VOULT

DATA PROTECTION AGREEMENT - SAAS

1. Scope

1.1 This '*Voult – Data Protection Agreement - SaaS*' (this "**DPA**") applies to Voult Ltd's ("**Voult**") Processing of Protected Data pursuant to the Agreement in connection with Voult's provision of certain '*Software as a Service*' Services. This DPA is made in connection with the provision by Voult of access to and use of such Services to its applicable customers (in this DPA each a "**Customer**").

1.2 In this DPA the "**Agreement**" means, in respect of the Customer in question, the master services agreement known as '*Voult – MSA – SaaS – 1 March 2025*' entered into/ accepted by that Customer. The online version of the Agreement where accepted being found at https://voult.com/legal/.

1.3 This DPA is a Voult Policy and applies to, forms part of and is supplemental to the Agreement. The terms of the Agreement shall apply to this DPA and are incorporated herein, *mutatis mutandis*, to this DPA.

1.4 For each Customer, this DPA together with the applicable Order Form, the Agreement, any applicable Solution Terms, the other Voult Policies and any other applicable document that forms part of and/or is supplemental to the Agreement from time to time, applies to the subject matter of that Order Form and that Customer's access to and use of the applicable Services.

1.5 Unless otherwise noted or where the context otherwise requires, all capitalised terms used herein shall have the meanings set forth in the Agreement and the definitions document known as '*Voult – Definitions re MSA - SaaS – 1 March 2025*' (https://voult.com/legal/).

1.6 It is hereby agreed and acknowledged that, despite Voult's technical access to, use, and storage of Protected Data, in general, when providing its services under the Agreement, Voult will only 'see' (where permitted) Customer Data in a very limited capacity.

2. Definitions

"**Article 46 Tools**"	the tools provided for in Article 46 of the GDPR as mechanisms for safeguarding Protected Data being the subject matter of a 'restricted' transfer (each an "**Article 46 Tool**").
"**Controller**"	has the meaning given to that term in Data Protection Laws. "Controller" also has the same meaning as "Business" as that term is defined under applicable Data Protection Laws.
"**Data Protection Laws**"	means all applicable data protection laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations which may include: (i) the GDPR; (ii) the Data Protection Act 2018 (being legislation in England and Wales); (iii) the California Consumer Privacy Act (CCPA); (iv) any laws which implement or supplement any such laws; (v) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing; and (vi) any other such data protection or privacy laws applicable to Voult or the Protected Data.
"**Data Protection Losses**"	means all liabilities arising directly or indirectly from any breach or alleged breach of any of the Data Protection Laws or of this DPA, including all: (i) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); (ii) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (iii) compensation which is ordered by a court or Supervisory Authority to be paid to a Data Subject; and/or (iv) costs of compliance with investigations by a Supervisory Authority.

"**Data Subject**"	means an identified or identifiable natural person.
"**Data Subject Request**"	means a request made by a Data Subject to exercise any applicable rights under Data Protection Laws in relation to Protected Data.
"**GDPR**"	means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time).
"**Hosting/ Data Storage Arrangements**"	as defined in **paragraph 8.2**.
"**Hosting/ Data Storage Regions**"	the particular designated regions by Voult from time to time (comprising one or more Hosting/ Data Storage Territories) where Voult or its applicable Sub-Processor(s) has a main hosting function (a Primary Datacenter Location) and a replicate/ back-up function (a Secondary Datacenter Location) in respect of the Hosting/ Data Storage Arrangements (each such region a "**Hosting/ Data Storage Region**").
"**Hosting/ Data Storage Territories**" and "**Hosting/ Data Storage Territory**"	each as defined in **paragraph 8.2**.
"**Lawful Safeguards**"	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time.
"**Permitted Auditor**"	as defined in **paragraph 9.2**.
"**Personal Data**"	or similar term as defined under Data Protection Laws.
"**Personal Data Breach"**	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data Processed by Voult (including any Sub-Processors).
"**Primary Datacenter Location**"	as defined in **paragraph 8.2.1**.
"**Processing**"	has the meaning given to that term in Data Protection Laws (and related terms such as "**Process**", "**Processes**" and "**Processed**" have corresponding meanings).
"**Processing Instructions**"	as defined in **paragraph 4.1.1**.
"**Processor**"	has the meaning given to that term in Data Protection Laws.
"**Protected Data**"	means Personal Data in the Customer Data.
"**Relevant Territory**"	a country or territory or those countries or territories where (as a result of local laws or local restrictions) Voult or its applicable Sub-Processor(s) cannot use its standard hosting of/ data storage in connection with the

	provision of the Services (via the Platform) and has implemented separate or enhanced arrangements for the hosting of/ data storage in connection with the provision of the Services (via the Platform) to comply with/ accommodate such local laws or local restrictions (details of any such arrangements to be notified to Customer in accordance with the Agreement) (and "**Relevant Territories**" shall be construed accordingly).
"**Restricted International Recipient**"	means the organisations, bodies, persons and other recipients to which transfers of the Protected Data are prohibited under **paragraph 8** without taking steps to ensure such transfers comply with applicable Data Protection Laws.
"**Secondary Datacenter Location**"	as defined in **paragraph 8.2.1**.
"**Site Reliability Engineering**"	the IT operations function (the Hosting/Data Storage Arrangements, quality assurance and security) in connection with the provision of the Services (via the Platform) and being specifically focused making sure production runs in respect of the same.
"**SRE Personnel**"	those persons employed by or contracted to: (i) Voult, Cyferd and/or any of its/ their Affiliates; or (ii) the Sub-Processor in question (as the case may be), who deal(s) with the Site Reliability Engineering (or any part of it).
"**Standard Contractual Clauses**"	refers to Module 2 of the Standard Contractual Clauses promulgated by the EU Commission Decision (EU) 2021/914, (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914) ("**Module 2**"). However, for transfers of Personal Data from the United Kingdom ("**UK**"), refers to Module 2 in tandem with the UK Addendum (https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf).
"**Supervisory Authority**"	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.
"**Voult's Systems**"	means, for purposes of this DPA, the Platform Perimeter, including any other facilities, systems, equipment and software Voult and its Sub-Processors use to Process Customer Data.

3. Processor and Controller

3.1 The Parties agree that, between the Parties, for all Protected Data, Customer shall be the Controller and Voult shall be the Processor. Nothing in the Agreement relieves the Parties of any responsibilities or liabilities under any Data Protection Laws.

3.2 Voult shall Process Protected Data in compliance with:

3.2.1 all applicable Data Protection Laws as a Processor (and where applicable as a sub-processor); and

3.2.2 the terms of the Agreement.

3.3 Customer shall comply with:

3.3.1 all applicable Data Protection Laws in connection with the Processing of Protected Data under the Agreement; and

3.3.2 the terms of the Agreement.

4. Instructions and details of Processing

4.1 Where and to the extent that Voult Processes Protected Data, Voult shall:

4.1.1 unless otherwise required by applicable law, Process the Protected Data only on and in accordance with Customer's documented instructions and to provide the services set out in the Agreement (including with regard to transfers of Protected Data to any Restricted International Recipient) ("**Processing Instructions**");

4.1.2 if applicable law requires it to Process Protected Data other than in accordance with the Processing Instructions, and where permitted by applicable law: (i) notify Customer of any such requirement before Processing the Protected Data; (ii) provide such necessary details that it may have about the requesting party, the types of Personal Data requested, and the purpose and methods of the disclosure, and (iii) where applicable, also comply with the notice obligations set forth in Clause 15.1 of the Standard Contractual Clauses;

4.1.3 promptly inform Customer if Voult becomes aware of a Processing Instruction that, in Voult's reasonable opinion, infringes Data Protection Laws. Voult (and each Sub-Processor) is not obliged to undertake any Processing of Protected Data that Voult reasonably believes infringes any of the Data Protection Laws;

4.1.4 unless expressly permitted by applicable Data Protection Laws, not retain, use, disclose, or otherwise Process Protected Data: (i) for any purposes other than those specified in the Agreement (including any applicable Order Form and applicable Solutions Terms), this DPA and in **Annex A**; (ii) for any commercial purpose other than the specific business purposes specified in the Agreement (including any applicable Order Form and applicable Solutions Terms) and this DPA, including to provide services to a different business; and (iii) outside the direct business relationship between Customer and Voult, including to combine or update Personal Data with information received from or on behalf of another source or collected from Voult's own interactions with a Data Subject;

4.1.5 limit Protected Data collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Processing set out in this DPA and the Agreement (including any applicable Order Form and applicable Solutions Terms) and not Process the Protected Data in a manner incompatible with those purposes;

4.1.6 not "sell" or "share" Protected Data, as applicable Data Protection Laws define those terms;

4.1.7 treat all Protected Data as the confidential information of Customer;

4.1.8 with respect to de-identified data, take reasonable measures to: (a) ensure that such data cannot be associated with a Data Subject or household, (b) publicly commit to Process such data only in a de-identified fashion and not attempt to re-identify such data; and (c) contractually obligate recipients to do the same; and

4.1.9 appoint and maintain a data protection officer, where required by applicable Data Protection Laws.

4.2 Customer acknowledges and agrees that the execution of any computer command to Process (as noted by definition includes but is not limited to the deletion of) any Protected Data made in connection with the applicable access to and use of the Services (via the Platform) by any applicable Authorised Users (including any consequential commands resulting from any automated process(es) in connection with such access to and use of the Services (via the Platform) (including in any Solution)) will be a Processing Instruction (other than to the extent such command cannot be fulfilled due to technical, operational or other reasons, including as set out in the Documentation). Customer acknowledges and accepts that if any Protected Data is deleted pursuant to any such command Voult is under no obligation to seek to restore it unless and to the extent that Data Protection Laws require such restoration.

4.3 The duration of Processing of the Protected Data by Voult under the Agreement, the nature and purpose of such Processing, the types of Personal Data and categories of Data Subjects so Processed are further specified in **Annex A** to this DPA.

4.4 The Customer shall be responsible for ensuring all of its Authorized Users read and understand this DPA.

5. Technical and organisational measures

5.1 Voult shall implement, maintain, and monitor a comprehensive written information security policy that contains appropriate administrative, technical, and organisational safeguards to ensure the confidentiality, integrity, and availability of Protected Data and prevent any unauthorised or unlawful Processing of such data. The safeguards will be appropriate to the nature of the Personal Data, meet or exceed prevailing industry standards, comply with Data Protection Laws, and the requirements set forth in the **Information Security Exhibit (Annex B).**

5.2 Voult will procure annual SSAE 18 Type II or SOC2 audits (or audits of a substantially similar standard) conducted by an independent third party. The results of such an audit will be provided to Customer upon request. Voult will also inform Customer of any material vulnerabilities discovered by any such audit and the nature of each such material vulnerability. If the audit reveals one or more material vulnerabilities which, in the reasonable opinion of Voult, would likely have an adverse material effect on the Processing of Protected Data by Voult, Voult will (subject to the next sentence) promptly correct each such material vulnerability at its sole cost and expense and will certify in writing to Customer when it has corrected all such material vulnerabilities within an agreed upon timeframe. Customer acknowledges that Voult provides a commoditized one-to-many service and the needs or assessments of other customers may differ. Voult shall not be obliged to implement any further or alternative security measures. If Voult cannot or will not correct any material vulnerability (revealed by such assessment/ audit), then it shall notify Customer of the same, and without prejudice to any other right or remedy of Customer, Customer may terminate the Agreement immediately by giving notice in writing to Voult within 30 (thirty) days of being notified that it cannot be corrected, such termination to take effect on the expiry of the notice. In the event of such valid termination by Customer under this **paragraph 5.2** then the applicable clauses of the Agreement shall apply.

5.3 In accordance with applicable Data Protection Laws, during the period in which Voult Processes any Protected Data, Customer shall be entitled to undertake a documented assessment, or other audit as appropriate, of whether the security measures implemented in accordance with **paragraph 5.1** are sufficient to protect the Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access under Data Protection Laws. Customer shall provide the results of such an assessment/ audit to Voult upon receipt, without undue delay. Voult will use reasonable efforts to make available all information necessary to demonstrate its compliance with Data Protection Laws and this DPA. Voult will: (i) cooperate with any such assessment/ audit; (ii) grant Customer or a Permitted Auditor reasonable access, during normal business hours, to Voult's Systems, records, procedures, and information that relate to the Processing of Protected Data to the extent necessary to undertake such assessment/ audit; (iii) (if such assessment/ audit reveals one or more material vulnerabilities which, in the reasonable opinion of Voult, would likely have an adverse material effect on the Processing of Protected Data by Voult) will (subject to the next sentence) address any such material vulnerability at its sole cost and expense by implementing industry best practices; and (iv) certify in writing to Customer when it has corrected all such material vulnerabilities within an agreed upon timeframe. Customer acknowledges that Voult provides a commoditized one-to-many service and the needs or assessments of other customers may differ. Voult shall not be obliged to implement any further or alternative security measures. If Voult cannot or will not correct any material vulnerability (revealed by such assessment/ audit), then Voult shall notify Customer of the same and without prejudice to any other right or remedy of Customer, Customer may terminate the Agreement immediately by giving notice in writing to Voult within 30 (thirty) days of being notified that it cannot be corrected, such termination to take effect on the expiry of the notice. In the event of such valid termination by Customer under this **paragraph 5.3** then the applicable clauses of the Agreement shall apply. Customer will bear the costs of such an audit, unless the audit reveals material vulnerabilities which, in the reasonable opinion of Voult, would likely have an adverse material effect on the Processing of Protected Data by Voult, in which case Voult will cover the costs of the audit.

6. Using staff and other Processors

6.1 Voult may not alter or add Sub-Processors except with the express written consent of Customer, which Customer shall not unreasonably withhold or delay. In the event Voult intends to alter or add Sub-Processors, Voult will provide Customer with at least thirty (30) days' prior written notice. Customer acknowledges that Voult provides a commoditized one-to-many service and the needs or assessments of other customers may differ. Customer agrees and acknowledges that it would be unreasonable to withhold or delay giving its consent where such addition or alteration does not materially adversely affect the use of the Services by Voult's customers generally.

6.2 Customer authorises the appointment of each of the Sub-Processors identified on the List of Sub-Processors as at the Effective Date.

6.3 Voult shall:

6.3.1 prior to the relevant Sub-Processor carrying out any Processing activities in respect of the Protected Data, ensure each Sub-Processor is appointed under a written contract containing materially the same obligations as under this DPA (including those obligations relating to sufficient guarantees to implement appropriate technical and organisational measures);

6.3.2 remain the primary point of contact for Customer regarding any Processing of Protected Data; and

6.3.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

6.4 Voult shall ensure that its personnel/ its Affiliate's personnel engaged in the Processing of Protected Data (including Voult's SRE Personnel) are informed of the confidential nature of the Protected Data, have received appropriate training on their responsibilities, and have executed applicable written confidentiality agreements.

7. Assistance with compliance and Data Subject rights

7.1 Voult shall promptly refer all Data Subject Requests (that expressly relate to Customer and any applicable Protected Data) it receives to Customer. To the extent that applicable Protected Data is in the control or possession of Voult (or its Sub-Processors), Voult will use reasonable efforts to cooperate, and follow any reasonable and lawful written instructions Customer issues to Voult, in responding to such requests in a timely and lawful manner, taking into account the technical restrictions of the Services, any applicable Solutions and/or the Platform.

7.2 Voult shall provide such reasonable assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to Voult (and its Sub-Processors) to Customer in ensuring compliance with Customer's obligations under Data Protection Laws, including but not limited to:

7.2.1 security of Processing;

7.2.2 data protection impact assessments (as such term, or similar term, is defined in Data Protection Laws);

7.2.3 prior consultation with a Supervisory Authority regarding high risk Processing; and

7.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by Customer in response to any Personal Data Breach,

8. International data transfers

8.1 Voult shall not transfer any Protected Data without taking steps to ensure such transfers comply with applicable Data Protection Laws.

8.2 (Subject to any special hosting and/or data storage arrangements agreed in writing by Voult with Customer in connection with the Agreement) those countries and territories which are applicable to the then current hosting and/or data storage arrangements for the Platform (and hence the Services and any Solution) (without which Customer could not access or use the Services (via the Platform) as provided for in this DPA, the Agreement (including in the provisions relating to the Hosting Services and/or the Database Services) and/or the List of Sub-Processors (such hosting and/or data storage arrangements being the "**Hosting/ Data Storage Arrangements**") include**:**

8.2.1 any country or territory that is a then country or territory where the Platform (and hence the applicable Services/ Solution) is then currently hosted (whether as a main hosting function (each such main hosting function location being a "**Primary Datacenter Location**") or a replicate and back-up function (each such replicate and back-up function location being a "**Secondary Datacenter Location**"), provided that such country or territory shall not include any countries or territories which are prohibited by applicable law for transfers of applicable Protected Data; and/or

8.2.2 (where Customer is based in a Relevant Territory and/or needs to access and use the Services (via the Platform) from a Relevant Territory) that Relevant Territory or each of the applicable Relevant Territories (as the case may be),

(such countries and territories being together the "**Hosting/ Data Storage Territories**" and each a "**Hosting/ Data Storage Territory**"). The transfer of Protected Data will occur between the applicable Hosting/ Data Storage Territories in a particular Hosting/ Data Storage Region as part of the Hosting/ Data Storage Arrangements. For example, if an Authorised User (based in the United Kingdom or Spain for the purposes of this example) of Customer (being based in France for the purposes of this example) executes a computer command to Process any Protected Data as part of/ during Customer's use of the Services (via the Platform) (being a Processing Instruction) then the applicable Primary Datacenter Location and the applicable and corresponding Secondary Datacenter Location will be the applicable Hosting/ Data Storage Arrangements for Customer and the result of that Processing Instruction will be: (i) recorded (in two separate copies) as part of the main current hosting arrangements for the Platform (and hence the applicable Services/ Solution) in the applicable Primary Datacenter Location and (ii) replicated (as an additional copy) as part of the replication/ back-up current hosting arrangements for the Platform (and hence the applicable Services/ Solution) in the applicable and corresponding Secondary Datacenter Location.

8.3 Customer hereby authorises Voult (or any Sub-Processor) to transfer any Protected Data for the purposes referred to in **paragraph 4.1** to any Restricted International Recipient(s), provided all transfers of Protected Data by Voult (or any Sub-Processor) to a Restricted International Recipient shall (to the extent required under Data Protection Laws) be effected by way of applicable Lawful Safeguards and at all times in accordance with Data Protection Laws and the Agreement. The provisions of the Agreement (including this DPA) shall constitute Customer's instructions with respect to transfers in accordance with **paragraph 4.1.1**.

8.4 The Lawful Safeguards employed in connection with transfers pursuant to **paragraph 8.3** shall be as follows: Voult will (where applicable) undertake a transfer risk assessment or a transfer impact assessment prior to making a 'restricted' transfer to verify, on a case-by-case basis, if the law or practice of the third county in question impinges on the effectiveness of the Article 46 Tool (or local equivalent) to be used and/or to see if there is a then current '*adequacy decision*' or '*adequacy regulation*' stating that the specific Restricted International Recipient or third country in question provides an adequate level of protection in respect of the proposed 'restricted' transfer. Voult will use applicable Standard Contractual Clauses as the mechanism for safeguarding Protected Data that is the subject matter of a 'restricted' transfer; or, where not possible, the use any of the other Article 46 Tools (or local equivalent) **PROVIDED THAT** where the applicable Article 46 Tool (or local equivalent) on its own would not (having regard to the transfer risk assessment/ transfer impact assessment) provide sufficient safeguards, Voult will (if and to the extent required) implement supplementary measures/ extra steps and protections, which may be standard contracts clauses, data privacy framework, organisational and/or technical, to bring protections up to the level required by law.

8.5 If the Parties will engage in transfers of Protected Data to Restricted International Recipients subject to the Standard Contractual Clauses—which are hereby incorporated by reference and deemed executed by the Parties as of the Effective Date—Voult will be the "*data importer*", Customer will be the "*data exporter*" and **Annex A** will provide the supplementary information required. References to a "*Member State*" and "*EU Member State*" will not be read to limit or prevent Data Subjects in Switzerland or other applicable jurisdictions from seeking to exercise their rights. If there is any conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

8.6 Customer acknowledges that due to the nature of cloud services, the Protected Data may be transferred to other geographical locations in connection with Customer's access to and use of the Services (via the Platform) further to access and/or computerised instructions initiated by Authorised Users. Customer acknowledges that Voult may not control such Processing.

9. Information and audit

9.1 Voult shall maintain, in accordance with applicable Data Protection Laws, written records of all categories of Processing activities carried out on behalf of Customer. Voult will already have access to the data logs relating to its tenancy(ies) which host the applicable Services/ Solutions. Voult (via its applicable Sub-Processor) will have access to 'Platform data logs' in respect of the Platform, part of which will relate to Voult's tenancy(ies) which host the applicable Services/ Solutions/ generic 'Platform' activity relevant to all customers and part of which will relate to other customers' tenancies relating to the Platform.

9.2 As noted in **paragraphs 5.2 and 5.3**, on request, Voult shall provide Customer (or a Permitted Auditor mandated by Customer) with a copy of the third-party certifications and audits to the extent applicable to the Protected Data or the data identified in **paragraph 4.1.8**, or as otherwise required by Data Protection Laws. A "**Permitted Auditor**" is an independent third-party auditor who is acceptable to both Parties. A Permitted Auditor shall be required to enter into a separate confidentiality agreement in favor of Voult in a form to Voult's satisfaction in this regard.

9.3 Notwithstanding the generality of **paragraph 9.2**, any information provided to Customer arising from, in connection with or relating to any information request or audit or inspection in connection with **paragraph 9.2** or otherwise shall be confidential to Voult and shall be Confidential Information as defined in the Agreement, and shall be subject to Customer's confidentiality obligations in the Agreement (*Section 5 - Confidentiality*). Where such audit, inspection or information request is for information over and above that referred to in **paragraph 9.2** and Voult is willing and able to accommodate the same then:

9.3.1 such audit, inspection or information request shall be reasonable, limited to information in Voult's possession or control and is subject to Customer giving Voult reasonable (and in any event at least 60 (sixty) days') prior notice of such audit, inspection or information request;

9.3.2 the Parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which Customer or third-party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure Voult is not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this **paragraph 9.3**);

9.3.3 Customer shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of Voult (or any applicable Sub-Processor);

9.3.4 the duration of any audit or inspection shall be limited to 1 (one) Business Day;

9.3.5 all costs of such audit or inspection or responding to such information request shall be borne by Customer, unless and to the extent Voult is found to be in material breach of this DPA;

9.3.6 Customer's rights under this **paragraph 9.3** in connection with such audit, inspection or information request may only be exercised once in any consecutive 12 (twelve) month period, unless otherwise required by a Supervisory Authority;

9.3.7 Customer shall promptly (and in any event within 1 (one) Business Day) report to Voult any non-compliance identified by such the audit, inspection or release of information; and

9.3.8 Customer shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any Permitted Auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of Voult (or any applicable Sub-Processor) while conducting any such audit or inspection.

10. Breach notification

10.1 In respect of any Personal Data Breach, Voult shall, without undue delay (but no later than 72 (seventy-two) hours):

10.1.1 notify Customer of the Personal Data Breach; and

10.1.2 provide Customer with all relevant details of the Personal Data Breach.

10.2 In respect of its access to and use of the Services (via the Platform), Customer (via its Customer Account Manager) is responsible for giving, managing and maintaining its Authorised Users' access by setting up its Authorised User Accounts. Customer shall, without undue delay:

10.2.1 notify Voult of any known Personal Data Breach, or other fact matter or circumstance that prejudice(s) the security of any applicable tenancy(ies) which host the applicable Services/ Solutions in respect of any Authorised User Account; and

10.2.2 provide Voult with details of the same.

Customer agrees and acknowledges that to the extent strictly necessary, Voult may need to, and if so, shall notify: (i) other applicable customers of the same where it would impact their access to and use of the applicable tenancy(ies) which host the applicable Solutions used by them or their; and/or (ii) any applicable Sub-Processors. Voult shall make any such notification(s) on a solely anonymised basis. Customer hereby expressly consents to any such notification(s) being made by Voult, provided Customer is not and cannot be identified.

11. Deletion of Protected Data and copies

In accordance with section 9.4 (*Effect of Termination*) of the Agreement, or at the request of Customer, Voult (including its Sub-Processors) shall, at Customer's direction, return or destroy (i.e., render permanently unreadable and not reconstructable into a usable format in accordance with industry standards and applicable law) of the applicable Protected Data (including all copies). Without undue delay, Voult shall certify to Customer that it has so either returned or destroyed of all copies of such data, except to the extent that Voult is required to maintain a copy to comply with applicable law. In such case, Voult shall only Process the remaining Personal Data for the purpose of compliance with such applicable laws. Voult shall have no liability (howsoever arising, including in negligence) for any loss of data resulting from its deletion or destruction of any such Protected Data undertaken in accordance with the Agreement.

12. Compensation and claims

12.1 Subject to the applicable provisions of the Agreement, Voult shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with the Agreement:

12.1.1 only to the extent caused by the Processing of Protected Data under the Agreement and resulting from Voult's (including any Sub-Processor's) breach of the Agreement (including this DPA); and

12.1.2 in no circumstances, to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of the Agreement by

Customer, and/or otherwise to the extent caused by the negligent actions or omissions of Customer and/or any of its Authorised Users.

Notwithstanding the foregoing or anything to the contrary herein or in the Agreement and having regard **to paragraph 4.2**, Voult shall have no obligations or liabilities to Customer or any other person under this DPA or the Agreement in respect of any loss of, corruption to or unauthorised access given in respect of any Customer Data (including any Protected Data) where that loss or corruption or unauthorised access was caused by or the fault of or given by (whether intentionally or not) Customer and/or any of its Authorised Users, accessing and using the Services (via the Platform). For example, a particular Authorised User:

12.1.3 deleting Customer Data in a Solution;

12.1.4 incorrectly updating Customer Data in a Solution; or

12.1.5 being given incorrect permission as an Authorised User by the Customer Account Manager and in turn being given access to Protected Data to which he/she should not have access.

12.2 If a Party receives a compensation claim from a person relating to Processing of Protected Data in connection with the Agreement or Customer's access to and use of the Services (via the Platform), it shall promptly provide the other Party with notice and full details of such claim.

12.3 The Parties agree that Customer shall not be entitled to claim back from Voult any part of any compensation paid by Customer in respect of such damage to the extent that Customer is liable to indemnify or otherwise compensate Voult in accordance with the Agreement and/or to the extent Voult has no liability for the same under the Agreement.

12.4 This **paragraph 12** is intended to apply to the allocation of liability for Data Protection Losses as between the Parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

12.4.1 to the extent not permitted by applicable law (including Data Protection Laws); and

12.4.2 that it does not affect the liability of either party to any Data Subject.

13. <u>Noncompliance</u>.

13.1 Voult will regularly assess its compliance with this DPA and, if Voult can no longer meet its obligations under this DPA in any material respect, it will notify Customer in writing within ten (10) days. Following receipt of any such notice, Customer may take reasonable and appropriate steps to stop and remediate any unauthorised Processing of Protected Data by Voult, up to and including terminating the Agreement. Voult will use reasonable efforts to cooperate with Customer's reasonable requests regarding any unauthorised Processing of Protected Data. In the event Voult materially breaches any of its obligations under this DPA: (i) and fails to cure such material breach (if capable of cure) within thirty (30) days following receipt of written notice by Customer, Customer will have the right to terminate the Agreement; and/or (ii) suspend Voult's Processing of any Protected Data unless and until such material breach is cured.

13.2 Customer agrees and acknowledges that if it exercises its right to immediately suspend Voult's continued Processing of Protected Data then, for all practicable purposes, Voult would need to suspend Customer's (and all of its Authorised Users') access to and use of the Services, the Solution(s) in question and limit all other Processing to the greatest extent possible, without deleting or damaging the Protected Data (e.g., suspending any applicable transactions, transfers, account access). While limited, Voult would still be providing the Hosting Services and the Database Services during such period of suspension which is Processing. Customer hereby agrees to such Processing by Voult during such period of suspension. Customer also agrees and acknowledges that Voult would not be in breach of the Agreement for failing to provide access to and use of the Services, the Solution(s) in question or the provision of the Standard Support Services during such period of suspension. For the purposes of section 1.3 (*Suspension*) of the Agreement, where Customer exercises its right to immediately suspend Voult's continued Processing of Protected Data, Voult will be permitted, without further penalty, to suspend Customer's (and in all of its Authorised Users') access to and use of the Services, the Solution(s) in question without having to provide notice to Customer of such suspension and will only have to reinstate such access and use if and when Customer ends such period of suspension. Nothing in the previous sentence shall absolve Voult's liability under this DPA for the applicable breach of this DPA giving rise to Customer exercising its right to immediately suspend Voult's processing of Protected Data.

14. Survival

This DPA shall survive termination (for any reason) or expiry of the Agreement with Customer and continue until no Protected Data in relation to Customer remains in the possession or control of Voult or any Sub-Processor, except that **paragraphs 11** to **13** (inclusive) shall continue indefinitely.

15. Data protection contact

Voult's '*Data Protection Officer*' may be contacted at pivacy@voult.com.

ANNEX A

Subject-matter of Processing:

Customer's access to and use of the Services/ applicable Solution(s) (via the Platform) including particular:

- The Hosting Services; and
- The Database Services.

Duration of the Processing:

The date of termination of the Agreement.

Frequency of the transfer:

Continuous basis depending on Customer's access to and use of the Services/ applicable Solution(s) (via the Platform).

Nature and purpose of the Processing:

The Processing of Protected Data by Voult under the Agreement shall be for the following purposes (such purposes being Processing Instructions given to Voult by Customer):

- Processing in accordance with the rights and obligations of the Parties under the Agreement;
- Processing to provide Customer's access to and use of the Services/ applicable Solution(s) (via the Platform) (including the Hosting/ Data Storage Arrangements);
- Processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement; and
- Processing as reasonably initiated, requested or instructed by:
    - Customer's Authorised Users in connection with their use of Customer's; and/or
    - Customer in connection with its,

  access to and use of the Services/ applicable Solution(s) (via the Platform) in each case in a manner consistent with the Agreement.

Type of Personal Data:

Customer may upload, submit, enter and/or otherwise Process (itself and/or via its Customer Account Manager and/or its Authorised Users) Protected Data as part of/ during Customer's access to and use of the Services/ applicable Solution(s) (via the Platform), the extent of which is controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects in relation to Customer (where the same are natural persons):

- Customer Account Manager;
- Authorised Users;
- Prospects, customers, clients, suppliers, contractors, subcontractors, consultants, freelancers, brokers, other service providers, agents, distributors, referrers, introducers and/or business partners of or to Customer and/or any of its Affiliates;
- Members, shareholders and/or partners of Customer and/or any of its Affiliates;
- Investors, lenders, funders, financiers, creditors, security or collateral providers, guarantors and/or sureties of or to Customer and/or any of its Affiliates;
- Advisors, professional advisors, other professional service providers, insurers;
- Employees, directors, officers and/or workers of any of the foregoing;
- Employees, directors, officers and/or workers of Customer and/or any of its Affiliates; and/or
- (in respect of a Solution) those other categories of Data Subjects identified in the applicable Solutions Terms.

Categories of Personal Data:

Customer may upload, submit, enter and/or otherwise Process (itself and/or via its Customer Account Manager and/or its Authorised Users) Protected Data as part of/ during Customer's access to and use of the Services/

applicable Solution(s) (via the Platform), the extent of which is controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First, last and any middle names
- Title
- Position
- Employer
- Contact information (company, email, phone, address)
- ID data
- Professional data
- Authorisation level data
- Localisation data
- (in respect of a Solution) those other categories of Personal Data identified in the applicable Solutions Terms.

Special or Sensitive categories of Personal Data:

Customer may input, upload, submit, enter and/or otherwise Process (itself and/or via its Customer Account Manager and/or its Authorised Users) "Special" categories (within the meaning of Article 9 of the GDPR) or "Sensitive" categories (as defined under applicable Data Protection Laws) of Protected Data as part of Customer's access to and use of the Services/ applicable Solution(s) (via the Platform), the extent of which is controlled by Customer in its sole discretion, and which is, for the sake of clarity, Personal Data revealing racial or ethnic origin; national origin; political opinions, religious or philosophical beliefs; or trade-union membership; citizenship or immigration status; Personal Data which is or contains genetic data or biometric data; precise geolocation; government identification card or number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials; contents of a consumer's mail, email, and text messages unless the business is the intended recipient; neural data; children under 13 years old; status of victim of a crime; data concerning health or data concerning a natural person's sex life or sexual orientation or status as transgender or nonbinary.

Restrictions and Safeguards for Special or Sensitive Categories of Data: Subject to the following paragraph entitled '***Restrictions and Safeguards for Special or Sensitive Categories of Data – Services***', if Voult will Process Special or Sensitive categories of Personal Data, as indicated above, please identify any restrictions or safeguards applicable to such data that take into consideration the nature of the data and the risks involved. Please check all that apply and supplement with additional restrictions or safeguards as necessary.

X Strict purpose limitation

X Access restrictions (including access only for staff having followed specialised training)

X Keeping a record of access to the data

X Restrictions for onward transfers

☐ Other (please specify)

Restrictions and Safeguards for Special or Sensitive Categories of Data – Services: If Voult will Process Special or Sensitive categories of Personal Data in providing access to and use of the Services (via the Platform) to Customer, Voult applies the same security, restrictions and/or safeguards to all Customer Data (including all Protected Data whether or not it includes Special or Sensitive categories of Personal Data as indicated above) – see the **Information Security Exhibit (Annex B)**.

Standard Contractual Clauses Elections: The Parties agree to elect the following options:

- For Clause 7 of the Standard Contractual Clauses, the parties elect to include the optional language.
- For Clause 9(a) of the Standard Contractual Clauses, the parties elect to include the language in Option 1 with 30 days as the specified time period.
- For Clause 11(a) of the Standard Contractual Clauses, the parties elect not to include the optional language.

Competent Supervisory Authority for the Standard Contractual Clauses: The Parties agree that, with respect to the European Economic Area, the Supervisory Authority of the Republic of Ireland, the Data Protection Commission, will act as the competent Supervisory Authority.

Governing Law for Standard Contractual Clauses: For purposes of Clause 17 of the Standard Contractual Clauses, with respect to the European Economic Area, the Parties agree that the law of the Republic of Ireland will be the governing law.

Choice of Forum and Jurisdiction for Standard Contractual Clauses: For purposes of Clause 18 of the Standard Contractual Clauses, with respect to the European Economic Area, the Parties agree that the courts of the Republic of Ireland will resolve any dispute arising from the Standard Contractual Clauses.

Description of Technical and Organisational Measures: The technical and organisational measures implemented by Voult (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons are described in the Information Security Exhibit.

For transfers to Sub-Processors, the specific technical and organisational measures to be taken by the Sub-Processors to be able to provide assistance to Customer and, for transfers from a Processor to a Sub-Processor, to the data exporter, are described in this DPA.

The specific technical and organisational measures Voult will take to assist Customer in fulfilling its obligations to respond to Data Subjects' Requests to exercise their rights under applicable Data Protection Laws are described in this DPA.

Table 4 of the UK Addendum: Which Party can terminate this DPA if the UK Data Protection Authority Changes this "Approved Addendum"

Ending This DPA When the Approved Addendum Changes	Which Parties may end this DPA as set out in Section 19 of the UK Addendum: ☐ Data Importer ✓ Data Exporter ☐ Neither Party

ANNEX B

Information Security Exhibit

1. **Access Controls**. Where access to Customer Data by Voult is authorised, Voult will abide by the '*principle of least privilege*' and permit access to Customer Data by its personnel solely on a need-to-know basis. Voult will promptly terminate its personnel's access within twenty-four (24) hours to such data when access is no longer required to provide the services under the Agreement. This **paragraph 1** does not apply to access given to Voult (or any of its personnel) via an Authorised User Account created by Customer in respect of an applicable tenancy which hosts the applicable Services/ Solutions in question.

2. **Account Management**. Voult will use reasonable measures to manage the creation, use, and deletion of all account credentials used to access Voult's Systems, including where applicable by implementing: (i) a segregated account with unique credentials for each user; (ii) strict management of administrative accounts; (iii) password best practices, including the use of strong passwords and secure password storage; and (iv) periodic audits of accounts and credentials. This **paragraph 2** does not apply to Customer giving access to an Authorised User and setting up an Authorised User Account for that Authorised User in respect of an applicable tenancy which hosts the applicable Services/ Solutions in question.

3. **Vulnerability Management**. Voult will: (i) use automated vulnerability scanning tools to scan Voult's Systems; (ii) log vulnerability scan reports; (iii) conduct periodic reviews of vulnerability scan reports over time; (iv) use patch management and software update tools for Voult's Systems; (v) prioritise and remediate vulnerabilities by risk; and (vi) use compensating controls if no patch or remediation is immediately available.

4. **Security Segmentation**. Voult will monitor, detect, and restrict the flow of information on a multilayered basis within Voult's Systems using tools such as firewalls, proxies, and network-based intrusion detection systems.

5. **Data Loss Prevention**. Subject to **paragraph 6**, Voult will use reasonable data loss prevention measures to identify, monitor, and protect Customer Data in use, in transit, and at rest. Such data loss prevention processes and tools will include: (i) automated tools to identify attempts of data exfiltration; (ii) the prohibition of, or secure and managed use of, portable devices; and (iii) use of certificate-based security.

6. **Data Loss Prevention – Services**. Unless and to the extent provided for to the contrary in any Solution Terms for a particular Solution, Voult does not as part of the Services or any Solution(s) (via the Platform) use data loss prevention measures to identify, monitor, and protect Customer Data in use, in transit, and at rest.

7. **Encryption**. Voult will encrypt, using industry standard encryption tools, all Customer Data that Voult: (i) transmits or sends wirelessly or across public networks or within Voult's Systems; (ii) stores on laptops or storage media, and (iii) stores on portable devices or within Voult's Systems. Voult will comply with secure key management policies and procedures and safeguard the security and confidentiality of all encryption keys associated with encrypted Customer Data.

8. **Secure Software Development**. Voult represents and warrants that any software used in connection with the Processing of Customer Data by or on behalf of Voult is or has been developed using secure software development practices, including by: (i) segregating development and production environments; (ii) filtering out potentially malicious character sequences in user inputs; (iii) using secure communication techniques, including encryption; (iv) using sound memory management practices; (v) using web application firewalls to address common web application attacks such as cross-site scripting, SQL injection and command injection; (vi) implementing the OWASP Top Ten recommendations, as applicable; (vii) patching of software; (viii) testing object code and source code for common coding errors and vulnerabilities using code analysis tools; (ix) testing of web applications for vulnerabilities using web application scanners; and (x) testing software for performance under denial of service and other resource exhaustion attacks. This **paragraph 8** does not apply to any application built on and using the Platform other than those Solution(s) which are Purchased Items of the Customer in question. In relation to any Open Source Software used, whilst Voult validates the output of the same as used by Voult it makes no representation or warranty as to the development process(es) used to deliver such output.

9. **Physical Safeguards**. Voult will maintain physical access controls where applicable that secure relevant Voult Systems used to Process any Customer Data, including an access control system that enables Voult to monitor and control physical access to each Voult facility, which includes without limitation 24/7 physical security monitoring systems and the use of trained and experienced security guards.

10. **Administrative Safeguards**. In any instance where Voult provides access to Customer Data to any of its personnel, Voult will: (i) ensure the reliability of such personnel, including by performing background screening (to the extent permitted by applicable law); and (ii) provide appropriate security training to such personnel to ensure such personnel can comply with the obligations under this Exhibit. Voult will

periodically provide additional training to its personnel as may be appropriate to help ensure that Voult's information security program meets or exceeds prevailing industry standards and complies with applicable Data Protection Laws.

11. **Organisational Safeguards**. Voult will maintain and comply with internal policies to: (i) limit the retention of Customer Data to the minimum amount of time necessary to perform Voult's obligations under the Agreement; and (ii) provide for meaningful consequences to its personnel who breach the obligations set forth in this Exhibit.

12. **Business Continuity and Disaster Recovery**. Voult will provide appropriate continuity and recovery plans to ensure (i) Voult can restore availability and access to Customer Data as soon as possible in the event of an applicable incident and (ii) continued service in an event that impacts Voult's datacenters or offices providing the contracted services, and to the extent applicable, in accordance with any service level agreements. Such plans must be tested at least annually.

13. **Incident Response Plan**. Voult will maintain a documented incident response plan that addresses detection, reporting, evidence management, post-incident restoration and incorporation of lessons learned, with respect to any potential Personal Data Breach. The plan must be tested at least annually.