General Customers Service Level & Data Processor Agreement

THIS AGREEMENT (herein defined as the "Agreement") is dated **as per the date the invoice for services was signed** and entered into between:

1. **"Customer"** hereinafter the may be called **"Data Controller"**
   -and-
2. **M1 Document Solutions Ltd having** its registered office at Dublin Road, Castleblayney, Co. Monaghan, A75 NP30
   (hereinafter the **"Company" and/or the "Data Processor")**

HEREINAFTER referred to as "the parties".

DEFINITIONS:
For the purposes of this Agreement:
"Working Day" means Monday to Friday excluding public holidays.
"Contract Year" being each entire year as from the anniversary date of this Agreement
"**Applicable Data Protection law"** means any EU and Irish law which may apply to the terms of this Agreement and which may vary from time to time;
"Data Controller" and "Data Processor" shall have the meanings as set out in Article 4(7) and (8) respectively of EU General Data Protection Regulation 2016/679 (the "GDPR");
"Data Protection Commissioner" (DPC or other supervisiory authority where appropriate) is the supervisory authority for the purposes of Article 51 of the GDPR;
"Data Subject" means an individual who is the subject of Personal Data;
"Personal Data" shall have the meaning set out in Article 4(1) of the GDPR;
"Prompt Notice" shall mean 24 hours unless otherwise expressly stated in this agreement;
"Special Category Data" shall have the meaning set out in Article 9(1) of the GDPR;
"Third Country" shall mean a location outside of the European Economic Area (EEA), the EEA being: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

The details of the data processing (as well as the Personal Data covered) are specified in Schedule 1 hereto.

WHEREAS:
Certain Personal Data concerning Data Subjects (both as defined above) may be transferred from the Data Controller to the Data Processor. Under the GDPR, a written Data Processor Agreement must be in place between the Data Controller and any organisation which processes personal data on its behalf, governing the processing of the data. **Section C** of this agreement is intended to govern such transfers and to satisfy that obligation. The details of the Processing and transfer of the Personal Data are specified in Schedule 1. Schedule 2 provides a list of Sub-Processors that Data Protection Training and Auditing services may use to deliver their services, and Schedule 3 provides details of the Technical and Organisational Measures (TOMs) that the Company has in place with regard to the Security of Data.

Section A: Agreed fees and methodology of the services

Confirmation of Fee

Sample processing instruction are shown. All job prices will be agreed with the client before hand and confirmed in writing (including by email)

Instruction of Processing: Document Destruction ☐ Hard drive/Media Destruction ☐ IT Recycling ☐ Other:			
Nature of Service:	On-site x☐ Off-site ☐ Regular ☐ Bulk ☐		
Material type	Paper x☐ Hard drive ☐ Media ☐ Products ☐		Other:
Storage units to be shred	M1 White sacks ☐ Bankers boxes ☐ File boxes ☐ Lever Arch folders ☐ Pallets ☐ Consoles ☐		Wheelie Bins ☐ Other:
Pricing Profile (per unit)	M1 White sacks _____ Bankers boxes _____ File boxes _____ Lever Arch folders__ Pallets _____ Consoles _____ Media _____ Hard drives: _____ Estimated cost of service: _____ Minimum call out charge: _____ Wheelie Bins		Per kg rate: _____ Job Lot Price _____
Supply of consoles/wheelie bins	Deposit: ___ Rental: _____ Courier Charge: ___		Delivery details (other than Above):
Service interval	Once off _____ Daily _____ Weekly _____ Monthly_____		Quarterly or as required x Other:
Fees for additional paper material and other material agreed beforehand with Customer			Details:
Collection time/Days	Access hours from: _____ to _____ Restricted opening from: _____ to _____		Weekdays: _____ Weekends: _____
Designated Storage and other Facilities addresses (other than as already detailed): • Dublin Rd, Castleblayney, Co. Monaghan		**Customer Site Instructions:**	
Fees for above professional services are calculated Ex VAT			Currency: Euro x☐ Stg ☐

Methodology of delivery of services

All media for destruction are always attended by a Company employee or physically secured from unauthorized access while in the custody of the destruction contractor before they are destroyed. All shredding is to be at the customers site unless there is a written Customer agreement stating otherwise. This written agreement is on the invoice/certificate of destruction. A mobile shredding unit will go to or adjacent to a business premises. (Time frame for all shredding jobs is dependent on amount of material to be shredded. However all material must be shredded before the lorry leaves the Customer's premises.). The primary means to ensure this is by using a 240 litre wheelie bins lockable wheelie bin to collect in material around the sites. Our operatives will collect the office paper for shredding in either lockable wheelie bins; or heavy-duty plastic bags; or cord tied canvas bags contained within (previously provided) lockable consoles from the customer offices/premises. This will ensure that all media are securely contained during transfer from Customers' custody to the shredding lorry to prevent loss from wind or other atmospheric conditions by means of lockable wheelie bin. While the lorry is unattended it shall be locked. The hut will be locked in between all jobs using a wrench lock mechanism. No bin shall be left unattended without being locked. The paper for shredding is to be a single stream standard office paper with no contamination. If material is contained with folders the operatives will remove the paper from the folders, the paper placed in lockable wheelie bins and the folders either given back to the client; or removed for further processing off-site. The operative will bring this paper to the mobile shredding unit and proceed to shred. The plastic bags will be reused. The shredded paper is stored in the mobile shredding unit until delivered to a permitted recycling depot. Any readable debris will be immediately shredded. The shredding hut will be kept clean and tidy at all times. An invoice and certificate of destruction will be presented to the Customer at the end of each job. This receipt will include: Date, Type of media (Please note bulk = paper documentation); Description; Signature of client or their representative.

All waste receptacles are checked to ensure that they are free from unshredded confidential materials and no loose information bearing materials are scattered around destruction area. Attendance and security of material from Customer's premises to lorry and to prevent loss from wind or other atmospheric conditions: All media for destruction are always attended by a Company employee or physically secured from unauthorized access while in the custody of the destruction contractor before they are destroyed. The primary means to ensure this is by using a 240 litre lockable wheelie bins to collect in material around the sites. All media are securely contained in the above manner during transfer from Customers' custody to transportation vehicle to prevent loss from wind or other atmospheric conditions. All material will be brought in the lockable wheelie bin from the customers office etc directly to the shredding lorry. Use of these wheelie bins and the lockable hut, together with the above procedures ensures that the destruction vehicle and transport from client's premise to lorry is protected from loss due to wind, tipping/spillage or other atmospheric conditions.

Hard drive destruction methodology

M1 Document Solutions methodology for the physical destruction of computer hard drives is as follows:

- No shredding will be engaged without written instructions by the Customer.
- That serial numbers of all hard drives or CPUs being destroyed for each Customer are recorded, unless the Customer has signed an agreement opting out of this requirement.
- And that any opt out agreement must state that the Company is obligated, under NAID Certification standards, to have the Customer sign the agreement if they choose to not have their serial numbers recorded.
- Hard drives may be removed from their aluminium casing.
- All hard drives platters are physically shredded
- Where possible, all cases are recycled
- That the log of recorded serial numbers of hard drives destroyed is returned to the Customer upon the completion of the service, unless the Customer has opted out of this requirement.
- That a certificate of destruction is furnished for the work done

Section B: Terms of Engagement

1. SERVICES

1.1 Services to be Furnished. The Company will provide Services (hereinafter called the "services") as required and outlined at Section A. The services may, at Customer's option and as indicated on Section A, be performed as part of a regular schedule or pursuant to specific directions which Customer shall give the Company from time to time. The Customer may also request customised services which are not set out at Section 2, in which case the Company will consult with Customer as to the terms and conditions of the services requested. This may require an extension of the within Terms of Engagement and if same are not extended or amended in writing by the parties hereto, the parties agree that the within Terms of Engagement shall automatically apply to any new Contract for customised services.

1.2 Services to Affiliates and Subsidiaries. Customer's related, affiliated and subsidiary companies (including subsidiaries of affiliates) may request services in reliance upon this Agreement. Any provision of services by the Company to such an affiliate or subsidiary company(ies) will be evidenced by an Order executed by an authorised representative of the applicable affiliate or subsidiary in its own corporate name and referencing this Agreement and confirmation of their authority to requisition such an Order by the Customer will be required to be provided. In the event this is not provided, the affiliate or subsidiary company will be required to enter into a similar Contract to the Customer as the within. Invoices for such services shall be directed to and be payable by such affiliate or subsidiary unless otherwise agreed in writing.

2. RESPONSIBILITIES

2.1 Right to Rely on Instructions. Company may act in reliance upon any instruction, instrument, or signature reasonably believed by Company to be genuine, and may assume that any of Customer's employees or any employee of Customer's affiliates or subsidiaries giving any written notice, request, or instruction has the authority to do so. The Company is not required to investigate the authority of the employee to provide such notice, request or instruction to the Company.

2.2 Compliance with Contracts, Laws and Regulations. Customer shall be responsible for, and warrant compliance with, all contractual restrictions and all applicable laws, rules and regulations, including but not limited to environmental laws and contractual restrictions and laws governing the confidentiality, retention and disposition of information contained in any materials delivered to Company. Company shall comply with applicable laws, statutes, regulations which govern the services provided.

3. FEES AND PAYMENTS - All standard charges for services under this Agreement shall be as specified at the start of this agreement (Section A). The prices set forth in Section A shall remain in effect for the first twelve (12) months of this Agreement. Thereafter, price adjustments shall be made only after thirty (30) days' prior written notice. For any service requested by Customer that is not listed on Section A, the charges will be as agreed to in writing by Customer and Company prior to the rendering of such Service. Other payment terms are detailed on our website www.confidentialpapershredding.ie/payment .

4. CONFIDENTIALITY - "Confidential Information" means any information relating to Customer's property, business and affairs. Unless such Confidential Information was (A) previously known to Company free of any obligation to keep it confidential, (B) is subsequently made public by Customer or (C) by a third party having a legal right to make such disclosure, or (D) was known to Company prior to receipt of same from Customer, it shall be held in confidence by Company and shall be used only for the purposes provided for in this Agreement. The Company shall use the same degree of care to safeguard the Customer's Confidential Information as it uses to safeguard its own. However, Company may comply with any Court Order, subpoena from a Statutory Body, An Garda Siochana, or similar order related to materials delivered to Company; provided that it shall, unless prohibited by law, notify Customer promptly of any such Order, subpoena or notice. The Customer shall pay Company's reasonable costs for such compliance.

5. TERM AND TERMINATION

5.1 Term. This Agreement shall commence on the Effective Date set forth above and, unless otherwise terminated in accordance with Section 5.2, shall continue in effect for one year, with automatic renewal for

successive one-year terms, unless written notice of nonrenewal is delivered by either party to the other not less than ninety (90) days prior to the date of expiration of such term.

5.2 Termination. Either party may terminate this Agreement if the other is in material or repeated breach (said breach to be notified in writing to the registered office or point of contact in the offending party's company) of any of its obligations hereunder and the breaching party has not remedied the breach within sixty (60) days after written notice from the injured party. In the event of any such termination, all amounts due for services rendered up to the effective date of termination shall become immediately due and payable. Upon termination, Customer shall return (or permit Company to retrieve) all Company bins and other property kept at Customer's site per Clause 1.4, and the Company shall have no obligation to provide further services to Customer.

5.3 During the term of this Agreement (and any extensions or renewals), the client (Data Controller) is excluded from entering into any service agreements with other third parties for the provision of destruction or shredding services for paper, data holding IT equipment, media and product.

6. CLAIMS AND DISPUTE RESOLUTION

6.1 Time for Presenting Claims. The Customer must present any claim with respect to any Service in writing to Company within a reasonable time and in no case later than three (3) months after the occurrence of the event on which the claim is based.

6.2 Arbitration. Any claim, controversy, or dispute arising out of or relating to this Agreement, or any interpretation or breach of this Agreement or performance under this Agreement, including without limitation any dispute concerning the scope of this Article 6, that cannot be resolved within fifteen (15) working days by informal discussions between the parties, shall be decided by an Arbitrator agreed by the parties or, in default of agreement, appointed by the President for the time being of the Law Society of Ireland or in the event of his or her being unwilling or unable to do so by the next senior officer of the Law Society who is willing and able to make the appointment provided always that these provisions shall also apply to the appointment (whether by agreement or otherwise) of any replacement Arbitrator where the original Arbitrator (or any replacement) has been removed by Order of the High Court, or refuses to act, or is incapable of acting or dies.

6.3 Services during Arbitration. During any arbitration proceedings, Company shall continue to provide services, and Customer shall continue to make payments to Company, in accordance with this Agreement. The fact that arbitration is in being shall not impair the exercise of any termination rights under this Agreement.

7. LIABILITY AND WARRANTY

7.1 Limitation of Liability. Company shall not be responsible or liable in any manner whatsoever for the release or loss of any materials deposited in bins or otherwise delivered to it for secure destruction unless the release or loss is due to the proven negligence of the Company or wilful misconduct. Company's maximum liability for any and all claims arising with respect to the services provided under this Agreement shall not exceed the aggregate amounts paid by Customer with respect to the services provided at the particular Customer location during the six (6) months preceding the event which gives rise to a claim. In no event shall Company be liable for any consequential, incidental, special or punitive damages, regardless of whether the action is brought in tort, contract or any other ground.

7.2 Ownership Warranty. Customer warrants that it is the owner, legal custodian or otherwise has the right to deliver for confidential destruction of any and all materials the Customer provides the Company hereunder. The Customer shall reimburse the Company for any expenses reasonably incurred by Company (including reasonable legal fees) by reason of Company complying with its obligations under this Agreement to destroy such materials particularly in the event of a dispute concerning the destruction of the materials provided by the Customer to the Company.

8. ASSIGNMENT OF THE CONTRACT

The Company shall be entitled without the prior consent of or prior notice being provided to the Customer to assign this Contract to any other person or persons in which event such person(s) shall be bound by the

terms hereof as if said person(s) were party thereto and for the avoidance of doubt, such person or persons shall include a subsidiary company or a company formed as a joint venture company comprising the Company or subsidiary company of the Company and one or more parties. Notice of this assignment shall be served on the Customer within 28 days of completion of the assignment.

9. MISCELLANEOUS

9.1 Notices. All notices hereunder shall be in writing and addressed to either party at its address set forth above (or to such other address as either party may specify by notice given in accordance with this Section). Notices to Company shall be sent to the attention of its General Manager, Company secretary or other authorised officer.

9.2 Binding Nature and Assignment. This Agreement shall be binding on the parties and their respective successors and assigns. Except as permitted by Section 1.3 above, neither party may assign this Agreement, except to an affiliate, without the prior written consent of the other party, which consent shall not be unreasonably withheld.

9.3 Force Majeure. Each party shall be excused from any delay or failure in performance under this Agreement for any period if and to the extent that such delay or failure is caused by acts of God, governmental actions, labour unrest, riots, unusual traffic delays or other causes beyond its control.

9.4 Relationship of Parties. The Company is acting as an independent contractor hereunder and has the sole right and obligation to supervise, manage, contract, direct, procure, perform, or cause to be performed all work to be performed by the Company under this Agreement. The Company will properly and adequately manage the risks associated with fulfilment of this Agreement.

9.5 Entire Agreement. This Agreement constitutes the entire agreement between Company and Customer with respect to the subject matter of this Agreement. No change, waiver, or discharge of this Agreement shall be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be enforced. Except as provided in Section B, this Agreement may be amended only by an amendment in writing signed by Customer and Company.

9.6 Invalidity. If any provision of this Agreement is declared invalid by any Court or tribunal of requisite jurisdiction, then such provision shall automatically be adjusted to the minimum extent necessary to comply with the requirements for validity as declared at such time and as so adjusted shall be deemed a provision of this Agreement as though originally included herein. In the event that the provision invalidated is of such a nature that it cannot be so adjusted, the provision shall be deemed deleted from this Agreement as though such provision had never been included herein. In either case, the remaining provisions of this Agreement shall remain in effect.

9.7 Exclusivity: Customer agrees to retain Company on an exclusive basis at all facilities covered by this agreement for the term of this contract.

9.8 Default: If the Customer fails to comply with its obligations hereunder, or if the Customer goes into compulsory or voluntary liquidation save for the purpose of reconstruction or amalgamation, or if a receiver is appointed in respect of the whole or any part of its assets or if the Customer makes an assignment for the benefit of or composition with its creditors or threatens to do any of these things or threatens to cease carrying on business then without prejudice to any other rights or remedy available the Company may suspend or terminate the contract with immediate effect by notice in writing .

Section C: Data Processing Agreement

TERMS

The parties agree that:

1.1 The Data Controller and the Data Processor acknowledge that for the purposes of the Applicable Data Protection Law, **M1 Document Solutions Ltd** is the Data Processor in respect of any Personal Data.

1.2 The Data Processor shall process Personal Data only for the purposes of carrying out their obligations arising under the Service Agreement.

1.3 The Data Controller shall instruct the Data Processor to process the Personal Data in any manner that may reasonably be required in order for the Data Processor to carry out the processing in compliance with this Agreement and in compliance with Applicable Data Protection law.

1.4 The Data Controller shall refrain from providing instructions which are not in accordance with applicable laws including Applicable Data Protection law, and, in the event that such instructions are given, the Data Processor is entitled to resist carrying out such instructions.

1.5 The details of the transfer and of the Personal Data are specified in Schedule 1. The parties agree that Schedule 1 may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required by law. The parties may execute additional annexes/schedules to cover additional transfers, or may include multiple transfers in Schedule 1, which will be submitted to the DPC or other supervisiory authority where appropriate where required.

1.6 This Agreement shall continue for no less a term than the term of the Service Agreement.

1.7 The rights and obligations of the parties with respect to each other under this Clause 1 shall survive any termination of the Agreement.

2. REGULATORY COMPLIANCE

2.1 To the extent required by law or regulation:

2.1.1 The Data Processor shall co-operate with the Supervisory Authority in connection with any activities performed by the Data Processor;

2.1.2 The Data Controller, its auditors and the DPC or other supervisiory authority where appropriate shall have effective access to data related to such activities, as well as effective access to the Data Processor's business premises;

2.1.3 The DPC or other supervisiory authority where appropriate shall have without notice the right of access to the Data Processor's business premises for purposes for this Clause 2; and

2.1.4 The Data Processor shall give prompt notice to the Data Controller of any development that may have a material impact on the Data Processor's ability to perform services effectively under this Agreement and in compliance with applicable laws and regulatory requirements.

3. OBLIGATIONS OF THE DATA CONTROLLER

The Data Controller warrants and undertakes that:

3.1 The Personal Data has been collected, processed and transferred in accordance with the GDPR and all Applicable Data Protection law.

3.2 It has used reasonable efforts to determine that the Data Processor is able to satisfy its legal obligations under this Agreement.

3.3 It will respond to enquiries from Data Subjects and the DPC or other supervisiory authority where appropriate concerning processing of the Personal Data by the Data Controller, unless the parties have agreed that the Data Processor will so respond, in which case the Data Controller will still respond to the extent reasonably possible and with the information reasonably available to it if the

Data Processor is unwilling or unable to respond. Responses will be made within a reasonable time and in accordance with the Applicable Data Protection law.

3.4 It will make available, upon request, a copy of this Agreement to Data Subjects who are relevant to the processing, the subject matter of this Agreement, unless this Agreement contains confidential information, in which case it may redact such information. The Data Controller shall abide by a decision of the DPC or other supervisiory authority where appropriate regarding access to the full text of this Agreement by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Data Controller shall also provide a copy of this Agreement to the DPC or other supervisiory authority where appropriate where required.

4. OBLIGATIONS OF THE DATA PROCESSOR

The Data Processor warrants and undertakes that:

4.1 It will comply with all applicable law including Applicable Data Protection law in its performance of this Agreement.

4.2 It will only process the Personal Data on the instructions of the Data Controller.

4.3 It will not transfer Personal Data to a Third Country without the prior written approval of the Data Controller and only then once the transfer to the Third Country has been legitimised and the Data Controller and the Data Processor are satisfied that an adequate Data Protection regime exists in the Third Country.

4.4 It will not appoint sub-processors to process the Personal Data on its behalf without the prior written approval of the Data Controller. Data Processor will impose on such Sub-Processors data protection terms that protect the Protected Data to the same standard provided for by this DPA. Upon Data Controllers request, the Data Processor will provide to Customer a list of the then-current Sub- Processors. For the avoidance of doubt, the Data Controller hereby authorises the engagement by Data Processor of the Sub-processors set out in Schedule 2.

4.5 Once approved by the Data Controllers, sub-processors will only process the Personal Data on the instructions of the Data Processor and the Data Processor will put in place a legal agreement in writing to govern the sub-processing.

4.6 It will have in place appropriate technical and organisational measures, and all measures pursuant to Article 32 of the GDPR, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

4.7 It will obtain guarantees from any sub-processors processing the Personal Data, that they will have in place appropriate technical and organisational measures, and all measures pursuant to Article 32 of the GDPR, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected, including as a minimum implementing those measures specified in Schedule 3.

4.8 It will have in place procedures so that any individual party it authorises to have access to the Personal Data, including employees of the Data Processor, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Data Processor shall be obligated to process the Personal Data only on instructions from the Data Processor. This provision does not apply to persons authorised or required by law or regulation to have access to the Personal Data.

4.9 It will not disclose any Personal Data to a third party in any circumstances other than at the specific written request of the Data Controller, unless such disclosure is necessary in order to fulfil the obligations of the Services Agreement, or is required by applicable law.

4.10 It will notify the Data Controller of any request for information by the DPC or other supervisiory authority where appropriate and will not disclose any Personal Data without the prior consent of the Data Controller.

4.11 It will notify the Data Controller of any complaint, notice or communication received which relates directly or indirectly to the processing of the Personal Data, or other connected activities, or which relates directly or indirectly to the compliance of the Data Processor and/or the Data Controller with relevant applicable law including Applicable Data Protection law.

4.12 **Breaches:** The Data Processor will give the Data Controller prompt notice of a Personal Data breach or a potential data breach, once becoming aware of same, and the Data Processor will cooperate with the Data Controller in implementing any appropriate action concerning the breach or the potential breach as the case may be, including corrective actions. The Data Processors shall include in its notification to the data controller pursuant to Clause 4.12 (as a minimum):

4.12.1 a description of the nature of the breach including, without limitation and where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

4.12.2 the name and contact details of the Data processors data protection manager who can provide further information to the customer about the breach;

4.12.3 a description of the likely consequences of the breach, including without limitation, the likely impact and consequences of the breach on the relevant data subjects, and the Data Controller

4.12.4 a description of the initial remedial measures taken by the Data Processor or proposed to be taken by Data Processor to address the breach, including without limitation and where appropriate, measures to mitigate its possible adverse effects;

4.13 It will delete from its systems all soft copies of any Personal Data and return all soft and hard copy documentation on the completion of the Service Agreement or on request from the Data Controller and will do so in a timely manner, giving a written confirmation of same having been done. The only exception to this Clause 4.14 shall be where the Data Processor shall have a legitimate reason, which is confirmed by the Data Controller, to continue to process particular data or where it is legally required to maintain data records.

4.14 Without prejudice to other legal provisions concerning the Data Subject's right to compensation and the liability of the parties generally, as well as legal provisions concerning fines and penalties, the Data Processor will carry full liability in the instance where it or its sub-processor is found to have infringed applicable law including Applicable Data Protection law through his processing of the Personal Data.

4.15 It has no reason to believe, at the time of entering into this Agreement, of the existence of any reason that would have a substantial adverse effect on the guarantees provided for under this Agreement, and it will inform the Data Controller (which will pass such notification on to the DPC or other supervisiory authority where appropriate where required) if it becomes aware of any such reason.

4.16 It will process the Personal Data for purposes described in Schedule 1, and has the legal authority to give the warranties and fulfil the undertakings set out in this Agreement.

4.17 It will identify to the Data Controller a contact person within its organisation authorised to respond to enquiries concerning processing of the Personal Data, and will cooperate in good faith with the Data Controller, the Data Subject and the DPC or other supervisiory authority where appropriate concerning all such enquiries within a reasonable time.

4.18 It will register with the DPC or other supervisiory authority where appropriate in accordance with the Applicable Data Protection law and do all things necessary to comply with the Applicable Data Protection law and be responsible in accordance with law, both statutory and common law to Data Subjects for any infringement of privacy or disclosure arising from its negligence, howsoever caused.

4.19 It will be capable of demonstrating its compliance with the obligations of Applicable Data Protection law.

5. **RIGHT OF AUDIT**

5.1. Upon reasonable request of the Data Controller, the Data Processor will submit it, and/or as appropriate its sub-processors will submit, data processing facilities, data files and documentation used for processing, reviewing, auditing and/or certifying by the Data Controller (or any independent or impartial inspection agents or auditors, selected by the Data Controller and not reasonably objected to by the Data Processor) to ascertain compliance with the warranties and undertakings in this Agreement, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Data Controller.

6. **DATA SUBJECTS' RIGHTS**

6.1. The Data Processor will assist the Data Controller, whenever reasonably required, in so far as possible, to fulfil the Data Controller's obligation to respond to requests for exercising the Data Subject's rights as provided under Applicable Data Protection law and the Data Processor will have the appropriate organisational and technical measures in place to deal with Data Subject requests.

7. **LIABILITY AND INDEMNITY**

7.1 The Data Processor will not be liable for any claim brought by a Data Subject arising from any action by the Data Processor to the extent that such action resulted directly from the Data Controller's instructions.

7.2 Except as provided for in Clause 7.1, the Data Processor shall indemnify the Data Controller for any monetary fine or penalty imposed on the Data Controller by the DPC or other supervisiory authority where appropriate that results from the Data Processor's breach of its obligations under this Agreement.

7.3 In the event that any claim is brought against the Data Controller by a Data Subject arising from any action by the Data Processor, to the extent that such action did not result directly from the Data Controller's instructions, the Data Processor shall indemnify and keep indemnified and defend at its own expense the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor or its directors, officers, employees, agents or contractors to comply with any of its obligations under this Agreement.

7.4 In the event that any claim is brought against the Data Processor by a Data Subject arising from any action or omission by the Data Processor to the extent that such action or omission resulted directly from the Data Controller's instructions, the Data Controller shall indemnify and keep indemnified and defend at its own expense the Data Processor against all costs, claims, damages or expenses incurred by the Data Processor for which the Data Processor may become liable due to any failure by the Data Controller or its directors, officers, employees, agents or contractors to comply with any of its obligations under this Agreement.

7.5 Either party will provide the other party with evidence of financial resources to confirm it has sufficient such resources to fulfil its responsibilities under Clause 7.3 and 7.4 as appropriate (which may include proof of insurance cover).

8. LAW APPLICABLE TO THIS AGREEMENT

This Agreement shall in all respects be governed by and interpreted in accordance with the laws of the Republic of Ireland. The parties hereto hereby submit to the exclusive jurisdiction of the Irish Courts for all the purposes of this Agreement.

9. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE DPC OR OTHER SUPERVISIORY AUTHORITY WHERE APPROPRIATE

9.1 In the event of a dispute or claim brought by a Data Subject or the DPC or other supervisiory authority where appropriate concerning the processing of the Personal Data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

9.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the DPC or other supervisiory authority where appropriate. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

9.3 Each party shall abide by a decision of the DPC or other supervisiory authority where appropriate which is final and against which no further appeal is possible.

10. TERMINATION

10.1 In the event that either the Data Processor or the Data Controller is in breach of its obligations under this Agreement, then the Data Controller may temporarily suspend the transfer of Personal Data to the Data Processor until the breach is repaired or the Agreement is terminated.

10.2 The parties agree that the termination of this Agreement at any time, in any circumstances and for whatever reason (except for termination under Clause 10.2) does not exempt them from the obligations and/or conditions under this Agreement as regards the processing of the Personal Data transferred.

SCHEDULE 1
DESCRIPTION OF THE TRANSFER / PROCESSING

a. The subject matter and nature of the processing:

The destruction of Confidential documentation and other media holding data, which includes personal data.

b. The purpose of the processing:

- The confidential destruction of documentation – on site / Off site
- The confidential destruction of Hard drives – on site / Off site
- The confidential destruction of Floppy disks, data tapes etc – on site / Off site

c. The type of personal data involved:

Personal data as defined by the GDPR including employee and customer details. May also include special categories of data including health records.

d. The categories of data subjects

General employee and customer details.

e. The duration of the processing:

For duration of this contract.

SCHEDULE 2
List of Sub-Processors

Our organisation maintains a list of sub processors to which personal data may be transfered. The Data Processors agreement that is in place with these processors is reviewed on an annual basis to ensure that it is in line with articles 28 and 29 of the GDPR.

Name of sub processor	**Function**	**Location**
Data Protection Training and Auditing Services	• Administrative Support • Data Protection Advice	Monaghan, Ireland
Hands on HR	• HR matters	Louth, Ireland
Cycubix	• IT consultancy	Dublin, Ireland
Collsoft	• Payroll	Meath, Ireland
Clinton Higgins Accountants	• Accounting services	Kildare, Ireland
MS 365 / One Drive	• Electronic Document Storage	EU
Dropbox	• Electronic Document Storage	EU
Inventise	• IT service Provider	Wicklow/Dublin, Ireland
Fastways	• Courier services	Louth/Dublin, Ireland
Siteguard	• Hosting services	EU
Bemoore.com	• Software Development	Cork, Ireland

SCHEDULE 3
Technical and Organisational Measures (TOMs) for the Security of Data within Data Protection Training and Auditing Services

M1 Document Solutions Ltd is a Monaghan based company providing an All-Island Document Shredding and Storage service. We have extensive experience in the secure document and material shredding, scanning and storage sector. Backed by Government permits and Certificates of Destruction, we come to our client's premises and shred all confidential documents, materials, hard-drives and CDs. We are committed to providing secure, confidential storage, scanning and shredding services to our clients in a cost effective and hassle free manner. This commitment is a keystone of all that we do, reflected in the services we provide to our customers, the conditions under which our employees work, and our interactions with the communities where we live and do business. We are responsible stewards of the environment and protect the health and wellbeing of our employees and neighbours.

The GDPR requires organisations to implement, test and evaluate Technical and Organisational Measures (TOMs) to ensure the security of the data processing. The following measures are designed to:

- ensure the security and confidentiality of Personal Data;
- protect against any anticipated threats or hazards to the security and integrity of Personal Data;
- protect against any actual unauthorised processing, loss, use, disclosure or acquisition of or access to any Personal Data

Section 1: People, Awareness and HR

Data Protection Officer

An expert, level 9 qualified (on national framework) Data Protection Officer has been appointed and registered with the Data Protection Commission.

Data Protection and IT Security Awareness Training

Monthly, online Security Awareness Training Course for employees ensuring continued High Levels of Security Awareness

- A new Security and Compliance Course every Quarter
- Certificates upon completion
- Users own portal login

Managed Phishing simulations and training campaigns to reduce the risk of malicious email

- Ensuring that spurious emails that slip through your existing IT screening infrastructure are not clicked on or accessed by staff
- Implementation of a monthly Phishing simulation campaign
- 3 minute "Golden Nugget" training at time of error for users to learn

Tailored Data Protection training:

- To ensure knowledge and compliance with organisations procedures with regard to Data Breaches, IT security incidents and Data subject Access Requests
- Annual internal Data Protection Readiness tests are conducted to verify the security practices
- Live interactive training with a Certified Data Protection officer

HR related data

- All recruitments follow a screening process
- In each contract each employee has Non-Disclosure Agreements clauses
- Data protection, IT Acceptable Use policy and IT Security policy statement are shared with all employees

- Access to systems is provided on a 'need to have basis' taken into account segregation of duties
- Work instructions on handling private data;
- User (password) codes for access to Private Data;
- Differentiated access regulations (e. g. partial blocking);
- Access Logging and control

Access and authentication

M1 Document Solutions Ltd. maintains a list of "NAID Access and non access personnel". All access Employees are obliged by contract to undertake:

- Confidentiality agreements
- Employment screening restriction requirements
- Criminal Record Search
- Drug Screening
- Employment history verification

All access employees are in uniform and have an identity badge which includes a photo, employee name and Company name.

Access Employee training programme of compliance

All access employees have studied the NAID Access Employee Training Video and completed the test for same. All access employees have passed this test.

Section 2: Security for Physical Data

Lorry security measures and Two- way communications

The lorry is lockable using standard key mechanism. The hut is lockable using a bolt and lock mechanism. Vehicle and hut are secured in line with operational policies. The vehicle cabs and hut are locked during transport and when unattended by Access Individual. All drivers of destruction vehicles have readily accessible two-way communication devices in this case a cell phone. Phone records available in invoices folder.

Paper and Media Destruction

- An appropriate Data retention policy is in place and monitored annually.
- Redundant or past retention period paper documents or records are placed into secure receptacles and confidentially shredded on-site by an EN 15713, NAID and Qualsec certified Shredding company.
- Hard drives are removed from redundant computers for secure destruction by an EN 15713, NAID and Qualsec certified Shredding company.
- Other media (CDs, video etc) is securely destroyed by an EN 15713, NAID and Qualsec certified Shredding company.
- All shredding or data destruction is certified

Physical Security of Building

- Access control and visitor management systems implemented for all visitors/guests
- CCTV surveillance to protect restricted areas
- Fire alarm and fire-fighting systems implemented for employee safety;
- Fire evacuations drills are conducted at specified frequencies

Clean desk policy

- Clean desk, clear screen and follow me printing, process implemented;

Remote working

- Except with prior specific authorization, laptops and desktops are not taken off the site;

- The remote users are working with laptop and desktop provided and maintained by our organisation.
- Encryption of the hard disk on company assigned laptops
- 2 Factors Authentication (PKI / Alternative)
- Centrally managed and anti-virus protection
- Management and monitoring of the software to control an authorized software installation
- Vendor supplied updates are installed
- Login ID and password controls are implemented to access information
- Periodic access review is implemented
- E-mails are automatically scanned by anti-virus and anti-spam software.

Section 3: IT Access Control and system security

Firewall configuration

- Appropriate Firewall security is in placed within the main office
- Access to coloud based data and system is subject to two-factor authentication

Security and confidentiality of personal data

Based on a risk assessment (and if required an additional DPIA) our organisation will ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- ensure a logical separation between its own data, the data of its customers and suppliers
- setup a process to keep processed data accurate, reliable and up-to-date.
- Process registers according GDPR requirements
- Access log systems' use with relevant for the purposes of being able to detect unauthorized access attempts

Secure Configuration of System

- Data is only stored in the EU Data Centers or in case of servers encrypted on the local device
- Multiple layers of firewalls & intrusion detection need to be passed;
- Access managed according to Role Based Access Control principles.

Anti-virus, malware and Patch Management

All devices have up to date anti-virus, malware and patch management in place

Backups and Restores

All records at these listed off-site cloud locations is backed up by internal procedures and backed-up both onsite at our offices and off-site at the general managers private residence on a password encrypted PC.

Section 4: Business Continuity Plan and certification

Business Continuity Plan is in place and is available upon request.

Certification

The following are a list of current certifications:

- IS EN15713
- NAID "AAA" Certification
- Qualsec Gold