DATA PROCESSING SCHEDULE – WEBSITE VERSION for use in the UK only
LAST UPDATED: December 15, 2021

This Data Processing Schedule ("**Schedule**") forms part of every agreement for shredding services ("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
This Schedule 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 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 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 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 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 Law. 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, 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 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 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 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. If the Services 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:

Technical and Organizational Measures for Shred-it

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, Stericycle, Inc. ("Stericycle") shall implement the following technical and organizational measures to ensure a level of security appropriate to the risks. In assessing the appropriate level of security, Stericycle considers the risks that are presented by processing from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

This document describes technical and organizational security measures and controls implemented by Stericycle to protect personal data and ensure the ongoing confidentiality, integrity, and availability of Shred-it products and services.

Shred-it specializes 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. Through Shred-it's strict chain-of-custody processes, hand-held technology, and reliable on-time, on-site and off-site shredding service, and a global network of local service facilities, we deliver our secure destruction services for **customer confidential material (CCM)**. CCM includes paper, electronic storage media materials (e.g., DVDs, CDs, tapes, and hard drives), as well as other customers' products (e.g., uniforms, shoes, and license plates) on a regular and ad-hoc basis.

On-Site Shredding and Recycling Process

Shred-it provides a secure on-site shredding service that is performed by a security vetted **Customer Service Representative (CSR)** who will arrive at a customer location on a designated, pre-agreed scheduled date in a logo-marked shredding vehicle, wearing the Shred-it uniform, and displaying photo identification on the outer most layer of clothing.

STEP 1: CCM is placed into the secure locked containers by customer staff for safe keeping. Staff can put paper material containing paper clips and staples in the containers as these will be shredded by Shred-it's powerful cross-cut shredders. Non-paper CCM (CDs, tapes, hard drives, etc.) are collected and destroyed separately from paper.

STEP 2: Per the customer schedule, a Shred-It destruction truck arrives at a location on a pre-agreed schedule to ensure confidential information is not stored longer than necessary.

STEP 3: Shred-it's CSR will identify themselves to a designated customer contact. Containers' bar codes are scanned using a handheld device to ensure that all bins are accounted for during the collection process. The bins' contents are entirely removed from the locked consoles and placed directly in a secured collection tote. The CSR's handling of the customers' papers, materials, and/or products is only for the physical transfer from one secured container to another and does not involve any examination of individual pieces. The handheld device will direct the CSR to all containers at the customer's site without causing any disruptions to customer staff.

STEP 4: When the collection of items for destruction is complete, Shred-it's CSR will re-lock each collection bin and then obtain a signature from the designated customer contact using the handheld device. At this point, a Certificate of Destruction displaying the number and type of units serviced for destruction is emailed to the designated customer contact.

STEP 5: Shred-It's CSR will then return to the Shred-It destruction truck with the secured collection tote where the customer's collected items are loaded into the hopper of the shredder of the onsite truck and is destroyed into unrecognizable shredded material. The CSR will then depart the location after all of the customer's collected items have been destroyed.

STEP 6: At the end of the day, the unrecognizable shredded paper material is taken to Shred-it's secure CCTV-monitored service facility, where it is baled and transported to a paper mill to be recycled into household products such as tissues and toilet rolls. Destroyed electronic media and other non-paper CCM are properly disposed of in accordance with local requirements by partner vendors that have responsible disposal agreements to handle/reclaim.

Off-Site Shredding and Recycling Process
Shred-it provides a secure off-site shredding and recycling service. This service is performed by a security vetted CSR who will arrive at a customer location on a designated, pre-agreed scheduled date in a logo-marked collection vehicle, wearing the Shred-it uniform, and displaying photo identification on the outer most layer of clothing.

STEP 1: The process begins with CCM being placed into the secure locked container by the customer's staff for safe keeping before destruction. Staff can put material containing paper clips and staples in Shred-it's containers, as these will be shredded by the powerful shredders. Non-paper CCM (CDs, tapes, hard drives, etc.) are collected and destroyed separately from paper.

STEP 2: As per the customer's schedule, Shred-it's collection vehicle will arrive at the customer's location on a pre-agreed schedule to ensure CCM are not stored longer than necessary (in accordance with any data protection laws and regulations).

STEP 3: Shred-it's CSR will identify themselves to the customer's designated contact prior to emptying containers, ensuring the barcode of the unit is scanned using a handheld device to initiate the chain of custody for the collected information. The handheld device will direct Shred-it's CSR to all containers at the customers' site, causing no disruption to staff.

STEP 4: Shred-it's CSR will re-lock each collection bin and then obtain a signature from the customer's designated contact using the handheld device. At this point, a Certificate of Destruction displaying the number and type of units serviced for destruction is emailed to the contact.

STEP 5: All CCM will then be carried to Shred-it's secure collection vehicle. The storage area of the truck is unlocked, and the CSR will move the material into their vehicle and secure the load. Once this is done, the CSR ensures the truck is locked and no access can be gained. Upon completion of the route the vehicle is returned to the Shred-it 24-hour alarmed facility. Here, the CSR unloads the vehicle into the CCTV-monitored warehouse.

STEP 6: All CCM are then shredded using a facility-based shredder.

All the unrecognizable shredded paper material is then baled within Shred-it's warehouse and transported to their pre-approved paper mill, where the material is recycled into household products such as tissues and toilet rolls. Destroyed electronic media and other non-paper CCM are properly disposed of in accordance with local requirements by partner vendors that have responsible disposal agreements to handle/reclaim.

How we ensure confidentiality of our Shred-it Services:

Shred-it Secure Service – Shred Facilities
- All Shred-it service facilities adopt measures in order to ensure that all confidential materials taken for off-site destruction and recycling are secure. When Shred-it'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. All doors are controlled by key fob activation systems only allowing entry to authorized personnel. Shred-it documents to whom key fobs are handed out to ensure that such are only in the possession of authorized personnel and are retrieved where necessary.
- All visitors sign in and out and sign a confidentiality agreement stating they will abide by Shred-it procedures. All visitors then receive an orientation to ensure they are aware of emergency procedures and site rules and are escorted at all times. Key areas of Shred-it's operations are restricted and cannot be viewed by visitors.

Shred-it Vehicles
- All of Shred-it's on-site destruction vehicles carry on-board industrial proprietary multi–edge, cross-cut shredders, which shred the materials into fragments, which are then automatically mixed together in the rear of the vehicle by the shredder, ensuring all confidential material is illegible and impossible to recreate into its original form.
- All vehicles used for transfer or destruction of customer's confidential materials are fully lockable.
    - All of Shred-it's owned or leased collection trucks are outfitted with an enhanced security package which can include the following: alarms systems, slam locks or high-security padlocks.

    - These units are decaled with the Shred-it logo and are locked at all times when the CSR is not entering or exiting the vehicle.
    - Except in the case of an emergency, no unauthorized person is permitted access to the cab, body, box, payload, or tail-lift of any vehicle.
    - No unauthorized person shall be transported as a passenger at any time, except in case of an emergency.
- Each vehicle can carry a large quantity of shredded paper.
- All CSRs carry out security checks on their vehicles before leaving the facility and on their return daily; this is to ensure the vehicle is in full operational order, fit for purpose, and meets Shred-It's required quality and security standard.
- All Shred-it 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 Shred-it to know where the customer's confidential materials are at all points of the process.

Shred-it Secure Equipment

- Shred-it has a variety of different sized lockable containers which can be supplied to customers to store confidential materials prior to destruction.
- **Shred-it Consoles** - Standard-sized, desk, and mini consoles are comprised with 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 by a human hand once deposited.
    - Key Operated Deadbolt Lock - only an authorized individual (Shred-It CSR or customer's designated employee) with a key can access the contents of the consoles.
- **Shred-it Totes - are comprised with the following features:**
    - Capacities of 65 and 96 gallons
    - Manoeuvrability - 12" Non-marking rubber wheel
    - 3" Locking caster wheels
    - Security Feed Slot - Standard lid with front paper slot and lock
    - Lockability - Hasp locking system or internal lid locking mechanism
    - Servicing Containers - the consoles will have either an internal cardboard liner or a nylon security bag to contain papers deposited. The Shred-it CSR will securely transfer the material from the liner or bag into a locked wheeled container which is used to carry the material to the truck. For the convenience of the customer's staff, stickers are placed on all consoles clearly displaying what can and cannot be placed inside, along with a number to call Shred-it's Client Care Associates, should they require support.

How we ensure integrity and availability of our services:

In addition to the above:

- **Risk Assessments**
    - We carry out periodic risk assessments of Shred-it'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 Shred-it vehicles.

- **Certificate of Destruction**
    - As part our ongoing duty of care to our customers, Shred-it will provide a Certificate of Destruction as part of the Service Certificate to the customer after each service has taken place. This confirms that Shred-it 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 Shred-it 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 number of containers or equipment serviced.
        - The date and time of service.
        - Customer's contact name and signature.
        - Customer's address.
        - Shred-it's CSR's name and signature.
        - Shred-it's facility that will service the customer (where off-site processing occurs).
        - Shred-it's Waste Carriers License Number along with their Waste Exemption Reference Number; or the facility's NAID Certifications and Endorsements.

- **Staff Vetting**
  - All Shred-it 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 Shred-it's Confidentiality Agreement, ensuring all employees are aware of their obligations and duties.

- **Shred-it Training**
  - Each job within Shred-it has been assessed for specific training requirements to ensure that a high level of competency is achieved throughout the work force. Where training is required, Shred-it arranges and assesses competence of the individual prior to allowing them to conduct critical operations. Staff that carries out shredding services are trained with respect to appropriate data protection practices and handling of personal data.
  - All Shred-it CSRs sign documents to confirm they have received training in vehicle incidents, personal accident procedures, manual handling/safe lifting, and safe shredder operation with all elements of the health and safety operations being evaluated by a supervisor.
  - All driving staff hold the required licenses or certifications necessary to operate their assigned vehicle and have been trained in-house to drive in a safe manner.

- **Data Security Incidents**
  - There is an internal procedure for employees to follow regarding security incidents to ensure the timely reporting and handling of identified incidents.

How we regularly test / assess / evaluate the effectiveness of our technical and organisational measures for to help ensure the security of the processing:

In addition to the periodic risk assessments and ongoing training needs of staff as described above:

- **Compliance Review**
  - Shred-it regularly reviews whether technical and organisational measures as outlined above are adequately implemented and adhered to by its employees.

- **Shred-it Accreditations & Memberships**
  - We are always striving to improve our services, and to this end, we have the following accreditations and memberships to industry associations in order to keep up to date with current legislation and best practices:

North America and Australia:

  - **NAID AAA Certified:** NAID AAA Certification verifies Shred-it's qualifications of certified information destruction provider through a comprehensive scheduled and unannounced audit program. AAA certification means Shred-it meets numerous laws and regulations requiring the protection of confidential customer information.

United Kingdom:

  - **ISO 9001:2008 -** This quality management system certification enables Shred-it to demonstrate their commitment to service quality and customer satisfaction. Customers can be assured that Shred-it is continually improving their quality management systems and integrating the realities of a changing world.
  - **ISO 14001:2004 -** This environmental management system certification demonstrates Shred-it's commitment to the environment. The standard provides guidelines on how Shred-it can manage the environmental aspects of their business activities more effectively, whilst taking into consideration pollution prevention, environmental protection, and socio-economic needs.
  - **BS EN 15713 -** This Code of Practice outlines the key requirements of a professional information destruction company and the importance of security. Shred-it is assessed against these requirements as part of their ISO 9001 external audit and it is listed on their ISO 9001 certificate.
  - **British Security Industry Association (BSIA) -** Shred-it has been a principal member of the BSIA since 2005. This is the trade association for the professional security industry in the UK. BSIA members are responsible for more than 70% of UK security products and services (by turnover) including the manufacture, distribution, and installation of electronic and physical security equipment, and the provision of security guarding and consultancy

services. Being a member of this industry leading association ensures that Shred-it customers benefit from Shred-it being at the fore-front of new legislation.

- **SAFEContractor -** This is a health and safety accreditation scheme for contractors. It simplifies the process of demonstrating to Shred-it customers that Shred-it has health and safety policies and procedures in place. This scheme assesses Shred-it's health and safety arrangements and their customers recognize the scheme and accept their SAFEContractor certificate as confirmation of competency.
- **Fleet Operator Recognition Scheme (FORS) Bronze accreditation** - Confirms Shred-it employs good practices and complies with the requirements laid out by the FORS Standard. This includes dedication to driver and vehicle safety, combined with improving operating practices through effective monitoring of fuel and tire usage.
- **Waste Carriers License Number Reference:** CBDU51993 (England and Wales), WCR/R/1137691 (Scotland) and ROC UT 681 9 (Northern Ireland).

Germany:

- **DIN 66399** – Shred-it holds a DIN 66399 certification in Germany, which defines machine and process requirements for shredding paper and electronic media. This standard was developed by the Standards Committee for Information Technology and Applications (NIA) of the German Institute for Standardisation (DIN).