

Data Protection Terms

This document (hereafter referred to as "DP Terms") sets out Scotia Gas Networks Limited's and all of its group companies' (hereafter referred to as "SGN") terms of business in relation to data protection and shall be deemed to be incorporated into any agreement we have with any third parties (hereafter referred to as "Supplier") we engage with. If the Supplier would like to discuss any of the terms set out in these DP Terms, the Supplier should contact SGN.

1 DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in these DP Terms.

1.1 Definitions.

Business Day: means a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

Data Controller and Data Processor: have the meanings set out in the DPA until 25 May 2018, and thereafter the meaning given to the term "controller" and "processor" (respectively) in Article 4 of GDPR

Data Protection Legislation: means any laws and regulations in any relevant jurisdiction relating to privacy or the use or processing of data relating to natural persons, including: (a) EU Directives 95/46/EC and 2002/58/EC (as amended by 2009/139/EC) and any legislation implementing or made pursuant to such directives, including (in the UK) the Data Protection Act 1998 (the "DPA") and the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) from 25 May 2018, EU Regulation 2016/679 ("GDPR"); and (c) Data Protection (Charges and Information) Regulations 2018; and (d) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR; and (e) any guidance or codes of practice issued by a governmental or regulatory body or authority in relation to compliance with the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

Regulator: means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Legislation.

Request: means a request from a Data Subject to exercise its rights under the Data Protection Legislation in respect of the SGN Personal Data.

SGN Personal Data: means all Personal Data processed by the Supplier on behalf of the Data Controller under or in connection with these DP Terms.

Security Breach: means any actual loss, unauthorised or unlawful processing, destruction, damage, alteration, or unauthorised disclosure of, or access to the SGN Personal Data (accidental or otherwise) and/or any other irregularity in processing the SGN Personal Data.

Standard Contractual Clauses: means the Standard Contractual Clauses set out in the European Commission's Decision 2010/87/EU of 5 February 2010 for the transfer of Personal Data to processors established in third countries (as may be amended by agreement of the parties for compliance with applicable Data Protection Legislation requirements).

Sub-Processor: means a subcontractor (including any affiliates of the Supplier) appointed by the Supplier to process SGN Personal Data.

1.2 In these DP Terms, the terms "Data Subject", "Personal Data", "process", "processing", "transfer" (in the context of transfers of Personal Data) and "technical and organisational measures" shall have the meanings and otherwise be interpreted in accordance with the DPA until 25 May 2018, and thereafter the GDPR

- 1.3 Clause, Schedule and paragraph headings shall not affect the interpretation of these DP Terms.
- 1.4 The Schedules form part of these DP Terms and shall have effect as if set out in full in the body of these DP Terms. Any reference to these DP Terms includes the Schedules.
- 1.5 Unless the context otherwise requires, words in the singular shall include the plural and in the plural, shall include the singular.
- 1.6 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.
- 1.7 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.
- 1.8 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
- 1.9 A reference to writing or written includes faxes and email unless specified otherwise.
- 1.10 A reference to these DP Terms or to any other agreement or document referred to in these DP Terms is a reference of these DP Terms or such other agreement or document as varied or novated (in each case, other than in breach of the provisions of these DP Terms) from time to time.
- 1.11 References to Clauses and Schedules are to the Clauses and Schedules of these DP Terms and references to paragraphs are to paragraphs of the relevant Schedule.
- 1.12 Any words following the terms including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

2 PROCESSING PERSONAL DATA

- 2.1 SGN and the Supplier acknowledge that for the purpose of the Data Protection Legislation, SGN is the Data Controller and the Supplier is the Data Processor.
- 2.2 SGN and the Supplier shall, at all times, comply with the provisions and obligations imposed by the Data Protection Legislation and the data protection principles set out therein when processing SGN Personal Data.
- 2.3 In performance of its obligations under the Agreement, the Supplier shall only process the type(s) of Personal Data, and only in respect of the categories of Data Subjects and types of processing as strictly necessary in order for the Supplier to provide its services and/or products to SGN.

3 SUPPLIER'S OBLIGATIONS

- 3.1 In processing SGN Personal Data, the Supplier shall:
 - 3.1.1 process such SGN Personal Data only in accordance with SGN's written instructions from time to time (including the terms of these DP Terms) unless it is otherwise required by applicable law (in which case, unless such law prohibits such notification on important grounds of public interest, the Supplier shall notify SGN of the relevant legal requirement before processing the SGN Personal Data);
 - 3.1.2 not process the SGN Personal Data for any purpose other than those expressly authorised by the SGN;
 - 3.1.3 notify SGN if, in its opinion, SGN's instructions would not comply with the Data Protection Legislation;

- 3.1.4 notify SGN within 24 hours if it receives a Request;
- 3.1.5 provide SGN with full co-operation and assistance in relation to any Request;
- 3.1.6 not disclose any SGN Personal Data to any Data Subject or to a third party (including any subcontractor or affiliate) other than at the request of the SGN or as expressly provided for in these DP Terms to the extent which is permitted by Law; and

4 SUB-PROCESSORS

- 4.1 The Supplier shall obtain the prior written consent of SGN to the appointment of Sub-Processors.
- 4.2 Sub-Processors shall only process SGN Personal Data in order to provide one or more of the Supplier's services and/or products.
- 4.3 Prior to transferring any SGN Personal Data to a Sub-Processor, the Supplier shall enter into a written agreement with that Sub-Processor (and upon SGN's written request, provide SGN with copies of such agreements) requiring the Sub-Processor to:
 - 4.3.1 process the SGN Personal Data only in accordance with the written instructions of the Supplier; and
 - 4.3.2 abide by data protection obligations which are no less onerous than those on the Supplier set out in these DP Terms; and
 - 4.3.3 allow SGN to audit the Sub-Processor on terms equivalent to those in Clause 9.1.
- 4.4 The Supplier is responsible and liable for the Sub-Processor's compliance with its obligations under these DP Terms.
- 4.5 Where any provision of the Agreement places an obligation on the Supplier, that obligation shall be construed as an obligation on the Supplier to procure that all its Sub-Processors, and its own and its Sub-Processors personnel, to comply with such obligations.

5 SECURITY

- 5.1 In processing SGN Personal Data, the Supplier shall:
 - 5.1.1 protect the SGN Personal Data from a Security Breach by ensuring that it has in place at all times the appropriate technical and organisational measures to protect the SGN Personal Data;
 - 5.1.2 implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of security measures; and
 - 5.1.3 ensure that its personnel are the only persons permitted to process the SGN Personal Data and are: (a) subject to written (or statutory) obligations to maintain the confidentiality of SGN Personal Data; and (b) are trained on the requirements of Data Protection Legislation and their obligations in respect of SGN Personal Data under the Agreement.

6 SECURITY BREACH

- 6.1 The Supplier shall, without undue delay (and in any event within 24 hours) after discovering any Security Breach or any failure of security which leads to, or may lead to, a Security Breach, notify SGN of the same and provide full details of the Security Breach and the consequences of the Security

Breach including: (a) the date and time of when the Security Breach occurred; (b) the type of data that was the subject of the Security Breach; (c) where possible, the categories and approximate number of Data Subjects concerned; (d) the identity of each affected Data Subject that has been identified to date; (e) any notifications made to Regulators or Data Subjects about the Security Breach; and (f) details of any steps taken to remedy the Security Breach and recover or safeguard the SGN Personal Data concerned.

- 6.2 In relation to a Security Breach or other failure of security, which is discovered by the Supplier, or notified to the Supplier by SGN or a third party, the Supplier shall, at the Supplier's sole expense, cooperate with SGN in all steps as SGN may consider appropriate, including notification to the relevant Regulator or to the affected Data Subject(s).
- 6.3 The Supplier shall not, unless required by applicable law, make any notifications to a Regulator or any Data Subject about the Security Breach without SGN's prior written consent (not to be unreasonably withheld).

7 RETURN OR DESTRUCTION OF SGN PERSONAL DATA

- 7.1 Subject to Clause 7.2, the Supplier shall, and shall ensure that all Sub-Processors shall:
 - 7.1.1 return or irretrievably delete (at SGN's sole option) all SGN Personal Data; and
 - 7.1.2 cease all processing of SGN Personal Data; and
 - 7.1.3 delete all copies of SGN Personal Data from any system under their control; and
 - 7.1.4 destroy all copies of any document containing SGN Personal Data, immediately upon the expiry of the Agreement, and provide written confirmation to SGN of the same.
- 7.2 To the extent that the Supplier is prevented by law from destroying all or part of the SGN Personal Data (the "Legally Retained Data"), the Supplier shall not be required to comply with Clause 7.1 in respect of the Legally Retained Data, in which case the Supplier undertakes that it shall:
 - 7.2.1 notify SGN of such restriction and of the SGN Personal Data that constitutes the Legally Retained Data; and
 - 7.2.2 cease all processing of the Legally Retained Data other than as required by the applicable law; and
 - 7.2.3 keep confidential all such Legally Retained Data and not disclose the Legally Retained Data to any third party;
 - 7.2.4 continue to comply with the provision of these DP Terms in respect of such Legally Retained Data.

8 RECORDS

- 8.1 The Supplier will keep detailed, accurate and up-to-date written records regarding any processing of SGN Personal Data it carries out for SGN, including but not limited to, the access, control and security of the SGN Personal Data, approved Sub-Processors and affiliates, the processing purposes, categories of processing, any transfers of personal data outside the EEA and related safeguards, and a general description of the technical and organisational security measures referred to in Clause 5.1.1 ("Records").

9 AUDIT

- 9.1 The Supplier shall comply with all requests of SGN (and/or its auditors and internal or external representatives, subject to reasonable and appropriate confidentiality undertakings being given by SGN's auditors or representatives) to inspect and audit the Supplier's (and its Sub-Processors') processing activities, and Records, to enable SGN to audit and verify that the Supplier (and its Sub-Processors) is complying fully with its obligations under the Agreement and under Data Protection Legislation in relation to the processing of Personal Data.
- 9.2 The Supplier shall provide such information, co-operation and assistance in relation to any request made by SGN (or its auditors, or its or their representatives) under Clause 9.1 as SGN may reasonably require.

10 CO-OPERATION AND ASSISTANCE

- 10.1 The Supplier shall promptly co-operate with SGN, and promptly provide such information and assistance as SGN may reasonably require, to enable SGN:
- 10.1.1 to comply with SGN's obligations under the Data Protection Legislation (including articles 32 to 36 of the GDPR) in respect of SGN Personal Data; and
- 10.1.2 to deal with and respond to all investigations and requests for information relating to the SGN Personal Data from any Regulator.
- 10.2 If the Supplier receives any complaint, notice or communication from a Regulator or other third party (excluding a Data Subject, communications from whom shall be dealt with in accordance with Clause 3.1) which relates directly or indirectly to SGN Personal Data or to either party's compliance with the Data Protection Legislation, it shall as soon as reasonably practicable notify SGN.

11 TRANSFER OF PERSONAL DATA

- 11.1 The Supplier shall not process SGN Personal Data, or transfer SGN Personal Data, outside of the EEA without the express prior written consent of SGN.
- 11.2 The consent of SGN under Clause 11.1 shall be conditional upon the Supplier ensuring there is adequate protection for such SGN Personal Data in accordance with applicable Data Protection Legislation. Such adequate protection may include, where specified by SGN, the Supplier (or applicable third party): (a) taking such steps as may reasonably be required by SGN on an on-going basis; and/or (b) entering into the Standard Contractual Clauses with SGN and/or any member of SGN's Group as set out in Schedule 1.
- 11.3 If SGN authorises the Supplier to transfer SGN Personal Data outside the EEA pursuant to Clause 11.1 and either (a) the means by which adequate protection for the transfer is achieved ceases to be valid or (b) any Regulator requires transfers of Personal Data pursuant to such Standard Contractual Clauses to be suspended, then SGN may (at its discretion) require the Supplier to immediately cease data transfers, to return all SGN Personal Data previously transferred and delete and return all SGN Personal Data previously transferred.

12 TERM AND TERMINATION

- 12.1 These DP Terms will remain in full force and effect until the later of:
- 12.1.1 SGN and the Supplier continuing to do business with each other; or
- 12.1.2 the Supplier retaining any SGN Personal Data in its possession or control.

- 12.2 Any provision of these DP Terms that expressly or by implication should come into or continue in force on or after SGN and the Supplier finish doing business with each other in order to protect SGN Personal Data will remain in full force and effect.
- 12.3 The Supplier's failure to comply with these DP Terms is a material breach of any agreement between SGN and the Supplier. In such event, SGN may terminate its engagement of the Supplier effective immediately on written notice to the Supplier without further liability or obligation.
- 12.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its obligations, the parties will suspend the processing of SGN Personal Data until that processing complies with the new requirements. If the Parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 30 days, they may terminate their agreement on written notice to the other party.

13 WARRANTIES

- 13.1 The Supplier warrants and represents that:
 - 13.1.1 its employees, Sub-Processors, agents and any other person or persons accessing SGN Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation relating to the Personal Data;
 - 13.1.2 it and anyone operating on its behalf will process the SGN Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;
 - 13.1.3 it has no reason to believe that the Data Protection Legislation prevents it from providing any of the service and/or products being provided by the Supplier to SGN; and
 - 13.1.4 considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of SGN Personal Data and the accidental loss or destruction of, or damage to, SGN Personal Data, and ensure a level of security appropriate to:
 - 13.1.4.1 the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
 - 13.1.4.2 the nature of the SGN Personal Data protected; and
 - 13.1.4.3 comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 5.1.1
- 13.2 SGN warrants and represents that the Supplier's expected use of the SGN Personal Data as specifically instructed by SGN will comply with the Data Protection Legislation.

14 INDEMNITY

- 14.1 The Supplier will indemnify and keep indemnified at its own expense SGN against all claims, liabilities, damages, administrative fine, losses or costs incurred by SGN or its affiliates or for which SGN or its affiliates may become liable caused by any act or omission of the Supplier or any of its agents, personnel or Sub-Processors in breach of these DP Terms or the Data Protection Legislation.
- 14.2 Save to the extent prohibited under the GDPR or applicable laws, the provisions of Clause 14.1 shall apply in substitution for any allocation of liability which may arise under Article 82 of the GDPR.

15 NOTICE

- 15.1 Any notice or other communication given to a party under or in connection with these DP Terms shall be in writing and shall be:
- 15.1.1 delivered by hand or by pre-paid first class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or
 - 15.1.2 sent by fax to its main fax number;
- 15.2 Any notice or communication shall be deemed to have been received:
- 15.2.1 if delivered by hand, on signature of a delivery receipt;
 - 15.2.2 if sent by pre-paid first post or other next working day delivery services, at 9:00 am on the second Business Day after posting;
 - 15.2.3 if sent by fax, at 9:00 on the next Business Day after transmission
- 15.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.
- 15.4 A notice given under these DP Terms is not valid if sent by email.

16 GOVERNING LAW

- 16.1 These DP Terms and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

17 JURISDICTION

- 17.1 Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with these DP Terms or its subject matter or formation.

SCHEDULE 1 STANDARD CONTRACTUAL CLAUSES

Standard contractual clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

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.

1 Definitions

For the purposes of the clauses:

- a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- b. 'the data exporter' means the controller who transfers the personal data;
- c. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d. 'the 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.

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.

3 Third-party beneficiary clause

- 3.1 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 6.2, clause 7, clause 8.2, and clauses 9 to 12 as third-party beneficiary.
- 3.2 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.
- 3.3 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 subprocessor shall be limited to its own processing operations under the clauses.
- 3.4 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.

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 subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the clauses; and
- j. that it will ensure compliance with clause 4(a) to (i).

5 Obligations of the data importer

The data importer agrees and warrants:

- a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- d. that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

- e. (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. (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. (g) to make available to the data subject upon request a copy of the clauses, or any existing contract for subprocessing, unless the clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h. (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- i. (i) that the processing services by the sub-processor will be carried out in accordance with clause 11;
- j. (j) to send promptly a copy of any sub-processor agreement it concludes under the clauses to the data exporter.

6 Liability

- 6.1 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.
- 6.2 If a data subject is not able to bring a claim for compensation in accordance with clause 6.1 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 or by operation of law, in which case the data subject can enforce its rights against such entity.

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

- 6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in clauses 6.1 and 6.2, 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.

7 Mediation and jurisdiction

- 7.1 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.
- 7.2 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.

8 Cooperation with supervisory authorities

- 8.1 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.
- 8.2 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.
- 8.3 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 clause 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

9 Governing law

The clauses shall be governed by the law of the Member State in which the data exporter is established, namely

.....

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.

11. Sub-processing

- 11.1 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. 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.
- 11.2 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 clause 6.2 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.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in clause

11.1 shall be governed by the law of the Member State in which the data exporter is established, namely

.....
11.4 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.

12 Obligation after the termination of personal data-processing services

12.1 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.

12.2 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 clause 12.1.

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)

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 the standard contractual clauses:

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: the data exporter promptly notifying the data importer of a claim; and the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.