

DATA PROCESSING SCHEDULE – WEBSITE VERSION

This Data Processing Schedule ("**Schedule**") forms part of every agreement for shredding services ("**Agreement**") between Shred-it Limited ("**Processor**") and Shred-it's customer ("**Controller**") (each a "**Party**", together the "**Parties**"), except to the extent (if any) that the Parties have agreed in writing that different terms shall govern the processing of data by Processor on behalf of Controller and will take precedence over the terms of this Schedule.

BACKGROUND

- (1) The Processor agreed to provide the Controller with services for shredding confidential materials as further specified in the Agreement and Annex 1 to this Schedule (the "**Services**");
- (2) In providing the Services, the Processor may from time to time be provided with, or have access to, information of the Controller which may qualify as personal data within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") and other applicable data protection laws and provisions; and
- (3) The Controller engages the Processor for the processing of personal data acting on behalf of the Controller, as stipulated in Article 28 of the GDPR.

In order to enable the Parties to carry out their relationship in a manner that is compliant with law, the Parties have entered into this Schedule as follows:

1. Terminology

For the purposes of this Schedule, the terminology and definitions as used by the GDPR shall apply. In addition to that:

"Applicable data protection laws"	shall mean European Union or Member State laws with respect to any personal data in respect of which the Parties are subject to including GDPR and/or all applicable laws, rules, regulations, regulatory requirements from time to time, in each case in each jurisdiction where the Services are delivered.
"Member State"	shall mean a country belonging to the European Union or to the European Economic Area.
"Subprocessor"	shall mean any further processor that is engaged by the Processor as a sub-contractor for the performance of the Services.

2. Responsibilities of the Controller

On the date of this Schedule and during the term of the Agreement:

- (a) The Controller confirms that, in respect of the processing to be carried out under this Schedule, the technical and organisational measures of the Processor, as set out in Annex 2, are appropriate and sufficient to protect the rights of the data subject. The Processor will not be required to change any of those measures unless required to do so by law.
- (b) The Controller is responsible for ensuring that the processing activities relating to the personal data, as specified in the Agreement and Annex 1 to this Schedule, are in accordance with Applicable data protection laws and are lawful, fair and transparent in relation to the data subjects. In particular, the Controller shall take all steps necessary, including without limitation, providing appropriate fair processing notices to data subjects and ensuring that there is a lawful basis for the Processor to process the personal data as part of the Services.
- (c) The Controller warrants on the date of this Schedule and during the Agreement that all personal data processed by the Processor on behalf of the Controller has been and shall be processed (including its disclosure to Processor) by the Controller in accordance with GDPR and other Applicable data protection laws.

3. Instructions

- (a) The Processor shall process the personal data only on behalf of the Controller and in accordance with the documented instructions given by the Controller, unless otherwise required by European Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
- (b) The Controller's instructions are provided in this Schedule and the Agreement. Any further instructions that go beyond the instructions contained in this Schedule or the Agreement shall not be effective unless recorded in a signed variation to this Schedule or the Agreement.
- (c) The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes Applicable data protection provisions. In such case, the Processor is not obliged to follow the instruction until and until the Controller has confirmed or changed it in such a way that it is no longer considered to be an infringement.

4. Obligations of the Processor

- (a) The Processor shall ensure that persons authorised by the Processor to process the personal data on behalf of the Controller, in particular the Processor's employees as well as employees of any Subprocessors, are subject to a binding obligation of confidentiality and that such persons process any personal data to which they have access in compliance with the Controller's instructions.
- (b) The Processor shall implement the technical and organisational measures as specified in Annex 2 before processing the personal data on behalf of the Controller. The Processor may amend the technical and organisational measures from time to time provided that the amended technical and organisational measures are not less protective than those set out in Annex 2.
- (c) The Processor shall make available to the Controller any information necessary to demonstrate compliance with the obligations of the Processor relating to information security as required by Applicable data protection law and by this Schedule to the extent applicable to the Services. The Processor is in particular obliged to allow for and contribute to audits (e.g., providing audit reports and/or other relevant information or certificates to Controller upon Controller's request) or on-site inspections, conducted by the Controller or another auditor mandated by the Controller in relation to the processing of the personal data. The Processor's contribution to such audits shall be proportionate to the nature and purpose of the processing and subject to receipt by the Processor of reasonable notice.
- (d) The Processor shall notify the Controller (using the contact details provided by the Controller) without undue delay of becoming aware of a Personal Data Breach and the Processor will assist the Controller with the Controller's obligation under Applicable data protection laws to inform the data subjects and the supervisory authorities, as applicable, by providing the necessary information taking into account the nature of the processing and the information available to the Processor. For the avoidance of doubt, these obligations shall not be construed as an acknowledgement by the Processor of any liability for a Personal Data Breach or failure to prevent it.
- (e) The Processor shall provide reasonable assistance (taking account of the nature of the processing and the information available to the Processor) to the Controller with its obligation under Applicable data protection laws, to carry out:
 - a. a data protection impact assessment; and
 - b. prior consultation with the supervisory authoritiesthat relates to the Services provided by the Processor to the Controller under this Schedule by providing the necessary and available information to the Controller on request to allow it to meet its obligations under the GDPR.
- (f) The Processor shall, at the option of the Controller, delete or return to the Controller all personal data which are processed by the Processor on behalf of the Controller under this Schedule after the end of the provision of the Services, and delete any existing copies unless European Union or Member State law requires the Processor to retain such personal data. For the avoidance of doubt, this obligation shall not be infringed by the shredding of material containing personal data which was provided to the Processor by the Controller for destruction in the normal course of the Services.
- (g) The Processor shall provide to the Controller the records of processing activities relating to the Services under this Schedule, to the extent necessary for the Controller to comply with its obligation to maintain records of processing activities.
- (h) The Processor shall designate a data protection officer and/or a representative, to the extent required by Applicable data protection law. The Processor shall provide contact details of the data protection officer and/or representative, if any, to the Controller.

5. Data subject rights

- (a) Taking into account the nature of the processing, the Processor shall provide reasonable assistance to the Controller, including through appropriate technical and organisational measures, with the fulfilment of the Controller's obligation to comply with the rights of the data subjects and respond to data subjects' requests relating to their rights of (i) access, (ii) rectification, (iii) erasure, (iv) restriction of processing, (v) data portability, and (vi) objection to the processing.
- (b) The Controller shall determine whether or not a data subject has a right to exercise any such data subject rights and to give instructions to the Processor to what extent the assistance is required.

6. Subprocessing

The Processor shall not engage any Subprocessor without prior specific authorisation of the Controller.

7. Term and termination

The term of this Schedule is identical to the term of the Agreement (inclusive of any renewals or extensions). Save as otherwise specified herein, termination rights and requirements shall be the same as those set out in the Agreement.

8. Liability and indemnification

- (a) Each Party's liability for government/authority fines and penalties and any other loss or expense whatsoever (whether direct or indirect) incurred by the other Party for failure to comply with the requirements of any laws or regulations that affect the other

Party, to the extent such failure was caused by the Party's breach of the terms of this Schedule, shall be subject to and limited by the limitations of liability contained in the Agreement.

- (b) The limitation of liability set out in clause 8 (a) above shall not apply in case of a Party's liability for intentional or wilful default and any mandatory statutory liability imposed on that Party.
- (c) Subject to clause 8 (a) and clause 8 (b) above, each Party shall indemnify and hold the other Party harmless from and against all losses due to claims from third parties including government/authority fines and penalties resulting from, arising out of or relating to any material breach of this Schedule by the indemnifying Party.

9. Miscellaneous

- (a) Each Party shall comply with its obligations under the GDPR and under any other Applicable data protection laws.
- (b) This Schedule shall be governed by the same law as the Agreement except as otherwise stipulated by Applicable data protection laws. The place of jurisdiction for all disputes regarding this Schedule shall be as determined by the Agreement except as otherwise stipulated by Applicable data protection laws.
- (c) In the event of conflict between the provisions of this Schedule and any other agreements between the Parties, the provisions of this Schedule shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this Schedule shall prevail.
- (d) Should any provision of this Schedule be invalid or unenforceable, then the remainder of this Schedule shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this Schedule contains any omission.
- (e) Each Party has the right to request changes to this Schedule to the extent required to satisfy any interpretations, guidance or orders issued by competent European Union or Member State authorities, national implementation provisions, or other legal developments concerning the GDPR requirements for the commissioning of data processors under the national laws applicable to the Controller. The Party receiving such a request shall not unreasonably delay or withhold its agreement.

Annex 1 to the Schedule – Description of the processing activities

1. Categories of data subjects

The personal data processed concern the following categories of data subjects:

- Customers of the Controller;
- Employees of the Controller;
- Other data subjects, whose personal data are contained in materials which the Controller places in Shred-it consoles for collection and destruction.

For the avoidance of doubt, the Processor does not review any materials collected and is not aware of the nature or extent of any personal data printed or stored on such materials.

2. Subject-matter of the processing

The subject-matter of the processing is material selected by the Controller and provided to the Processor for shredding, as described in the Agreement. The subject-matter of the materials, and the extent (if any) to which they contain personal data, depends on the nature of the business of the Controller.

3. Nature and purpose of the processing

The nature and purpose of the processing is destruction by shredding as described in the Agreement. If the Agreement indicates that the Services are “off-site”, the Processor will additionally be securely transporting the Controller’s materials to the Processor’s secure facility prior to undertaking the shredding.

For the avoidance of doubt, once materials have been shredded, any data contained in them is irretrievably destroyed.

4. Type of personal data and special categories of data

The personal data processed by the Processor on behalf of the Controller concerns all categories of data subject, as determined by the Controller and provided in files, materials and other data carriers related to the business of the Controller.

For the avoidance of doubt, the Processor does not review any materials collected and is not aware of the nature or extent of any personal data printed or stored on such materials.

Annex 2 to the Schedule – Description of the technical and organisational measures implemented by Processor in accordance with Applicable data protection laws:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement technical and organisational measures to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. In assessing the appropriate level of security the Controller and the Processor took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The technical and organisational measures applicable to the Services are set out in the document "Shred-it Security Information", a copy of which can be accessed at <https://www.shredit.co.uk/en-gb/about/data-protection>.