the group, as a result of providing the service to the group, who is a processor, and such a service requires the collection and/or processing of PI belonging to a controller, the supplier or business partner will conclude a data transfer agreement with the group on the terms set out in Annexure A of this policy (which is not negotiable).

The following policy statement relates only to the provision of cloud services, where in scope:

5.1.7 Where the supplier is a cloud service provider, the group will provide to the supplier its cloud services-specific terms and conditions, which will be incorporated into the agreement with the supplier.

5.2 Processing limitation

5.2.1 The supplier or business partner will, as far as possible, collect PI directly from the data subject to whom the PI relates unless: the information is contained in or derived from a public record; or deliberately made public by the data subject; or the data subject has consented thereto; or it is in the legitimate interest of the data subject or the group; or collection from another source is legally required; or needed for court proceedings or national security; or otherwise directed in writing by the group; or such PI and/or record is provided by the group.

5.2.2 The supplier or business partner will process PI of data subjects lawfully and in a reasonable manner so that it does not unreasonably intrude on the data subject's right to privacy. The supplier or business partner will ensure that, where legally necessary for a particular processing action, consent is collected from the data subject as per the instructions provided by the group, and that such consent will be retained as per records management best practice principles.

5.2. Purpose specification

5.2.3 The supplier or business partner shall collect PI and/or records only as far as such PI is necessary for the supplier or business partner to comply with the agreement, or for the exercise of the supplier's rights or instructions in terms of the agreement with the group.

5.2.4 The group requires the supplier or business partner to maintain all PI and/or records for the period required by the applicable legislation and to keep an up-to-date retention schedule as required by records management principles. The supplier or business partner will be required to maintain the records and apply records management best practice principles to all PI, in accordance with the applicable legislation, irrespective of the form. All retention periods, disposal methods and/or processes must be documented and the evidence of the destruction of all records must be maintained. A copy or applicable extract of the group's records retention and destruction policies will be made available where necessary or required.

5.3 Further processing limitation

5.3.1 The supplier or business partner shall only collect and/or process PI and/or records for the purpose for which it was originally collected and to fulfil all its obligations to the group in terms of its agreement with the group.

5.3.2 If there is a requirement for any further processing of PI and/or records, authorisation from the group will be requested in writing by the supplier or business partner. No reliance may be placed by the supplier or business partner on the exceptions contained in section 15 of POPIA.

5.4 Information quality

5.4.1 The supplier or business partner shall ensure that, where PI is processed in fulfilment of its obligations under any agreement with the group, that such PI is complete, accurate, not misleading and updated where necessary. Should the supplier or business partner become aware of any PI changes, the supplier or business partner must as soon as practically possible inform the group of such changes; and whether a data subject's PI is incomplete, inaccurate or misleading so that the necessary updates are made.

5.5 Openness

5.5.1 If the supplier or business partner collects PI, SPI or children's PI on behalf of the group, the supplier or business partner must notify the data subject from whom the information is being collected, to the extent required by applicable privacy laws, of the following:

- that the supplier or business partner is acting on behalf of the group;
- what information is being collected;
- the purpose of the collection of that information;
- any legal requirements for collection;
- whether the supply of the information is voluntary or mandatory;
- the consequences for failure to supply such information;
- the name and address of the responsible party;
- where applicable, whether the responsible party intends to transfer the information across a border or borders, to another country and the level of protection afforded the information by that country;
- the right of the data subject to access and correct the PI; and
- any further information as required by the group (such as the recipients of the information, existence of the right to access/rectify the information, existence of the right to object to the processing of the information, and the right to lodge a complaint to the Information Regulator and its contact details).

5.5.2 All employees, agents and subcontractors of the supplier or business partner shall take reasonable steps to identify themselves to a data subject who has been contacted. Further to that, the data subject must be informed that the said supplier or business partner is acting on behalf of the group.

5.6 Security safeguards

5.6.1 The supplier or business partner shall secure the integrity and confidentiality of all PI and/or records in its possession by putting appropriate, reasonable, technical and organisational measures in place to prevent loss or unauthorised destruction of PI, as well as to prevent unlawful access to or processing of PI in the supplier's or business partner's possession.

5.6.2 The supplier or business partner must complete the the group PI third-party privacy assessment prior to the conclusion of the agreement. The control environment must be agreed upon with the group prior to the commencement of the engagement.

5.6.3 The supplier and business partner are prohibited from disclosing or transferring PI and/or records to any external third party, except for the purposes of fulfilling their obligations in terms of the relationship with the group; or unless otherwise directed to do so by the group in writing; or unless otherwise required by law.

5.6.4 Where the supplier or business partner is requested to disclose PI and/or records for a purpose not authorised under the agreement with the group, or if disclosure is required by law, then the supplier or business partner will immediately notify the group regarding the request or demand disclosure in writing, and must not disclose the PI unless directed to do so in writing by the group, or unless otherwise required by law. Where disclosure is required by law, the supplier or business partner will, where possible, provide the group with reasonable written notice of such requirement in order to provide the group with an opportunity to exercise its rights, and will only disclose such PI and/or records as it is strictly required to disclose by law.

5.6.5 The supplier or business partner shall identify all reasonably foreseeable internal and external risks to PI in the fulfilment of its obligations in terms of the agreement with the group. Appropriate safeguards must be established and maintained against the identified risks. Regular verification of the effective implementation of such safeguards and continual review and updates of safeguards in response to new risks must be undertaken by the supplier and business partner. Records of the reviews must be retained.

5.6.6 The group may, at any time and upon reasonable notice to the supplier or business partner, enter the premises of the supplier or business partner to inspect or audit, or request a third party to audit the supplier's or business partner's compliance with this policy. This includes but is not limited to security and information management requirements under the provisions of privacy legislation and/or the terms and conditions of the agreement as concluded between the supplier or business partner and the group. The supplier or business partner is required to cooperate with any such audit or inspection.

5.6.7 The supplier or business partner must notify the responsible party (the group) immediately where there are reasonable grounds to believe that the PI that it processes on behalf of the group has been accessed or acquired by any unauthorised person or entity.

5.6.8 The group will nominate a contact person to receive such privacy incidents, which will also be specified in the agreement.

5.6.9 At the time of the privacy incident, the supplier or business partner must report the privacy incident information to the group as per Annexure B.

5.6.10 The group will put in place internal processes and procedures with clearly defined roles and responsibilities. This will ensure that the discovery or identification, recording and management of security compromises as they arise, are in line with its internal privacy incident management plan.

5.6.11 In the event that the supplier or business partner handles or processes payment card information on behalf of the group, they must at all times fully comply with the relevant and current standard as outlined in the Payment Card Industry Data Security Standard (PCI DSS) (www.pcisecuritystandards.org) to ensure continuous protection of sensitive cardholder data. The supplier or business partner will at all times be responsible for security when processing and transmitting card information and PI. The group may, as and when required, request proof of compliance to PCI DSS.

5.7 Data subject participation

5.7.1 A data subject has the right to, after providing adequate proof of identity and after payment of any fee required by law (if applicable):

- enquire if PI about them has been collected by the supplier or business partner on behalf of the group;
- enquire how the PI is being used by the supplier or business partner whilst acting on behalf of the group;
- enquire whom the information has been disclosed to by the supplier or business partner whilst acting on behalf of the group;
- challenge the accuracy and completeness of PI in the possession of the supplier or business partner who is acting on behalf of the group;
- object to the processing of such PI by the supplier or business partner who is processing on behalf of the group; and
- withdraw their consent to the processing of their PI by the supplier or business partner who is processing on behalf of the group.

5.7.2 The supplier or business partner must immediately direct any requests by a data subject to access and/or amend any PI, or requests to withdraw consent to the processing of their PI that the supplier or business partner holds on behalf of the group, to the group to be handled in terms of the group's PAIA manual and process.

6 AUDIT AND INSPECTION OF PI AND RECORDS

6.1 Prior to the conclusion of any agreement with any supplier or business partner that will process PI and/or records on behalf of the group, the group may conduct a third-party privacy assessment when required.

6.2 The group reserves the right to audit, upon providing the supplier with reasonable notice of the said audit, the controls implemented by the supplier and business partner throughout the duration of the agreement, as a measure of continued due diligence or privacy risk mitigation on the part of the group.

6.3 The group reserves the right to audit:

- the supplier's or business partner's adherence to privacy principles, as well as security, information and records management practices, but most importantly the supplier's or business partner's compliance with the policy requirements set out herein; and
- the PI and/or records that the supplier or business partner holds on behalf of the group in performance of its obligations towards the group.

7 CROSS-BORDER TRANSFER

7.1 In cases where the supplier or business partner (or any of its subcontractors) is domiciled outside the Republic of South Africa, or transfers PI and/or records outside the Republic of South Africa whilst collaborating with or providing the group with goods and/or services, such information may only be transferred in terms of the agreement with FirstRand.

7.2 Where the processing of PI occurs in a country which has legislation more stringent than POPIA, then the more stringent legislation's provisions will be applicable to the processing of such personal information.

7.3 The supplier and business partner may not transfer PI that is being processed on behalf of the group outside the borders of the Republic of South Africa unless:

- the supplier, business partner or third party who is receiving the information is subject to a PI protection law, binding corporate rules or binding agreement rules that effectively uphold the principles of reasonable processing and contain provisions that have substantively similar provisions to POPIA regarding transfer of PI to foreign jurisdictions;
- the data subject has provided consent for the transfer;
- the transfer of such PI is required for the performance of a contract between the data subject and the group;
- the transfer of such PI is necessary for the performance of a contract concluded between the group and a third party, in the interest of the data subject;
- the transfer of such PI is for the benefit of the data subject and it is not practical to obtain consent and the data subject would have provided such consent had the data subject been able to; or
- with the prior written approval of the group.

8 NOTIFICATIONS BY SUPPLIER OR BUSINESS PARTNER TO THE GROUP

8.1 All notifications to the group relating to access to PI and/or records in the possession of a supplier or business partner that contain PI but belong to the group, shall be addressed to the group in writing.

8.2 These notifications include notifications to comply with requests from the Information Regulator in terms of POPIA compliance; requests for access to PI; requests to address complaints from the Information Regulator; and requests to access information, in terms of PAIA, that is the property of the group.

9 THIRD-PARTY MANAGEMENT

9.1 The supplier or business partner must inform the group in writing, prior to engaging the services of a third party or subcontractor, to assist in providing services in terms of the main agreement with the group. The group may approve or decline the use of such third party or subcontractor.

9.2 Where the group approves the appointment of such third party or subcontractor, the supplier or business partner shall provide the group with written confirmation of such appointment, which includes the identity and location of such third party or subcontractor.

9.3 The supplier or business partner may only disclose PI and/or records to third parties under the following circumstances:

- in the case that the supplier or business partner has contracted with a third party to provide goods and/or services on behalf of the supplier or business partner in order for the supplier or business partner to perform its obligations under the agreement with the group;
- has the consent of the data subject;
- to protect the legitimate interest of the data subject;
- to pursue the legitimate interest of the group;
- to pursue the legitimate interest of a third party; or
- in cases where the supplier or business partner is under a legal duty to share PI and/or records, to comply with a legal obligation.

9.4 In sharing this information, the supplier or business partner shall ensure that the third party provides the same level of protection to the PI as required by this policy, the agreement with the group and applicable PI protection laws. The contract between the third party and/or supplier or business partner must adhere to the requirements contained in this policy. For the purposes of this section, “third party” means any person or entity other than the supplier and/or operator, the group or other persons authorised by the group to process PI for the responsible party, this being the group.

10 TERMINATION EXPECTATIONS

10.1 At termination of the agreement, the supplier or business partner will, at the direction of the group:

- return to the group all PI and/or records that contain PI that belong to the group that were created throughout the duration of the agreement, including PI and/or records that were provided to the supplier and business partner at the inception of the engagement with the group, irrespective of when they were created or provided; or

- provide the group with the destruction certificate indicating that all PI and/or records that contain PI that were the possession of the supplier or business partner have been destroyed; and
- ensure that all PI and/or records in the possession of a third party (as defined in paragraph 9.4) or subcontractor are returned to the group.

11 GENERAL

The group reserves its right to enforce its rights as stated in the agreement between the group and the supplier or business partner if the supplier or business partner fails to comply with the provisions of this policy or the applicable legislation provisions. Failure to comply with the provisions of this policy may, without limitation, result in legal action and/or termination of the master agreement with the group.

12 OWNERSHIP AND REVIEW

This policy is owned by FirstRand Group Compliance and must be reviewed at least every two years. This policy will also be reviewed when any applicable code of conduct under POPIA is published or there is any amendment to any overarching legislation.

-END-

ANNEXURE A

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 to a 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 certain safeguards, 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 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.

(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 December 2001 on standard contractual clauses for the transfer of 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 scope of 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 Federation of 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 have the 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 represented 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 irrespective of the Member State from which the data transfer originates, in particular in those cases where the data importer receives data for further processing from different establishments of the data exporter in the 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 processors established outside the European Union should not prejudice the fact that the processing activities should be 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 transferred by 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 safeguards of 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 under the 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 established 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 freedoms of 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 a sub-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 where those 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 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 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 data exporter, 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 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 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 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 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 in accordance 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.

ANNEXURE B

Reporting of privacy incidents by suppliers and business partners

(a) Reporter information

Name, surname, employee number, email address, cell number of person reporting the privacy incident.

(b) Description of the privacy incident circumstances

1. Root cause information relating to the privacy incident. The root cause should be further classified according to external causal factors (e.g. phishing attacks, denial of services); people causal factors (e.g. unauthorised activity by internal or external staff in relation to the PI); governance causal factors (e.g. no proper escalation processes and lack of proper oversight in relation to PI processing activities); process causal factors (e.g. inefficient/ineffective process design or inadequate or ineffective procedures in relation to the exchange of PI with third parties); and technology, infrastructure, facilities causal factors (e.g. inadequate data/system security, including access/protection/configuration).
2. Does the privacy incident involve identifiable PI or is the PI anonymised?
3. Date of the privacy incident.
4. Who was the privacy incident reported to?
5. Systems involved?
6. How many (volume of) records affected?
7. How many customers/data subjects affected?
8. Does the privacy incident include special personal information or sensitive information of a data subject?
9. Group operating business/customer segments/business unit(s) affected.

(c) Remediation actions

Information relating to the remedial actions undertaken by the supplier or business partner. Such actions should be described in detail.

(d) Non-compliance to privacy law and/or other legislation

Specify which sections in the applicable privacy legislation has been breached.