Data Processing Agreement

The agreement between a controller and their processor to fulfil the controller's obligation to enter into a contract with the processor and vice versa.

between the **Customer / End-User** (the "controller")

and **Sage South Africa (Pty) Ltd** (the "processor")

Organisation or person's name	Sage South Africa (Pty) Ltd
Registration or identification number	2003/015693/07
Physical address	6th Floor, Gateway West Offices, 22 Magwa Crescent, Waterfall, Midrand

Agreement

1. Introduction

This is the agreement between:

- **the controller** – a company incorporated under the laws of the country of their incorporation in terms of the applicable Order; and
- **Sage South Africa (Pty) Ltd – the processor** – a company incorporated under the laws of the Republic of South Africa;

each having their registered offices and principal business places at the physical addresses and with the registration or identification numbers specified on this agreement's cover page, to fulfil controller's obligation as a controller to enter into a contract with processor as controller's processor and visa versa.

2. Definitions, parties, principal agreement and interpretation

2.1. ***Definitions***. In this agreement:

'applicable data protection laws' means relevant data protection laws, including:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); and
- the South African Protection of Personal Information Act 4 of 2013;

together with any:

- national implementing laws;
- ePrivacy laws; and
- other related laws agreed between the parties in writing;

'appropriate technical and organisational measures' means regarding a given goal, the technical and organisational efforts that a reasonable person in processor's position would use to achieve that goal as quickly, effectively, and efficiently as possible;

'personal data' means any information about a living human being or existing organisation (as applicable data protection laws require), provided that someone is capable of identifying them from that information;

'personnel' means any:

- director, employee, or other person who works (permanently or temporarily) under either party's supervision; or
- person who renders services to either party for the purpose of their obligations under this agreement as their agent, consultant, contractor, or other representative;

'processing' means doing anything with personal data, including gathering it, disclosing it, or combining it with other information; and

'subprocessor' means any downstream processor that the processor engages to process personal data in accordance with the principal agreement and this agreement, as those documents permit.

2.2. ***Parties***. In this agreement:

the controller (unless otherwise expressly indicated in this agreement) and means the person who determines the purpose ('why') means ('how') of processing the personal data alone or in conjunction with others, although it is more important that they determine why to process the personal data than how, and those related to it; and

Sage South Africa (Pty) Ltd is the processor as specified on this agreement's cover page (unless otherwise expressly indicated in this agreement) and means the person who:

- processes personal data on controller's behalf in terms of a contract; and
- enters into this agreement with controller; and

those related to them.

2.3. ***Principal agreement meaning***. In this agreement, **'principal agreement'** means the agreement between controller and processor in terms of which processor processes personal data on controller's behalf.

2.4. ***Principal agreement terms***. The principal agreement's terms remain in full force and effect except as modified in this agreement.

2.5. **Controller's documented instructions**. In this agreement, **'controller's documented instructions'** means the principal agreement and any other relevant written agreements between the parties, unless the parties agree otherwise in writing.

2.6. ***Undefined terms***. Any terms not otherwise defined in this agreement have the meaning the principal agreement gives to them.

2.7. ***Data protection law terms***. Terms used in this agreement that have meanings ascribed to them in applicable data protection laws,

including ‘data subject’, ‘processing’, ‘personal data’, ‘controller’ and ‘processor’, carry the meanings set out under those laws to the extent that this principal agreement does not define them.

2.8. ***Agreement terms prevail***. This agreement’s provisions will prevail in the event of a conflict between any of the principal agreement’s provisions and this agreement’s provisions.

3. Purpose

This agreement adds supplementary requirements to controller’s principal agreement with processor and clarifies the relationship between controller and processor in terms of applicable data protection laws.

4. Application

This agreement applies when processor processing personal data on controller’s behalf for specific activities subject to applicable data protection laws to achieve controller’s purposes as set out in the principal agreement between controller and processor. It does not apply to any of processor’s:

- processing on controller’s behalf in terms of any other activity not set out in the principal agreement between controller and processor; or
- other processing, such as on processor’s own behalf.

5. Requirements

5.1. ***Measure guarantees***. Processor guarantees that they will implement appropriate technical and organisational measures to:
- meet applicable data protection laws’ requirements; and
- protect the data subject’s rights.

5.2. ***Required details***. Annexure 2 provides an overview of the following details related to the processing:
- the processing’s subject-matter;
- the processing’s duration;
- the processing’s nature;
- the processing’s purpose;
- the personal data type;
- the data subject categories; and
- the controller rights;

to the extent that the principal agreement does not specify those details.

5.3. ***Purpose pursuit***. The parties have entered into a principal agreement for the purposes set out in Annexure 2 and processor may choose the means they consider necessary to pursue those purposes in their own discretion, provided that their choices are compatible with:
- this agreement’s requirements; and
- particularly controller’s written instructions.

5.4. ***Downstream processor contracts***. Processor must respect the conditions for downstream processor contracts in terms of applicable data protection laws.

5.5. ***Downstream contract***. Processor must enter into a contract or other written agreement with any subprocessor to govern processing by a subprocessor in the same way as the contract or other agreement between controller and processor, particularly when it comes to appropriate technical and organisational measures.

6. Controller and processor

6.1. ***Determination by controller***. Controller will determine the scope, purposes and manner by which processor may access or process the personal data, to the extent that the principal agreement does not adequately describe processor’s data processing activities.

6.2. ***Processing instructions***. Processor may only process the personal data:
- on controller’s documented instructions;
- to the extent that providing the services related to the processing activities requires them to.

6.3. ***Infringing instructions notification***. Processor will immediately tell controller if they believe that any instruction infringes applicable data protection laws, provided that this:
- is not an obligation to monitor or interpret the laws that apply to controller; and
- does not constitute legal advice to controller.

6.4. ***Controller’s warranties***. Controller warrants that:
- they (and their instructions to process personal data) comply with applicable data protection laws;
- they have all necessary rights to provide the personal data to processor for the processing to be performed in relation to the services related to the processing activities;
- one or more lawful grounds set out in applicable data protection laws support the lawfulness of the processing; and
- their instructions to processor or any subprocessor relating to processing of personal data will not put processor or any subprocessor in breach of applicable data protection laws.

6.5. ***Controller's responsibilities***. Processor may charge controller (and controller is responsible for payment) where processor assists controller with controller's data protection requirements or otherwise. Controller is responsible for making sure that certain designated personnel within their organisation:

- provide all necessary privacy notices to data subjects;
- obtain any necessary data subject consent to the processing;
- maintain a record of such consent;
- communicate the fact that a data subject has revoked consent to processor where a data subject does so;

to the extent that applicable data protection laws require.

7. Data sharing

7.1. ***Responsibility for secure data transfer***. Each party is responsible for the secure transfer of any data they share with the other party.

7.2. ***Technical and organizational safeguards for secure data transfer***. Each party must take appropriate technical and organisational measures to make sure that they transfer data securely to the other party. Technical measures may include the use of:

- a virtual private network (VPN);
- secure file transfer protocol (SFTP);
- a web portal or an application with an encrypted connection; or
- any other means that will sufficiently secure the data stream from any incident that may compromise the integrity of the data concerned.

Organisational measures may include any methods that make sure personnel implement these technical measures, such as:

- written policies;
- documented procedures; and
- necessary training.

8. Confidentiality

8.1. ***Authorised persons confidentiality***. Processor must make sure that their personnel authorised to process the personal data have committed themselves to confidentiality, such as by:

- signing an appropriate confidentiality agreement; or
- being otherwise bound to a duty of confidentiality;

or are under an appropriate statutory obligation of confidentiality.

9. Security

9.1. ***Data security***. Controller and processor will implement appropriate technical and organisational security measures to make sure that the level of security is appropriate to the risks to the personal data in terms of applicable data protection laws, taking into account the:

- state of the art (being the most recent level of development of technology of security measures at that particular time);
- implementation costs;
- processing nature, scope, context and purposes; and
- varying risks to people's rights and freedoms in terms of likelihood and severity.

9.2. ***Security policies***. Controller and processor will each maintain and fully implement written security policies that apply to personal data processing.

9.3. ***Audits***. Processor must allow for and contribute to audits (including inspections) by the controller or another auditor that they mandate. Processor must immediately tell controller if they think the instruction to allow for and contribute to audits breaks the law.

9.4. ***Audit terms.*** Controller will be responsible for the cost of engaging any third-party auditor to conduct an audit. If processor has commissioned an audit.report which it offers to make available to controller, controller may only perform (or commission a third-party auditor to perform) its own audit if controller, acting in good faith, is reasonably dissatisfied with processor's audit report. Controller must (and must ensure that their third-party auditor does):

- coordinate timing and scope of audit with processor, so as to limit impact on processor's services;
- exclude processor's other customers' data (including personal data) from the audit;
- acquire processor's approval before using any tools or software on processor's infrastructure;
- not include in the audit any sensitive data (including personal data, special personal data, or data that could harm the security of the services described in the principal agreement);
- give processor a reasonable opportunity to review the audit report and resolve any questions or issues of fact; and
- keep the results of any audit confidential and not disclose them, unless otherwise required by law.

9.5. **Evidence of compliance**. Processor may use their adherence to either an approved:

- code of conduct; or
- certification mechanism;

recognized under applicable data protection laws as an element to show compliance with the requirements set out in relevant data

protection laws, provided that the code of conduct or certification mechanism also addresses the requirements contained in Annexure 3.

10. Improvements to security

10.1. ***Cost negotiations***. The parties will negotiate the cost to implement material changes required by specific updated security requirements set out in applicable data protection laws or by data protection authorities of competent jurisdiction in good faith.

10.2. ***Amendment negotiations***. The parties will negotiate an amendment to the principal agreement in good faith where one is necessary to execute a controller instruction to processor to improve security measures as may be required by changes in applicable data protection laws from time to time.

11. Data transfers

11.1. ***Transferring instructions***. Processor may only transfer personal data to a third country or international organisation on controller's documented instructions, unless required to do so by applicable law. Processor must tell controller about the legal requirement before processing the personal data, unless the law prohibits them from doing so in the public interest.

11.2. ***Pre-authorised transfers***. Controller grants its authorisation for the transfers set out in Annexure 4 on conclusion of this agreement.

11.3. ***Statutory mechanism cooperation***. The parties agree to cooperate in good faith if they are relying on a specific statutory mechanism to standardize international data transfers and:

- the relevant authority subsequently modifies or revokes that mechanism; or
- a court of competent jurisdiction holds it to be invalid;

by:

- promptly suspending that transfer; or
- pursuing a suitable alternate mechanism that can lawfully support the transfer.

11.4. ***Responsibility.*** Controller is responsible and processor is not responsible for any transfers of personal data that occurs where controller (or controller's users or customers) access the services described in the principal agreement through a browser from a third country or international organisation.

12. Processing of personal data outside of the European Economic Area (EEA)

12.1. ***The SCCs***. The standard contract clauses are the clauses set out in the European Commission's Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to data-processors established in third countries, under the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (as the European Commission may amend or replace from time to time). They are incorporated into this agreement by this reference and attached in their current form as Annexure 5.

12.2. ***Where they apply***. The standard contract clauses apply to any processing where the parties:

- directly (or via onward transfer) transfer personal data outside of the EEA or otherwise to an undesignated territory; or
- processes personal data originating in the EEA outside of it or otherwise in an undesignated territory.

An undesignated territory is another territory outside the EEA that the European Commission has not designated as ensuring an adequate level of protection according to relevant data protection law.

12.3. ***Where they don't apply***. They do not apply:

- to any personal data that the parties otherwise transfer or process; or
- where the parties have adopted binding corporate rules or a similar mechanism or alternate recognised compliance standard for the lawful transfer of personal data outside the EEA.

12.4. ***Transfer impact assessment***. controller will, with processor's cooperation and assistance, assess whether each intended transfer of personal data meets the following requirements:

- the level of protection of the third country meets the level that applicable data protection laws require; and
- the laws of the third country enable processor to comply with the SCCs.

If the intended transfer does not meet these requirements, the parties will:

- take supplementary measures to ensure a level of protection equivalent to the protection that applicable data protection laws provide; and
- implement any guidance from the relevant supervisory authority to determine those supplementary measures.

13. Information obligations and incident management

13.1. ***Processor incident notification***. Processor must notify controller after becoming aware of a personal data incident without undue delay, provided that the incident has a material impact on personal data processing that is the subject of the principal agreement.

13.2. ***Incident scope***. A personal data incident means:

- a complaint or a request regarding the exercise of a data subject's rights under applicable data protection laws;
- an investigation into or personal data seizure by government officials, or a specific indication that such an investigation or

seizure is imminent;

- any unauthorized, accidental or otherwise unlawful personal data processing;
- any breach of security or confidentiality in terms of this agreement leading to confirmed or possible risks to the personal data; or
- where implementing an instruction received from controller would violate applicable laws to which controller or processor are subject, in the opinion of processor.

13.3. ***Incident notification requirements***. Processor will address any incident notifications to the controller's employee whose contact details are set out in Annexure 1 of this agreement and should contain the following information to assist controller in fulfilling its obligations under applicable data protection laws:

- a description of the nature of the incident, including where possible the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of processor's data protection officer or another contact point where controller can obtain more information; and
- a description of the likely consequences of the incident.

14. Contracting with subprocessors

14.1. ***Downstream processor restriction***. Processor may not subcontract any of their services related to the processing activities consisting of the processing of the personal data or assign their obligations to another processor without controller's:

- general written authorisation (provided that the processor tells the controller the details of any processor that they intend to subcontract or assign their obligations to and gives the controller an opportunity to object); or
- prior specific authorisation.

14.2. ***Prior specific authorisation***. Controller authorises processor to engage the subprocessors listed in Annexure 4 for the data processing activities related to the services described in Annexure 2.

14.3. ***Subprocessor changes***. Processor will inform controller of any addition or replacement of subprocessors and give controller an opportunity to object to such changes, provided that:

- the parties will make a good-faith effort to resolve controller's objection if controller timeously sends processor a written objection notice, setting forth a reasonable basis for objection; and
- each party may terminate the portion of the service which cannot be provided without the subprocessor and controller may request a pro-rated refund of the applicable service fees if processor's efforts are not successful within a reasonable time.

14.4. ***Processor remains liable***. Processor remains fully liable to controller for any subprocessor's failure to perform their data protection obligations despite controller's authorisation.

14.5. ***Processor's subprocessor obligations***. Processor will:

- make sure that the subprocessor is bound by data protection obligations compatible with those of processor under this agreement; and
- impose on its subprocessors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of applicable data protection laws.

14.6. ***Controller's verification right***. Controller may make sure that processor has complied with its obligations that controller has imposed on them in conformity with this agreement by:

- requesting that processor audit a third party subprocessor; or
- providing confirmation that such an audit has occurred.

15. Relationship management

15.1. ***Data protection officer***. Both parties will appoint a data protection officer or other contact point, primarily responsible for the management of the relationship between the parties and the processing of personal data.

15.2. ***Information security officer***. Both parties will appoint an information security officer primarily responsible for the technological and organisational measures necessary to establish and maintain the information security safeguards for personal data.

15.3. ***Contact information***. Annexure 1 records the name, phone number, mobile number and email address of the data protection officer or other contact point and information security officers of both parties.

15.4. ***Regular meetings***. The data protection officers or other contact points and any persons who the data protection officers or other contact points may deem necessary, will meet as often as may be necessary but no less than once every three months, to consider the processing of personal data by operator. These meetings will cover the following routine agenda items:

- the confirmation of the identity and contact details of the data protection officers or other contact points and information security officers of both parties;
- compliance with applicable data protection laws, rulings of relevant data protection authorities and the security measures contained in Annexure 3;
- novel threats that may pose a risk to personal data;
- advances in technologies and plans of either party to use different technologies; and
- any other relevant issue that may impact on the processing of personal data.

The data protection officers or other contact points of both parties will cooperate to:

- prepare an agenda including the routine agenda items and any other issues for each meeting;
- minute the proceedings of each meeting, distribute the minutes of the meeting to all relevant parties within five business days of the meeting having taken place; and
- if necessary, prepare amendments to annexures to this agreement for acceptance by the respective data protection officers or other contact points or information security officers and filing with the agreement.

16. Return or destruction of personal data

16.1. ***Deletion or return obligations***. Processor must:

- delete or return all the personal data to controller, at the controller's choice; and
- delete all existing copies unless the law requires them to continue to store those copies;

when:

- processor has finished providing processor with the services related to the processing;
- this agreement terminates;
- controller requests processor to do so in writing; or
- processor has otherwise fulfilled all purposes agreed in the context of the services related to the processing activities where controller does not require them to do any further processing.

16.2. ***Processor's third party termination obligations***. On termination of the agreement, processor will notify all third parties supporting its own personal data processing.

17. Assistance to controller

17.1. ***Help controller respond***. Processor must help controller with appropriate technical and organisational measures to fulfil their obligation to respond to requests by data subjects exercising their rights, provided that:

- processor will assist controller with appropriate technical and organisational measures insofar as possible to respond to requests by data subjects exercising their rights; and
- controller will be responsible for reasonable costs processor incurs in providing this assistance.

17.2. ***Other help to controller***. Processor must help controller with:

- their obligations regarding security of processing; and
- their prior consultation obligations in terms of applicable data protection laws;

considering the nature of the processing and the information available to processor.

17.3. ***Make compliance information available***. Processor must make all information necessary to show compliance with the legal rules that apply to processors available to controller on request.

18. Liability and indemnity

Each party indemnifies the other and holds them harmless against all claims, actions, third party claims, losses, damages and expenses that the other party incurs arising out of a breach of this agreement or applicable data protection laws by the indemnifying party, provided that:

- each party provides the other with a notice of the claim promptly after receiving it;
- the indemnified party gives the indemnifying party the right to control the defense;
- the indemnified party will provide the indemnifying party with reasonable assistance as necessary; and
- the indemnified party will avoid admission of liability.

19. Duration and termination

19.1. ***Commencement***. This agreement will come into effect on the effective date of the principal agreement.

19.2. ***Duration***. Processor will process personal data until the principal agreement expires or terminates, unless:

- controller instructs them to do otherwise; or
- they or their subprocessor (as the case may be) returns or destroys the personal data (at controller's choice).

20. General

20.1. ***Governing law***. This agreement is governed by the laws of country specified in the relevant provisions of the principal agreement.

20.2. ***Dispute resolution***. Any disputes arising from or in connection with this agreement will be brought exclusively before the competent court of the jurisdiction specified in the relevant provisions of the principal agreement.

Annexure 1: Officer Contact Information

1. Processor's data protection officer or contact point

Contact information of processor's data protection officer or other appropriate contact point:

privacy.ZA@sage.com

Annexure 2: Requirement Details

1. Processing subject-matter

The processing's subject-matter:

The provision of the processor's services to the controller, as detailed in the principal agreement.

2. Processing duration

The processing's duration:

The duration of the principal agreement, including any transitional periods before the start or after termination of the principal agreement.

3. Processing nature

The processing's nature:

Any or all of the following processing natures, depending on the services described under the principal agreement, the controller's use of or requirements for the services, any specific requirements described in the principal agreement, or any third party requests or other extraneous events:

- Collection
- Recording
- Organisation
- Structuring
- Storage
- Adaptation/alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission / dissemination or otherwise making available
- Alignment / combination
- Restriction
- Erasure / destruction
- Others: .....

4. Processing purpose

The processing's purpose:

Any or all of the following processing purposes, depending on the relevant circumstances:

- Providing the services described under the principal agreement
- Concluding contracts
- Adhering to obligations imposed by law or regulation
- Engaging in processor's legitimate interests
- As otherwise described in the principal agreement
- Others: .....

5. Personal data type

The personal data type:

Any or all of the following personal data types, depending on the purposes:

- **Personal details** – being any information that identifies the data subject and their personal characteristics (e.g. name, address, contact details, age, sex, date of birth, physical description and any identifier issued by a public body, including a national identity number or passport number);
- **Education and training details** – being any information which relates to the education and any professional training of the data subject (e.g. academic records, qualifications, skills, training records, professional expertise, and student and pupil records);
- **Family, lifestyle and social circumstances** – being any information relating to the family of the data subject and the data subject's lifestyle and social circumstances (e.g. current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities and membership of charitable or voluntary organisations);
- **Employment details** – being any information relating to the employment of the data subject (e.g. employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records and security records) and pension information);
- **Financial details** – being any information relating to the financial affairs of the data subject (e.g. income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details and pension information);

- **Goods and services provided** – being any information relating to goods and services that have been provided (e.g. goods or services supplied, licences issued, agreements and contracts);
- **Special categories of personal data** – being racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a data subject, data concerning health or data concerning a data subject's sex life or sexual orientation;
- **Criminal data** – being any criminal convictions and offences or related security measures, including personal data relating to: (a) the alleged commission of offences by the individual (b) proceedings for an offence committed or alleged to have been committed by the individual or the disposal of such proceedings, including sentencing;
- Others: .....

6. Data subject categories

The data subject categories:

Any or all of the following categories of data subjects relating to the controller, depending on the purposes:

- Staff, including volunteers, agents, and temporary or casual workers
- Customers or clients
- Suppliers
- Contact persons of corporate entities (e.g. at suppliers, customers or clients)
- Members or supporters (including shareholders)
- Complainants, correspondents or enquirers
- Relatives, guardians or associates of other data subjects
- Advisers, consultants and other professional experts or legal representatives
- Partners, resellers
- Donors, supporters
- Students (if input by controller)
- Offenders and suspected offenders (if input by controller)
- Landlords or tenants
- Users of the services (described in the principal agreement) not included in the above
- Others: .....

Annexure 3: Security Measures

See **https://www.sage.com/en-gb/legal/status/governance/**

Annexure 4: Authorized Cross-border Transfers (only complete if applicable)

Transfers to subprocessors in third countries for which controller has granted its authorization, including countries outside the European Economic Area (EEA) without an adequate level of protection:

Subprocessor Name	**Country**
[insert]	[insert]
[insert]	[insert]
[insert]	[insert]

Annexure 5: SCCs

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

The entity identified as “controller” in the agreement

(the data exporter)

And

The entity identified as “processor” in the agreement

(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 these 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 these 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 these 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 Annex 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 these 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 these Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex 2 to these Clauses;

(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 these Clauses, with the exception of Annex 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 these Clauses, unless these Clauses or the contract contains 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 these 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 and agrees to procure that its Affiliates agree and warrant:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and these 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 these 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 Annex 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 these Clauses, or any existing contract for subprocessing, unless these Clauses or contract contains commercial information, in which case it may remove such commercial information, with the exception of Annex 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 these 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 these 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 these 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 these 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

These 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 these Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict these Clauses.

Clause 11

Subprocessing

1. The data importer shall not, and shall procure that its Affiliates shall not, subcontract any of its processing operations performed on behalf of the data exporter under these Clauses without the prior written consent of the data exporter. Where the data importer or its Affiliate subcontracts its obligations under these 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 or its Affiliate under these 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 or its Affiliate 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 these 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 these 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

Obligations 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

Please see Annexure 2 for details of the data exporter, data importer, data subjects, categories of data, special categories of data (if appropriate) and processing operations.

Appendix 2 to the Standard Contractual Clauses

Please see Annexure 3 for a description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c).