|  |
| --- |
| **PERSONAL DATA PROCESSING AGREEMENT** |

This agreement is dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PARTIES

1. **FLOGAS BRITAIN LIMITED**, a company incorporated in England, with company number 00993638 and having its registered office at 81 Rayns Way, Syston, Leicester, Leicestershire, LE7 1PF (Flogas)
2. **[INSERT]** incorporated and registered in England with company number **[INSERT]**  whose registered office is at **[INSERT]**. (Provider)

BACKGROUND

1. Flogas and the Provider entered into an agreements for services or any other relevant agreements (Master Agreement) that may require the Provider to process Personal Data on behalf of Flogas.
2. This Personal Data Processing Agreement (Agreement) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing services under the Master Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this Agreement.

* 1. Definitions:
1. AuthorisedPersons: the persons or categories of persons that Flogas authorises to give the Provider personal data processing instructions.
2. Business Purposes: the services described in the Master Agreement or any other purpose specifically identified in ANNEX A.
3. Data Subject: an individual who is the subject of Personal Data.
4. Personal Data: means any information relating to an identified or identifiable natural person that is processed by the Provider as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
5. Processing, processes and process: either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.
6. Data Protection Legislation: the UK Data Protection Legislation and any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the relevant data protection or supervisory authority and applicable to a party.
7. UK Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.
8. Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
9. Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, a completed copy of which comprises ANNEX B.
	1. This Agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Agreement.
	2. The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.
	3. A reference to writing or written includes faxes and email.
	4. In the case of conflict or ambiguity between:
		1. any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;
		2. the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail;
		3. any of the provisions of this Agreement and the provisions of the Master Agreement, the provisions of this Agreement will prevail; and
		4. any of the provisions of this Agreement and any executed SCC, the provisions of the executed SCC will prevail.
10. Personal data types and processing purposes
	1. Flogas and the Provider acknowledge that for the purpose of the Data Protection Legislation, Flogas is the controller and the Provider is the processor.
	2. Flogas retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

* 1. ANNEX A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Provider may process to fulfil the Business Purposes of the Master Agreement.

1. Provider's obligations
	1. The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with Flogas's written instructions. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify Flogas if, in its opinion, Flogas's instruction would not comply with the Data Protection Legislation.
	2. The Provider must promptly comply with any Flogas request or instruction requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
	3. The Provider will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless Flogas or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Provider to process or disclose Personal Data, the Provider must first inform Flogas of the legal or regulatory requirement and give Flogas an opportunity to object or challenge the requirement, unless the law prohibits such notice.
	4. The Provider will reasonably assist Flogas with meeting Flogas's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.
	5. The Provider must promptly notify Flogas of any changes to Data Protection Legislation that may adversely affect the Provider's performance of the Master Agreement.
	6. The Provider will only collect Personal Data for Flogas using a notice or method that Flogas specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of Flogas's identity and its appointed data protection representative, the purpose or purposes for which their Personal Data will be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing. The Provider will not modify or alter the notice in any way without Flogas's prior written consent.

1. Provider's employees
	1. The Provider will ensure that all employees:
		1. are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;
		2. have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and
		3. are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.
	2. The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable law on all of the Provider's employees with access to the Personal Data.
2. Security
	1. The Provider must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in ANNEX C. The Provider must document those measures in writing and periodically review them to ensure they remain current and complete, at least annually.
	2. The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:
		1. the pseudonymisation and encryption of personal data;
		2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
		3. 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
		4. a process for regularly testing, assessing and evaluating the effectiveness of security measures.
3. Personal Data Breach
	1. The Provider will promptly and without undue delay notify Flogas if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Provider will restore such Personal Data at its own expense.
	2. The Provider will immediately and without undue delay notify Flogas if it becomes aware of:
		1. any accidental, unauthorised or unlawful processing of the Personal Data; or
		2. any Personal Data Breach.
	3. Where the Provider becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide Flogas with the following information:
		1. description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;
		2. the likely consequences; and
		3. description of the measures taken, or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.
	4. Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Provider will reasonably co-operate with Flogas in Flogas's handling of the matter, including:
		1. assisting with any investigation;
		2. providing Flogas with physical access to any facilities and operations affected;
		3. facilitating interviews with the Provider's employees, former employees and others involved in the matter;
		4. making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by Flogas; and
		5. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.
	5. The Provider will not inform any third party of any Personal Data Breach without first obtaining Flogas's prior written consent, except when required to do so by law.
	6. The Provider agrees that Flogas has the sole right to determine:
		1. whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in Flogas's discretion, including the contents and delivery method of the notice; and
		2. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.
	7. The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.2 and clause 6.4 unless the matter arose from Flogas's specific instructions, negligence, wilful default or breach of this Agreement, in which case Flogas will cover all reasonable expenses.
	8. The Provider will also reimburse Flogas for actual reasonable expenses that Flogas incurs when responding to a Personal Data Breach to the extent that the Provider caused such a Personal Data Breach, including all costs of notice and any remedy as set out in clause 6.6.

1. Cross-border transfers of personal data
	1. The Provider (or any subcontractor) must not transfer or otherwise process Personal Data outside the European Economic Area (EEA) without obtaining Flogas's prior written consent.
	2. Where such consent is granted, the Provider may only process, or permit the processing, of Personal Data outside the EEA under the following conditions:
		1. the Provider is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. The Provider must identify in ANNEX A the territory that is subject to such an adequacy finding; or
		2. the Provider participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Provider (and, where appropriate, Flogas) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation ((EU) 2016/679). The Provider must identify in ANNEX A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Provider must immediately inform Flogas of any change to that status; or
		3. the transfer otherwise complies with the Data Protection Legislation for the reasons set out in ANNEX A.
	3. If any Personal Data transfer between Flogas and the Provider requires execution of SCC in order to comply with the Data Protection Legislation (where Flogas is the entity exporting Personal Data to the Provider outside the EEA), the parties will complete all relevant details in, and execute, the SCC contained in ANNEX B, and take all other actions required to legitimise the transfer.
2. Subcontractors
	1. The Provider may only authorise a third party (subcontractor) to process the Personal Data if:
		1. Flogas provides prior written consent prior to the appointment of each subcontractor;
		2. the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon Flogas's written request, provides Flogas with copies of such contracts;
		3. the Provider maintains control over all Personal Data it entrusts to the subcontractor; and
		4. the subcontractor's contract terminates automatically on termination of this Agreement for any reason.
	2. Those subcontractors approved as at the commencement of this Agreement are as set out in ANNEX A. The Provider must list all approved subcontractors in Annex A and include any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.
	3. Where the subcontractor fails to fulfil its obligations under such written agreement, the Provider remains fully liable to Flogas for the subcontractor's performance of its agreement obligations.
	4. The Parties consider the Provider to control any Personal Data controlled by or in the possession of its subcontractors.
	5. On Flogas's written request, the Provider will audit a subcontractor's compliance with its obligations regarding Flogas's Personal Data and provide Flogas with the audit results.

1. Complaints, data subject requests and third party rights
	1. The Provider must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to Flogas as Flogas may reasonably require, to enable Flogas to comply with:
		1. the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
		2. information or assessment notices served on Flogas by any supervisory authority under the Data Protection Legislation.
	2. The Provider must notify Flogas immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.
	3. The Provider must notify Flogas within 2 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.
	4. The Provider will give Flogas its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.
	5. The Provider must not disclose the Personal Data to any Data Subject or to a third party other than at Flogas's request or instruction, as provided for in this Agreement or as required by law.
2. Term and termination
	1. This Agreement will remain in full force and effect so long as:
		1. the Master Agreement remains in effect; or
		2. the Provider retains any Personal Data related to the Master Agreement in its possession or control (Term).
	2. Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Data will remain in full force and effect.
	3. The Provider's failure to comply with the terms of this Agreement is a material breach of the Master Agreement. In such event, Flogas may either terminate the Master Agreement or terminate any part of the Master Agreement authorising the processing of Personal Data effective immediately on written notice to the Provider without further liability or obligation.
	4. If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of 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 the Master Agreement on written notice to the other party.
3. Data return and destruction
	1. At Flogas's request, the Provider will give Flogas a copy of or access to all or part of Flogas's Personal Data in its possession or control in the format and on the media reasonably specified by Flogas.
	2. On termination of the Master Agreement for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by Flogas, return and not retain, all or any Personal Data related to this Agreement in its possession or control.
	3. If any law, regulation, or government or regulatory body requires the Provider to retain any documents or materials that the Provider would otherwise be required to return or destroy, it will notify Flogas in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.
	4. The Provider will certify in writing that it has destroyed the Personal Data within 7 days after it completes the destruction.
4. Records
	1. The Provider will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for Flogas, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5.1 (Records).
	2. The Provider will ensure that the Records are sufficient to enable Flogas to verify the Provider's compliance with its obligations under this Agreement and the Provider will provide Flogas with copies of the Records upon request.
	3. Flogas and the Provider must review the information listed in the Annexes to this Agreement once a year to confirm its current accuracy and update it when required to reflect current practices.

1. Audit
	1. The Provider will permit Flogas and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least 7 days' notice, during the Term. The Provider will give Flogas and its third-party representatives all necessary assistance to conduct such audits. The assistance may include, but is not limited to:
		1. physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing Personal Data;
		2. access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and
		3. inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.
	2. The notice requirements in clause 13.1 will not apply if Flogas reasonably believes that a Personal Data Breach occurred or is occurring, or the Provider is in breach of any of its obligations under this Agreement or any Data Protection Legislation.
	3. If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, the Provider will:
		1. promptly, conduct its own audit to determine the cause;
		2. produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;
		3. provide Flogas with a copy of the written audit report; and
		4. remedy any deficiencies identified by the audit within 30 days.
	4. At least once a year, the Provider will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.
	5. On Flogas's written request, the Provider will make all of the relevant audit reports available to Flogas for review, including as applicable: The Provider's latest Payment Card Industry (PCI) Compliance Report. Flogas will treat such audit reports as the Provider's confidential information under this Agreement.
	6. The Provider will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Provider's management.
2. Warranties
	1. The Provider warrants and represents that:
		1. its employees, subcontractors, agents and any other person or persons accessing 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;
		2. it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;
		3. it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and
		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 Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:
			1. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
			2. the nature of the Personal Data protected; and
			3. comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.
	2. Flogas warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by Flogas will comply with the Data Protection Legislation.
3. Indemnification
	1. The Provider agrees to indemnify, keep indemnified and defend at its own expense Flogas against all costs, claims, damages or expenses incurred by Flogas or for which Flogas may become liable due to any failure by the Provider or its employees, subcontractors or agents to comply with any of its obligations under this Agreement or the Data Protection Legislation.
	2. Any limitation of liability set forth in the Master Agreement will not apply to this Agreement's indemnity or reimbursement obligations.

1. Notice
	1. Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For Flogas: Legal and Compliance Counsel, Flogas Britain, 81 Rayns Way, Watermead Business Park, Syston, Leicestershire LE7 1PF

For the Provider: [INSERT]

* 1. clause 16.1 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.
	2. A notice given under this agreement is not valid if sent by email.

This agreement has been entered into on the date stated at the beginning of it.

|  |  |  |
| --- | --- | --- |
| Signed by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |
| for and on behalf of **FLOGAS BRITAIN LIMITED** |  | Director |
| Signed by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |
| for and on behalf of **[INSERT]** |  | Director |

1. Personal Data Processing Purposes and Details

**Subject matter of processing**:

The subject matter of the Processing is set out in the Master Agreement which is the provision of [DESCRIBE GOODS AND/OR SERVICES].

**Duration of Processing:**

For the duration necessary for:

* Complying with applicable laws and regulations;
* Any other purposes stipulated in the Master Agreement

**Nature of Processing**:

[DESCRIBE NATURE OF PROCESSING]

Any other Processing as stipulated in the Master Agreement

**Business Purposes**:

[DESCRIBE BUSINESS PURPOSE]

Any other business purposes set out in the Mater Agreement.

**Personal Data Categories**:

[LIST DATA FIELDS]

**Data Subject Types**:

[LIST DATA FIELDS]

**Approved Subcontractors:**

* [PLEASE LIST THE NAMES OF ALL SUBCONTRACTORS THAT YOU WILL USE]
1. 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 organization |  |
| (the **data exporter**) |  |

|  |  |
| --- | --- |
| Name of the data importing organisation: |  |
| address: |  |
| tel: |  |
| fax: |  |
| e-mail: |  |
| Other information needed to identify the organisation |  |
| (the **data importer**) |  |

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 Annex A.

1. **DEFINITIONS**

For the purposes of the Clauses:

* + 1. **personal data, special categories of data, process/processing, controller, processor, data subject and supervisory autho**rity 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);
		2. the **data exporter** means the controller who transfers the personal data;
		3. the **data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its 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;
		4. 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 its instructions, the terms of the Clauses and the terms of the written subcontract;
		5. 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;
		6. **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.
1. **DETAILS OF THE TRANSFER**

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

1. **THIRD-PARTY BENEFICIARY CLAUSE**

The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.

The data subject can enforce against the data importer this clause, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 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.

* 1. The data subject can enforce against the sub-processor this clause 3.1, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 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.

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.

1. **OBLIGATIONS OF THE DATA EXPORTER**

The data exporter agrees and warrants:

* + 1. 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;
		2. 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;
		3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex B to this contract;
		4. 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;
		5. that it will ensure compliance with the security measures;
		6. 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;
		7. 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;
		8. to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex B 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;
		9. 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 subjects as the data importer under the Clauses; and
		10. that it will ensure compliance with clause 4(a) to clause 4(i).
1. **OBLIGATIONS OF THE DATA IMPORTER**

The data importer agrees and warrants:

* + 1. 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;
		2. 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;
		3. that it has implemented the technical and organisational security measures specified in Annex B before processing the personal data transferred;
		4. that it will promptly notify the data exporter about:
			1. 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;
			2. any accidental or unauthorised access; and
			3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
		5. 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;
		6. 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;
		7. 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 Annex B 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;
		8. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
		9. that the processing services by the sub-processor will be carried out in accordance with clause 11; and
		10. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.
1. **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 its 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.

* 1. 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.
1. **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:
		1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
		2. 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.
2. **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).
3. **GOVERNING LAW**

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

1. **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 Clauses.

1. **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. 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 ...........................................
	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.
2. **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) |  |

**ANNEX A**

**[TO THE STANDARD CONTRACTUAL CLAUSES]**

This Annex 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 Annex A.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer) : ………………………………………………

**Data importer**

The data importer is (please specify briefly your 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** |  | **DATA IMPORTER** |  |
| Name: |  | Name: |  |
|  |  |  |  |
| Authorised signature: |  | Authorised signature: |  |
|  |  |  |  |

**ANNEX B**

**[TO THE STANDARD CONTRACTUAL CLAUSES]**

This Annex B 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 clause 4(d) and clause 5(c) (or documents/ legislation attached):

1. Security measures

[PLEASE AMEND TO REFLECT THE SECURITY MEASURES YOU WILL IMPLEMENT]

The Parties will, as a minimum, implement the following types of security measures:

**Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

* Establishing security areas, restriction of access paths;
* Establishing access authorizations for employees and third parties;
* Access control system (ID reader, magnetic card, chip card);
* Key management, card-keys procedures;
* Door locking (electric door openers etc.);
* Security staff, janitors;
* Surveillance facilities, video/CCTV monitor, alarm system;
* Securing decentralized data processing equipment and personal computers.

**Virtual access control**

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

* User identification and authentication procedures;
* ID/password security procedures (special characters, minimum length, change of password);
* Automatic blocking (e.g. password or timeout);
* Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
* Creation of one master record per user, user master data procedures, per data processing environment.

**Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

* Internal policies and procedures;
* Control authorization schemes;
* Differentiated access rights (profiles, roles, transactions and objects);
* Monitoring and logging of accesses;
* Disciplinary action against employees who access Personal Data without authorization;
* Reports of access;
* Access procedure;
* Change procedure;
* Deletion procedure.

**Disclosure control**

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

* Tunneling;
* Logging;
* Transport security.

**Entry control**

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

* Logging and reporting systems;
* Audit trails and documentation.

**Control of instructions**

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

* Unambiguous wording of the contract;
* Formal commissioning (request form);
* Criteria for selecting the Processor.

**Availability control**

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

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

**Separation control**

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

* Separation of databases;
* "Internal client" concept / limitation of use;
* Segregation of functions (production/testing);
* Procedures for storage, amendment, deletion, transmission of data for different purposes.