DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of every agreement for shredding services ("Services Agreement") between Waste Paper Solutions ("Processor") and Waste Paper Solutions' customer ("Controller") (each a "Party", together the "Parties").

BACKGROUND

This DPA reflects the Parties' agreement with regard to the Processing of Personal Data because:

(1) The Processor agreed to provide the Controller with services for shredding materials as further specified in the Services 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 Applicable Data Protection Laws; 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 General Data Protection Regulation ("GDPR") shall apply. In addition to that:

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"Applicable Data Protection Laws" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the Data Protection Act 2018 and other

data protection or privacy legislation in force from time to time in the United Kingdom. In this DPA, in circumstances where and solely to the extent that the UK GDPR applies, references to the GDPR and its provisions shall be construed as references to the UK GDPR and its corresponding provisions, and references to "EU or Member State laws" shall be construed as references to UK laws.

"Subprocessor" shall mean any further processor that is engaged by the Processor as a subcontractor for the performance of the Services.

---

2. Responsibilities of the Controller

On the date of this Schedule and during the term of the Services 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 Services 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 or providing all relevant notices to, and obtaining all relevant consents from, data subjects (as the case may be).

(c) The Controller warrants on the date of this Schedule and during the Services 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 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 Applicable Data Protection Laws 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 Services Agreement. Any further instructions that go beyond the instructions contained in this Schedule or the Services

Agreement shall not be effective unless recorded in a signed variation to this Schedule or the Services Agreement.

(c) The Processor shall inform the Controller if, in its opinion, an instruction infringes provisions of Applicable Data Protection Laws. In such case, the Processor is not obliged to follow the instruction until and unless 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 Laws 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 provide reasonable assistance to 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 authorities that 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 reasonable request to allow it to meet its obligations under the Applicable Data Protection Laws.

(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 Applicable Data Protection Laws require 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 designate a data protection officer and/or a representative, to the extent required by Applicable Data Protection Laws. The Processor shall provide contact details of the data protection officer and/or representative, if any, to the Controller.

(h) The Processor shall not process personal data outside of the country where the personal data was originally received from the Controller.

---

5. Data Subject Rights

(a) Taking into account the nature of the processing and subject to Applicable Data Protection Laws, 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

(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 reasonably 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 Services 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 Services 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 Services 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 Applicable Data Protection Laws.

(b) This Schedule shall be governed by the same law as the Services 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 Services 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 authorities, national implementation provisions, or other legal developments concerning the GDPR, and UK GDPR requirements for the commissioning of data processors under the national laws applicable to the Controller or to comply with Applicable Data Protection Laws. 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 Waste Paper Solutions 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 Services 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 Services Agreement. 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 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:

Technical and Organisational Measures for Waste Paper Solutions

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 Waste Paper Solutions shall implement the following technical and organisational measures to ensure a level of security appropriate to the risks. In assessing the appropriate level of security, Waste Paper Solutions considers the risks that are presented by processing from accidental or unlawful destruction loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.

This document describes technical and organisational security measures and controls implemented by Waste Paper Solutions to protect personal data and ensure the ongoing confidentiality, integrity, and availability of Waste Paper Solutions products and services.

Waste Paper Solutions specialises in providing a tailored destruction service that allows businesses to comply with legislation and ensures that customer, employee, and confidential business information are always kept secure. Waste Paper Solutions provides secure destruction of your confidential materials, including paper and various electronic storage media such as DVDs, CDs, tapes, and hard drives. Our stringent chain-of-custody protocols and trusted shredding services guarantee the safe disposal of your confidential material, available for both regular and one-off needs.

Waste Paper Solutions provides a secure off-site shredding and recycling service. Trained, uniformed operatives perform this service, arriving at a customer's location on a pre-agreed date in an unmarked vehicle and carrying photo identification

Our Secure Destruction Process

1. Secure Collection: Your staff places **confidential paper waste** into our secure, locked containers for safekeeping. Non-paper items like CDs, tapes, and hard drives should be kept separate. We can provide security shredding sacks for storage of these items until collection.

2. Scheduled Pickup: On your pre-agreed schedule, a Waste Paper Solutions collection vehicle arrives at your location to prevent your confidential waste from being stored longer than necessary, aligning with data protection regulations.

3. Chain of Custody Initiation: Our shredding operative identifies themselves to your designated contact, then empties each console. They replace the internal sack and secure the contents for disposal.

4. Service Confirmation: After emptying and re-locking each bin, our shredding operative obtains a signature from your contact. At this point, a waste transfer note, detailing the time, date, and volume of waste collected, is generated at our Head Office.

5. Secure Transport: All confidential material is loaded into our secure, locked collection vehicle. Once the route is complete, the vehicle returns to our 24-hour alarmed facility. Our operative then unloads the material into our CCTV-monitored shredding facility.

6. Shredding: All confidential waste is shredded using our industrial cross-cut shredder.

7. Certification: Finally, your waste transfer note and certificate of destruction are emailed to you. This completes the paper trail from collection to secure disposal.

All shredded paper is then baled at Waste Paper Solutions's secure facility, where it is recycled into household products like tissue and toilet rolls. Destroyed electronic media and other non-paper waste are properly disposed of by our partner vendors, who have responsible disposal and reclamation agreements in place, ensuring compliance with local requirements.

How we ensure confidentiality of our Waste Paper Solutions Services:

Waste Paper Solutions Secure Service – Shred Facilities

- All Waste Paper Solutions service facilities adopt measures in order to ensure that all confidential materials taken for off-site destruction and recycling are secure. When Waste Paper Solutions’s off-site service is utilized, confidential materials are kept in a highly secured facility containing an intruder alarm, which covers all shredding and storage areas, and is connected to an alarm receiving centre. All shredding facilities have CCTV recording equipment in place (for areas where legally permitted) to record all unloading, storage, and shredding areas, and retain footage for a designated period.
- All external doors are secured with high security locks and have restricted entry.

- Members of the public are not permitted to enter our shredding facilities. Key areas of Waste Paper Solutions's operations are restricted and cannot be viewed by visitors.

Waste Paper Solutions Vehicles

- All vehicles used for transfer or destruction of customer's confidential materials are fully lockable.
- All operatives carry out security checks on their vehicles before leaving the facility, this is to ensure the vehicle is in full operational order, fit for purpose, and meets Waste Paper Solutions's required quality and security standard.
- All Waste Paper Solutions vehicles follow maintenance schedules, and an annual service plan.
- All vehicles are GPS tracked (according to applicable laws), which provides an additional layer of security by allowing Waste Paper Solutions to know where the customer's confidential materials are at all points of the process.
- We operate both **unmarked and branded vehicles**. Our unmarked fleet, featuring onboard CCTV, is specifically used for secure facilities where discretion is paramount.

Waste Paper Solutions Secure Equipment

- Waste Paper Solutions provides lockable consoles and/or heavy-duty shredding sacks with individually numbered security tags for the secure storage and transportation of confidential waste.
- Waste Paper Solutions Consoles comprised of the following features:
    - Security Feed Slot - consoles have bevelled slots capable of accepting a relatively high quantity of documents at once while at the same time ensuring that papers cannot be retrieved once deposited.
    - Key Operated Lock - only an authorised individual (Waste Paper Solutions operative or customer's designated employee) with a key can access the contents of the consoles.

How we ensure integrity and availability of our services:

In addition to the above:

- Risk Assessments
    - We carry out periodic risk assessments of Waste Paper Solutions's equipment and processes to ensure the safe and secure delivery of goods and services. Among these are risk assessments on the use of all shredders, manual handling procedures, and the operation of Waste Paper Solutions vehicles.

- Certificate of Destruction
    - As part of our ongoing duty of care to our customers, Waste Paper Solutions will provide a Certificate of Destruction to the customer after each service has taken place. This confirms that Waste Paper Solutions has taken steps to maintain the integrity of its collection for destruction process and fulfilled its duty of care in disposing of the customer's confidential materials by applying the applicable laws and regulations.
    - The Certificate of Destruction is provided free of charge as part of the Waste Paper Solutions service. The content on the Certificate of Destruction will vary based on local regulatory and legal requirements and may display the following types of information:
        - The volume of waste collected.
        - The collection date.
        - Customer's name and collection address.
        - Waste Paper Solutions's attending vehicle registration number.
        - Waste Paper Solutions's facility that will service the customer (where off-site shredding is carried out).
        - Waste Paper Solutions's Waste Carriers License number.
- Staff Vetting
    - All Waste Paper Solutions employees are screened prior to employment, to ensure their eligibility to perform their job responsibilities.
    - Upon commencement of employment and on an ongoing basis, all employees are required to read, sign, and abide by Waste Paper Solutions's Confidentiality Agreement, ensuring all employees are aware of their obligations and duties.
- Waste Paper Solutions Training
    - Each job within Waste Paper Solutions has been assessed for specific training requirements to ensure that a high level of competency is achieved throughout the workforce. Where training is required, Waste Paper Solutions arranges and assesses competence of the individual prior to allowing them to conduct critical operations. Staff that carry out shredding services are trained with respect to appropriate data protection practices and handling of personal data.

©Waste Paper Solutions I October 2024

Waste Paper Solutions
Sunnybank House
High Street
Mayfield TN20 6AA

T: 01435 408118
E: hello@wastepapersolutions.co.uk

wastepapersolutions.co.uk