Last revised: 11 August 2026.

By executing an Order Form or creating a profile or account through the Services, or otherwise using the Services or Materials, you confirm your agreement to abide by and be bound by the terms set out below (the "**Terms of Service**"). You may not use the Services or Materials unless you agree to the Terms of Service.

1. **Interpretation**

1.1 In this Agreement:

(a) "**Affiliate**" means, in relation to a party, any entity that directly or indirectly controls, is controlled by or is under common control with that party from time to time;

(b) "**Agreement**" means these Terms of Service together with the Order Form (if any);

(c) "**Analytics**" has the meaning given to it in Clause 5.4(a) (*Ownership and use of Intellectual Property*);

(d) "**Authorised User**" means any employee, agent, contractor or representative of the Organisation authorised by it to access and use the Services, using their own unique identifier provided by Risk Ledger;

(e) "**Business Days**" means any day other than a Saturday or Sunday or public holiday in England on which banks are physically open for the transaction of general banking business in London or, where Risk Ledger Inc. is the contracting entity, any day (other than a Saturday, Sunday or US federal holiday) on which banks in Chicago, Illinois are physically open for the transaction of general banking business;

(f) "**Charges**" means Risk Ledger's fees for the Services, as stated in the Order Form, together with such other additional fees as may be charged in accordance with this Agreement or otherwise agreed between the parties from time to time;

(g) "**Confidential Information**" means information that is proprietary or confidential to a party and is disclosed or made available by it to the other party in connection with this Agreement, as this definition is supplemented by Clause 6 (*Confidential Information*);

(h) "**Contract Year**" means the 12-month period following the Effective Date and each succeeding 12-month period;

(i) "**Documentation**" means Risk Ledger's technical and functional documentation for the relevant Services including (where applicable) as referred to in the Order Form or otherwise made available to you by us from time to time;

(j) "**Effective Date**" means the earlier of the date specified as such on the Order Form (if any) and the date on which you start using the Services;

(k) "**Federated Principal**" means a person that has procured access to the Services for itself and/or for the benefit of one or more Federated Sub-organisations;

(l) "**Federated Sub-organisation**" means a person designated by a Federated Principal as able to use the Services within the limits set out in the Federated Principal's Order Form;

(m) "**Initial Term**" means the period stated as the initial term on the Order Form (if any) and otherwise shall not apply;

(n) "**Intellectual Property**" means any and all patents, copyrights (including future copyrights), design rights, trade marks, service marks, domain names, trade secrets, know-how, database rights, and all other intellectual property rights, whether registered or unregistered, and including applications for any of the foregoing and all rights of a similar nature which may exist anywhere in the world;

(o) "**Materials**" means written documentation and content, verbal, electronic and other information, data and databases, computer software, designs, drawings, pictures or other images (whether still or moving), the Site, sounds or any other record of any information in any form belonging or licensed to Risk Ledger but for the avoidance of doubt not including any Organisation Data or Participant Data;

(p) "**Order Form**" means an ordering document or online order specifying the Services to be provided, that is entered into between you or your Federated Principal (if applicable) and Risk Ledger;

(q) "**Organisation**", "**you**" or "**your**" means the person or entity submitting the Order Form or applying for or creating a profile or account (or, if different, on whose behalf such an Order Form is submitted or the profile or account is requested) to use the Services;

(r) "**Organisation Data**" means any information, data or other materials supplied or made available by you or your Authorised Users to or through or in connection with the Services;

(s) "**Participant**" means any person permitted by Risk Ledger to use its software and services, other than the Organisation and its Authorised Users;

(t) "**Participant Data**" means any information or data shared with or accessible to the Organisation via the Services and relating to or provided by one or more identifiable Participants;

(u) "**Renewal Term**" has the meaning given to it in Clause 12.1(a) (*Term, suspension and termination*);

(v) "**Risk Ledger**" or "**us**" or "**our**" means the Risk Ledger entity determined in accordance with Clause 18 (*Contracting entity, governing law and dispute resolution*);

(w) "**Scheduled Maintenance**" means any work notified to you (including, without limitation, by publishing a notice through the Services or on the Site) that may cause the Services to be temporarily suspended or disrupted;

(x) "**Services**" means those services as set out in the Order Form (if any) or otherwise provided by us from time to time through https://app.riskledger.com and/or any other endpoint we may make available from time to time;

(y) "**Site**" means Risk Ledger's website at https://riskledger.com, its user platform at https://app.riskledger.com, or other websites or endpoints operated by Risk Ledger;

(z) "**SLA**" means Appendix 1 (*Service level agreement*) to these Terms of Service, which defines the service levels to be provided by Risk Ledger under this Agreement;

(aa) "**VAT**" means value added tax chargeable under English law and any similar additional tax, and any similar tax levied in any jurisdiction, including United States sales and use taxes; and

(bb) "**Working Hours**" means 9am to 5pm UK time on Business Days.

1.2 Any reference in these terms to "writing" or related expressions includes email and written notices or communications from Risk Ledger via the Services or on the Site.

1.3 Except where the context requires otherwise:

(a) the singular includes the plural and vice versa; a reference to one gender includes all genders; words denoting persons include a natural person, corporate or unincorporated body (whether or not having separate legal personality); a reference to a "company" includes any company, corporation or other body corporate, wherever and however incorporated or established; and a reference to a "party" includes that party's personal representatives, successors and permitted assigns; and

(b) any words that follow "include", "includes", "including", "in particular" or any similar words and expressions shall be construed as illustrative only and shall not limit the sense of any word, phrase, term, definition or description preceding those words.

1.4 Any reference to an English legal term for any action, remedy, method of judicial proceeding, legal document, legal status, court, official or any legal concept or thing shall, in respect of any jurisdiction other than England, be deemed to include a reference to what most nearly approximates in that jurisdiction to the English legal term.

1.5 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time. A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

2. **Use of the Services**

2.1 Subject to your payment of any applicable Charges and your compliance with the terms of this Agreement, Risk Ledger:

(a) shall use its reasonable efforts to provide you with access to the Services; and

(b) grants you a limited, personal, non-exclusive, non-sublicensable and non-transferable (save in accordance with Clause 14.2 (*Transfer and subcontracting*)) licence to use Materials made available to you through the Services as reasonably necessary for you to make full use of the Services, solely for your internal risk management, security assurance and compliance purposes,

for the duration of this Agreement, strictly in accordance with its terms. You shall not be entitled to use the Services or the Materials for any other purpose. In particular, and without limitation, you shall have no right to copy, translate, reproduce, adapt, reverse engineer, decompile, disassemble, or create derivative works of the Services, Materials or any part of them except as required by applicable law. Further, you shall have no right to sell, rent, lease, transfer, assign or sublicense the Services, the Materials or rights under this Agreement (other than in accordance with Clause 14.2 (*Transfer and subcontracting*)) without Risk Ledger's prior written consent.

2.2 Your usage of the Services is subject to any limits outlined on the Order Form (if any) or as otherwise indicated to you by Risk Ledger in writing. If your use exceeds those limits, Risk Ledger may (in its discretion and subject to any fair usage policy operated by Risk Ledger from time to time), either:

(a) invoice you for your usage in excess of the relevant limits at or below the same marginal per-unit rate (with Federated Principals having primary responsibility for overages incurred by Federated Sub-organisations, save for where the overage relates to an Order Form entered into directly by that Federated Sub-organisation); or

(b) suspend or terminate this Agreement if you do not restore your usage below the agreed levels within 14 days of a written request from Risk Ledger to do so.

2.3 Where the Site or Services contain resources provided by third parties and links to other sites, these are provided for information only on an "as is" and "as available" basis. Risk Ledger has no control over the availability or content of such resources or sites and has no responsibility or liability for them or for any loss or damage that may arise from your use of them.

2.4 Risk Ledger is always finding ways to improve the Services and add features. The Organisation agrees that Risk Ledger may change the Services from time to time, provided that any such changes do not fundamentally alter the nature of the Services.

2.5 The Charges stated in an Order Form will only cover the Services described in the Order Form and, unless the Order Form provides otherwise, stated on an annual basis. Risk Ledger and the Organisation will agree pricing for any additional chargeable services provided by Risk Ledger through one or more separate Order Forms as necessary.

2.6 Where the Organisation is a Federated Sub-organisation, the Organisation authorises Risk Ledger to treat instructions given, and settings or configurations applied, by the Organisation's Federated Principal as given or applied by the Organisation.

3. **Charges and payment**

3.1 The Organisation shall pay the Charges (if any) for the Services in accordance with this Agreement. Payment shall be made in the currency indicated on the Order Form or, if not specified, GBP or, where Risk Ledger Inc. is the contracting entity, USD.

3.2 All Charges quoted to the Organisation for the provision of the Services are exclusive of any VAT.

3.3 If the Organisation requires a purchase order number on invoices, it shall provide a purchase order number on the Order Form or as soon as reasonably practicable following the date the Order Form (or other Charges) are agreed. If the Organisation does not provide a purchase order number as required under this clause, the Organisation shall pay any related invoices without a purchase order number and may not withhold or delay payment of an invoice due to the absence of, or the Organisation's delay in providing, a purchase order number. Any terms stated by the Organisation on or otherwise to be applicable to a purchase order shall not apply to the Services or the Agreement.

3.4 Risk Ledger will invoice the Charges (if any) to the Organisation in advance on an annual basis for payment within 30 days of the date of receipt of any such invoice, unless expressly stated otherwise on the Order Form or extended on the invoice. Sums shall be paid in full without set off or deduction. Risk Ledger's first provision of the Services is subject to its receipt of payment for the first Contract Year.

3.5 Without limiting Risk Ledger's ability to charge the Organisation for additional usage volumes under Clause 2.2 (*Use of the Services*), if the Initial Term is one year or less, the Charges will increase by 5% of the then current annual fee on the commencement of each Renewal Term without the need for notice or, if the Initial Term is more than one year, the Charges will increase by 5% of the then current annual fee at the commencement of each Contract Year of the Initial Term and on the commencement of each Renewal Term, without the need for notice. For any other increase or addition to the Charges (other than an increase in accordance with Clause 2.2 (*Use of the Services*)), Risk Ledger shall provide the

Organisation with at least 60 days' written notice prior to the start of the Renewal Term to which the increase or addition will apply.

3.6 No payment shall be deemed to have been made until Risk Ledger has received such payment in cleared funds from the Organisation.

3.7 If the Organisation fails to pay Risk Ledger any Charges by the due date then, without prejudice to its other rights and remedies, Risk Ledger shall be entitled to charge interest on the outstanding amount at the rate of 4% above the base rate of the Bank of England or, where Risk Ledger Inc. is the contracting entity, the lower of 4% above the prime rate published in the Wall Street Journal and the maximum rate permitted by applicable law, (whether before or after any judgment) accruing daily and compounded quarterly, from the later of due date for payment or 30 days from the Organisation's receipt of the invoice, until the outstanding amount is paid in full.

4. **Organisation's obligations**

4.1 The Organisation shall not, and shall ensure that its Authorised Users shall not:

(a) use the Services, Materials or Participant Data in any way so as to bring Risk Ledger or any other party into disrepute;

(b) use the Services, Materials or Participant Data in a manner which is unlawful, harmful, threatening, abusive, harassing, tortious, indecent, obscene, libellous or menacing;

(c) use the Services, Materials or Participant Data in a manner which infringes the Intellectual Property, proprietary or personal rights of any third party, including data subjects;

(d) misuse the Site or Materials by introducing viruses, trojans, worms, logic bombs, prompt injections or other material which is technologically harmful;

(e) attempt to gain unauthorised access to the Site, Materials or Services, the servers on which the Site, Materials or Services are stored, or any server, computer or database connected to the Site or Services;

(f) attack the Site, Materials or Services via a denial-of-service attack or a distributed or malicious denial-of-service attack;

(g) access the Site, Materials or Services in order to build a product or service which competes with the Site, Materials or Services; or

(h) use the Services, Materials, Organisation Data or Participant Data, or disclose them to third parties, except as authorised in writing by Risk Ledger or as permitted under this Agreement.

4.2 The Organisation shall keep its password and other access details for use with the Services confidential and restricted to those members of staff who need to know such details and shall ensure that all Authorised Users are aware of the confidential nature of such information and treat it accordingly. The Organisation shall notify Risk Ledger immediately if it believes that such information is no longer secret. The Organisation is solely responsible for all activities that occur using the Organisation's authentication credentials. The Organisation shall not permit any person to access the Services for any purpose that would constitute a breach of this Agreement if such a breach were carried out by the Organisation, and the Organisation remains responsible in full for any such unauthorised use.

4.3 The Organisation shall take all reasonable steps to ensure that nobody other than Authorised Users accesses the Services using Authorised User accounts. Authorised User accounts may

not be shared between individuals. Organisations may have up to the number of Authorised Users stated on the Order Form (or, if not so specified, up to 5). Organisations may be able to purchase additional Authorised User accounts from Risk Ledger upon request.

4.4 The Organisation warrants, undertakes and agrees that:

(a) the Organisation has all rights, licences and permissions necessary for Risk Ledger to provide the Services in accordance with this Agreement; and

(b) the Organisation shall provide Risk Ledger with all information, access and cooperation reasonably required for Risk Ledger to provide the Services.

5. **Ownership and use of Intellectual Property**

5.1 The Organisation acknowledges and Risk Ledger warrants that:

(a) Risk Ledger is as between the Organisation and Risk Ledger the proprietor or authorised licensee of the Intellectual Property in the Site, Services and Materials; and

(b) so far as Risk Ledger is aware, the Intellectual Property in the Site, Services and Materials, and their use as contemplated in this Agreement, do not infringe the Intellectual Property rights of any third party.

5.2 The Organisation grants to Risk Ledger in respect of the Organisation Data a worldwide, non-exclusive, royalty-free and sublicensable licence to host, use, distribute, modify, run, copy, display, translate and create derivative works for the purpose of operating the Services. Risk Ledger shall use this licence in a manner consistent with the Organisation's sharing and privacy settings configured via the Services. This licence shall terminate upon the deletion of the Organisation Data from our systems. Risk Ledger aims to delete Organisation Data from its systems within 90 days of an instruction to delete specific content or the termination of this Agreement, save for where:

(a) the Organisation Data has been sublicensed to Participants (e.g., through sharing via the Services) prior to termination or your deletion request and they have not deleted it;

(b) deletion within 90 days is not possible due to technical limitations of our systems, in which case we will effect the deletion as soon as technically feasible; or

(c) we are required by law to retain the Organisation Data and/or share it with others,

in which cases this licence shall continue to apply until that content has been fully deleted.

5.3 Risk Ledger may sublicense Participant Data to the Organisation in line with the instructions and settings of the contributing Participant(s). Any such sublicence is granted on a worldwide, non-exclusive basis for the limited purpose of enabling the Organisation to use, modify, copy, translate or create derivative works of the Participant Data to evaluate, query or respond to queries regarding practices and/or requirements relating to information security and/or third party risk management. This sublicence shall survive termination of this Agreement solely to the extent necessary for the Organisation's retention and internal use of records of its use of the Services, subject to Clause 6 (*Confidentiality*).

5.4 The Organisation agrees to Risk Ledger collecting via the Services, and grants to Risk Ledger a worldwide, non-exclusive, perpetual, irrevocable, royalty-free licence (with the right to sublicense) to use the following data for the corresponding uses:

(a) **Analytics** – Subject to the terms of this Agreement, Risk Ledger may analyse and process Organisation Data (including the contents of profiles, responses to questions

and interactions with other Participants and Participant Data via the Services) in order to distil behaviours, trends and patterns ("**Analytics**"), and the results and learnings of such Analytics. Risk Ledger uses these Analytics to improve the approach taken to risk assessments as part of the Services; to indicate potential areas for improvement of cybersecurity and third party risk management practices; to develop and improve the Services; and to produce anonymised, pseudonymised or aggregated statistical reports and research.

(b) **System usage** – Risk Ledger will use the number of Authorised Users, and data relating to the volume and categories of data or connections processed through the Services, to calculate and verify the Charges. Risk Ledger may analyse Authorised Users' login metadata (including IP address, concurrent logins, and similar indicators) for security purposes to monitor the Organisation's compliance with Clause 4.3 (*Organisation's obligations*).

5.5 The Organisation, on behalf of itself and its Authorised Users, assigns Risk Ledger all Intellectual Property rights in all suggestions or feedback given by any means to Risk Ledger in relation to the Site, Services and Materials.

5.6 If the Organisation becomes aware that any other person, firm or company alleges that the Intellectual Property in the Site, the Services and/or Materials is invalid or that use of such Intellectual Property infringes any Intellectual Property rights of another party, the Organisation shall as soon as reasonably possible give Risk Ledger full particulars in writing thereof and shall make no comment or admission to any third party in respect thereof.

5.7 Risk Ledger shall have the conduct of all proceedings relating to the Intellectual Property in the Site, the Services and/or Materials and shall in its sole discretion decide what action if any to take in respect of any matter arising under Clause 5.6 or any action to bring any claim of infringement of such Intellectual Property brought by a third party to an end. Such action may include: (i) procuring the rights to use that portion of the Services alleged to be infringing; (ii) replacing the alleged infringing portion of the Services with a non-infringing alternative; (iii) modifying the alleged infringing portion of the Services to make it non-infringing; or (iv) terminating the allegedly infringing portion of the Services or this Agreement (in which case, to the extent applicable, Risk Ledger shall either ensure that such actions do not materially adversely affect the functional capabilities of the Services, or may refund to the Organisation a proportion of any Charges paid in advance in respect of parts of the Service which the Organisation is no longer able to use).

5.8 The Organisation shall reasonably assist Risk Ledger upon Risk Ledger's reasonable request in any proceedings brought or threatened by or against Risk Ledger. Risk Ledger agrees to reimburse the Organisation's reasonable expenses incurred in complying with this Clause 5.8 provided that they are agreed in advance with Risk Ledger.

6. Confidentiality

6.1 Each party may be given access to Confidential Information from the other party in order to perform its obligations under this Agreement. A party's Confidential Information shall not include information that:

(a) is or becomes publicly known (other than through any act or omission of the receiving party in breach of this Agreement);

(b) was in the other party's lawful, non-confidential possession before the disclosure;

(c) is lawfully disclosed to the receiving party by a third party on a non-confidential basis, without breach of applicable restrictions on disclosure;

(d) is independently developed by the receiving party, which independent development can be shown by written evidence; or

(e) is required to be disclosed by law, any court of competent jurisdiction or by any regulatory or administrative body and the terms of such compelled disclosure do not provide for confidential treatment of the disclosed materials.

6.2 Each party shall hold the other's Confidential Information in confidence and, unless required by law, not make the other's Confidential Information available to any third party, or use the other's Confidential Information for any purpose other than the implementation of this Agreement.

6.3 Each party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its personnel in violation of the terms of this Agreement.

6.4 The Organisation acknowledges that the Materials constitute Risk Ledger's Confidential Information.

6.5 In connection with the provision of the Services, Organisation Data may be used and shared:

(a) as necessary to provide the Services in accordance with the Documentation;

(b) as indicated through the Services when the Organisation or its Authorised Users create or update Organisation Data, make or accept connections, or otherwise interact with Participants via the Services;

(c) in accordance with settings configured or choices made by the Organisation and its Authorised Users through the Services; and

(d) as otherwise specifically detailed in the Agreement.

6.6 As part of the Services, the Organisation may receive Participant Data. The Organisation undertakes to Risk Ledger that it and its Authorised Users will treat all Participant Data as Confidential Information and will not use Participant Data for any reason other than to evaluate, query or respond to queries regarding practices and/or requirements relating to information security and/or third party risk management.

6.7 The Organisation consents to Participants (including, where relevant, a Federated Principal and Federated Sub-organisations participating in a federated arrangement with a Participant) receiving and using, on substantially the same basis as the Organisation may receive and use Participant Data under Clause 6.6 and in line with the Documentation and the Organisation's settings configured via the Services, Organisation Data.

6.8 No party shall use the other party's trade marks or make any public announcement concerning this Agreement, without the prior written consent of the other party. Risk Ledger may use the Organisation's name and logo for the limited purpose of identifying the Organisation as a customer of Risk Ledger.

6.9 This Clause 6 shall remain in force in perpetuity unless agreed otherwise in writing between the parties.

7. **Data protection**

Appendix 2 applies in respect of personal data processed in the performance of this Agreement.

8. **Warranties**

8.1 Each party shall comply with all laws and regulations applicable to it in connection with:

(a) in the case of Risk Ledger, the operation of Risk Ledger's business as it relates to the Services; and

(b) in the case of the Organisation, the Organisation Data and the Organisation's use of the Services.

8.2 Risk Ledger warrants that it will:

(a) provide the Services with reasonable skill and care and in substantial conformance with the Documentation; and

(b) use commercially reasonable efforts to maintain the availability of the Services set out in the SLA, and to provide reasonable notice in advance of any Scheduled Maintenance.

9. **Indemnities**

9.1 Where the Organisation receives Services under an Order Form, and subject to Clauses 5.6-5.8 (*Ownership and use of Intellectual Property*) (and the Organisation complying with its obligations therein), Risk Ledger will defend the Organisation against any third party claim that the Organisation's use of the Services or Materials as permitted by this Agreement infringes a third party's Intellectual Property rights ("**Infringement Claim**"), and will indemnify the Organisation against the amount of any adverse final judgment or settlement relating to use in such period. Risk Ledger shall not be liable under this indemnity for any claim to the extent it arises from the Organisation's (i) breach of this Agreement, (ii) use of Organisation Data or Participant Data, or (iii) use of the Services or Materials with systems, data or materials not supplied or approved in writing by Risk Ledger. Risk Ledger's indemnification obligations set out in this Clause 9.1, and any action taken by Risk Ledger pursuant to Clause 5.7 (*Ownership and use of Intellectual Property*), shall be the Organisation's sole and exclusive remedy in respect of an Infringement Claim.

9.2 The Organisation shall indemnify Risk Ledger against any liabilities, costs, expenses, damages and losses (including reasonable legal fees, settlements and judgments) incurred by Risk Ledger in connection with all third party claims that relate to (i) the Organisation's breach of Clauses 4.1(a), 4.1(b), 4.1(c) and/or 4.1(h) (*Organisation's obligations*) or Clause 6 (*Confidentiality*) of this Agreement, or (ii) Organisation Data.

10. **Disclaimer and limitation of liability**

10.1 Nothing in this Agreement limits or excludes the liability of either party:

(a) for death or personal injury caused by negligence;

(b) for the Organisation's payment obligations;

(c) for its obligations under Clause 9 (*Indemnities*);

(d) for fraud or fraudulent misrepresentation; or

(e) for any other liability that cannot be limited or excluded under applicable law.

10.2 The Organisation acknowledges that it is solely responsible for verifying the Materials and Participant Data it receives and for ensuring that it manages its own risks appropriately and

in accordance with applicable laws and codes of practice. Except as expressly and specifically provided in this Agreement:

(a) the Organisation assumes sole responsibility for results obtained from the use of the Services, the Site, the Materials or any part of them, and for conclusions drawn from such use. Risk Ledger shall, subject to Clause 10.1, have no liability for damage caused by errors or omissions in any information, instructions or scripts shared using the Services, or any actions taken by Risk Ledger at the Organisation's direction; and

(b) the Services are provided on an "as-is" and "as-available" basis and all warranties, representations, conditions and all other terms of any kinds whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this Agreement.

10.3 Without limiting the effect of Clause 10.2(b), Risk Ledger does not warrant that:

(a) the supply of Participant Data, Materials and the Services will be free from interruption;

(b) any Materials and Participant Data is accurate, up to date, complete, reliable, useful, fit for purpose or timely; or

(c) using the Services and Materials will meet any statutory obligations of the Organisation.

10.4 Subject to Clause 10.1 and Clause 10.2:

(a) neither party shall be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation (whether innocent or negligent), restitution or otherwise for any (i) loss of profits, business, business opportunities, revenue, turnover, reputation or goodwill; (ii) loss or corruption of data or information; (iii) loss of anticipated savings or wasted expenditure; or (iv) indirect, incidental, consequential, exemplary, punitive or special damages; and

(b) each party's total liability under or in connection with this Agreement, whether in contract, tort (including negligence), misrepresentation, restitution, under statute or otherwise, in respect of any and all events arising in a Contract Year, that first give rise to a claim, shall in no event exceed the higher of (i) £100 or (ii) the total Charges paid or payable by the Organisation to Risk Ledger under this Agreement for that Contract Year.

11. **Force majeure**

11.1 Neither party shall be in breach of this Agreement or liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure results from events, circumstances or causes beyond its reasonable control. In such circumstances, the affected party shall be entitled to a reasonable extension of the time for performing such obligations. If the period of delay or non-performance continues for 30 days or more, either party may terminate this Agreement by giving 7 days' written notice to the other party. Notwithstanding the foregoing, this clause shall not affect the Organisation's payment obligations under Clause 3 (*Charges and payment*).

12. **Term, suspension and termination**

12.1 This Agreement shall commence on the Effective Date and shall continue as follows, unless terminated earlier in accordance with this Clause 12:

(a) Where this Agreement includes an Initial Term, the Agreement shall continue for the Initial Term and shall automatically extend for a further 12-month period ("**Renewal Term**") at the end of the Initial Term and at the end of each Renewal Term. Either

party may give written notice to the other party, not later than 30 days before the end of the Initial Term or the relevant Renewal Term, to terminate this Agreement.

(b) If no Initial Term applies, this Agreement shall continue until it is terminated by either party giving written notice to the other party to terminate this Agreement on the date stated in such notice.

12.2 Where an Order Form states that the Initial Term shall be a free trial, either party may terminate this Agreement at any time during the Initial Term by giving the other party not less than 7 days' written notice. If the free trial is not so terminated, the Agreement shall automatically extend for its first Renewal Term as stated in Clause 12.1(a).

12.3 Risk Ledger may (in its discretion) terminate this Agreement or suspend the right of the Organisation or any of its Authorised Users to access or use any portion or all of the Services immediately if:

(a) the use of the Services by the Organisation or any of its Authorised Users:

(i) poses a security risk to the Services or any third party;

(ii) could adversely impact Risk Ledger's systems, the Services or the systems or content of a Participant;

(iii) could subject Risk Ledger, its Affiliates, or any third party to liability; or

(iv) could be fraudulent,

and in each case Risk Ledger shall provide such notice of termination or suspension as it is able to do so in the circumstances;

(b) the Organisation or any of its Authorised Users are in breach of this Agreement and (if capable of remedy) the Organisation fails to remedy the breach within 14 days after being required by written notice to do so.

12.4 Either party may terminate this Agreement immediately by giving written notice to the other party if:

(a) the other party commits any material breach of this Agreement and (if capable of remedy) fails to remedy the breach within 14 days after being required by written notice to do so; or

(b) the other party becomes insolvent or bankrupt, enters into an arrangement with creditors, has a receiver or administrator appointed or its directors or shareholders pass a resolution to suspend trading, wind up or dissolve that party other than for the purposes of amalgamation or reconstruction, or it ceases or threatens to cease trading.

12.5 Any termination of this Agreement for any reason shall be without prejudice to any other rights or remedies a party may be entitled to at law or under this Agreement and shall not affect any accrued rights or liabilities of either party nor the coming into force or the continuance in force of any provision of this Agreement which is expressly or by implication intended to come into or continue in force on or after such termination.

12.6 The period during which Risk Ledger may suspend the Services in accordance with this Agreement will continue until the circumstances giving rise to Risk Ledger's right to suspend the Services ceases to subsist or until this Agreement is terminated.

12.7 In the event that Risk Ledger suspends the provision of Services as permitted by Clause 2.2(b) or Clause 12.3 (up to the duration permitted by Clause 12.6), the Organisation shall continue to be obliged to pay any Charges owing or that arise during the period when the

Services are suspended. Risk Ledger shall end the suspension as soon as reasonably practicable once the cause of the suspension is rectified.

12.8 Risk Ledger reserves the right to terminate this Agreement with immediate effect if, in its reasonable opinion:

(a) the Organisation has built or is building a product or service which compete with the Site or Services; or

(b) the Organisation is using the Services in a manner which seeks to circumvent any contractual usage restrictions or in a manner which is not permitted in accordance with this Agreement.

13. **Effects of termination**

13.1 Upon termination of this Agreement for any reason:

(a) there shall be no refund of any element of the Charges to the Organisation, save for refunds pro-rata where the Organisation has terminated properly under Clause 12.4 (*Term, suspension & termination*) or where Risk Ledger has terminated under Clause 5.7 (*Ownership and use of Intellectual Property*);

(b) all unpaid Charges shall become immediately due to Risk Ledger (in whole or in part on a pro rata basis where part of a periodic charge which is charged in arrears is due), save in instances where the Organisation has terminated properly under Clause 12.4 (*Term, suspension & termination*) or where Risk Ledger has terminated under Clause 5.7 (*Ownership and use of Intellectual Property*), in which case only the Charges due in relation to the period and usage prior to the effective date of termination shall become payable under this subclause;

(c) save as contemplated in Clause 13.1(f), Risk Ledger shall be under no obligation to retain any data (including Organisation Data);

(d) the Organisation shall immediately cease using Risk Ledger's Intellectual Property and the Materials;

(e) the licences granted to the Organisation under this Agreement shall immediately terminate, save to the extent expressly stated in this Agreement to survive termination; and

(f) subject to Clause 13.1(g), each party shall return or destroy (or erase from its computer systems) as notified to it in writing by the other party and make no further use of the data, the Materials (in the case of the Organisation) or any Confidential Information then in its possession, with the exception that each party shall be entitled to retain such Confidential Information then in its possession for legal purposes, the surviving licence(s) granted under Clauses 5.2, 5.3 and 5.4 (*Ownership and use of Intellectual Property*), and as contemplated in paragraph 10 of Appendix 2, subject to ongoing compliance with Clause 6 (*Confidentiality*) and Appendix 2; and

(g) upon the Organisation's request, Risk Ledger will retain Organisation Data for up to 30 days and provide a copy of the Organisation Data to the Organisation subject to payment of reasonable fees incurred in providing such access.

14. **Transfer and subcontracting**

14.1 Risk Ledger may assign, transfer or deal in any other manner with all or any of its rights under this Agreement or any part thereof to a third party. Risk Ledger may subcontract the Services or parts of them to third parties provided that the terms of agreements with

subcontractor are consistent with the terms of this Agreement. Risk Ledger is responsible for breaches of this Agreement caused by its subcontractors. Risk Ledger may exercise its rights and perform its obligations under this Agreement through one or more of its Affiliates (where Risk Ledger Inc. is the contracting entity, the Services are operated by its Affiliate Risk Ledger Ltd.), and the licences and consents granted to Risk Ledger under this Agreement extend to its Affiliates to the extent necessary for the operation and provision of the Services. Risk Ledger remains responsible for the acts and omissions of its Affiliates in connection with this Agreement as if they were its own.

14.2 Save as permitted by Clause 14.1, neither party may assign, subcontract, sublicense or otherwise transfer any rights or obligations under this Agreement or any part thereof (except in connection with the sale or transfer of all, or substantially the whole, of its assets) without the prior consent in writing of the other party.

15. **Bribery and corruption**

15.1 For the purposes of this Clause 15, the expressions "**adequate procedures**" and "**associated with**" shall be construed in accordance with the Bribery Act 2010 and legislation or guidance published under it, together with any other applicable anti-bribery and anti-corruption laws (including, where applicable, the United States Foreign Corrupt Practices Act of 1977) (the "**Bribery Laws**").

15.2 Each party shall comply with applicable Bribery Laws including ensuring that it has in place adequate procedures to prevent bribery and ensure that:

(a) all of that party's personnel;

(b) all others associated with that party; and

(c) all of that party's subcontractors

involved in performing this Agreement so comply.

15.3 Without limitation to Clause 15.2, neither party shall offer, promise, give, request, agree to receive, or accept any bribe (as defined in the Bribery Act 2010) or other improper payment, or allow any such to be made or received on its behalf, in any location, and shall implement and maintain adequate procedures to ensure that such bribes or payments are not made or received directly or indirectly on its behalf.

15.4 Each party shall immediately notify the other as soon as it becomes aware of a breach or possible breach of any of the requirements in this Clause 15.

16. **Anti-slavery**

16.1 Each party recognises that it is bound by laws relating to antislavery and human trafficking and warrants that it has in place and complies with policies and procedures designed to enable it to comply with those laws.

16.2 Each party shall notify the other party as soon as it becomes aware of any actual or suspected slavery or human trafficking in a supply chain which has a connection with this Agreement.

17. **Communication and notices**

17.1 All notices shall be in writing and given when delivered to:

(a) for Risk Ledger, the address of the Risk Ledger contracting entity stated in Clause 18.1 or, if sent by email, to legal@riskledger.com;

(b) for an Organisation, the contact details provided by the Organisation at the time of registration on the Site or in the Order Form, or via the Services,

unless otherwise instructed by the relevant party in writing.

17.2 Any such notice shall be deemed to have been received:

(a) if delivered personally, at the time of delivery;

(b) if sent by email or via the Services, at the time of transmission;

(c) if sent by post within the country of the recipient's notice address, 2 Business Days after posting; and

(d) if sent by international post, 5 Business Days after posting,

provided that, if deemed receipt occurs after 5pm in the recipient's location on a Business Day, or on a day that is not a Business Day, then the notice shall be deemed to have been given on the next Business Day.

18. **Contracting entity, governing law and dispute resolution**

18.1 The Risk Ledger entity contracting with the Organisation depends on where the Organisation is domiciled when this Agreement is formed, unless the Order Form specifies a different Risk Ledger entity:

(a) where the Organisation is domiciled (based on its billing address on the Order Form or, where there is none, its place of formation) in the Americas, "Risk Ledger" means Risk Ledger Inc., a Delaware corporation with its notice address at Resident Agents Inc., 8 The Green, Suite R, Dover, DE 19901, United States; and

(b) where the Organisation is domiciled (based on its billing address on the Order Form or, where there is none, its place of formation) anywhere else, "Risk Ledger" means Risk Ledger Ltd., a company registered in England and Wales with company registration number 10831970 and its registered office at Adam House, 7-10 Adam Street, London, United Kingdom, WC2N 6AA.

18.2 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the choice of law identified for the contracting Risk Ledger entity in the table below:

Risk Ledger contracting entity	**Choice of law**
Risk Ledger Ltd.	England and Wales
Risk Ledger Inc.	Illinois, United States

18.3 Where Risk Ledger Ltd. is the contracting entity, the parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), save that Risk Ledger may elect to bring proceedings against the Organisation in the courts of any jurisdiction where the Organisation or any of its assets may be found or located.

18.4 Where Risk Ledger Inc. is the contracting entity, any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims) shall be finally resolved by binding arbitration administered by the

American Arbitration Association in accordance with its Commercial Arbitration Rules, by a single arbitrator, seated in Chicago, Illinois and conducted in English. Judgment on the award may be entered in any court of competent jurisdiction, and the Federal Arbitration Act governs the interpretation and enforcement of this Clause 18.4. Each party shall keep confidential the existence, content and outcome of any arbitration under this Clause, save as required by law or as necessary to enforce an award. Nothing in this Clause prevents either party from seeking injunctive or other equitable relief from a court of competent jurisdiction, and Risk Ledger may bring proceedings to recover unpaid Charges in the courts of any jurisdiction where the Organisation or any of its assets may be found or located. Each party waives any right to trial by jury, and claims may not be consolidated or arbitrated on a class or representative basis.

18.5 For clarity, an update to these terms in accordance with Clause 19 (*Amendments to the Terms of Service*) does not change the Risk Ledger entity that is party to any existing Agreement; this Clause 18 determines the contracting entity when an Agreement is formed.

19. Amendments to the Terms of Service

19.1 Risk Ledger may make commercially reasonable changes to these terms and any connected documents from time to time, providing at least 30 days' notice by one or more of the following methods prior to any material changes taking effect:

(a) email to Authorised Users; and/or

(b) providing a notification of the forthcoming update in the Services.

19.2 Any notice given under Clause 19.1 shall be deemed to have been given at the time of sending or posting, as applicable.

19.3 Where a change to these terms by Risk Ledger under Clause 19.1 affects the terms related to data privacy or security, such changes shall not reduce the overall security of the Services.

20. General

20.1 Except where otherwise expressly stated herein, this Agreement constitutes the entire agreement between the parties relating to the subject matter of this Agreement and supersedes any previous agreement or understanding whatsoever whether oral or written relating to the subject matter of this Agreement.

20.2 Unless otherwise stated, in the case of any conflict between the Order Form and these Terms of Service the Order Form shall prevail.

20.3 Except as amended pursuant to Clause 19 (*Amendments to the Terms of Service*), no variation of the provisions of this Agreement shall be valid unless confirmed in writing by the authorised signatories of both parties on or after the date of the last required signature on this Agreement.

20.4 Each party warrants to the other that it has the power and authority to enter into this Agreement and perform its obligations under this Agreement, and that entering into and performing its obligations under this Agreement will not cause it to breach any legal obligations.

20.5 This Agreement shall not be deemed to create any partnership or employment relationship between the parties.

20.6 Other than a Participant protecting its Confidential Information pursuant to Clause 6 (*Confidentiality*) or a Federated Principal acting for the benefit of one or more of its Federated Sub-organisations covered by an Order Form executed by the Federated Principal

(each an intended third party beneficiary of the relevant provision(s), which it may enforce including, where this Agreement is governed by the law of England and Wales, under the Contracts (Rights of Third Parties) Act 1999), a person who is not party to this Agreement shall have no rights (under the Contracts (Rights of Third Parties) Act 1999, as a third party beneficiary, or otherwise) to enforce any term of this Agreement. The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under this Agreement are not subject to the consent of any other person.

20.7 No act, failure or delay to act, or acquiescence by Risk Ledger or the Organisation in exercising any of its rights under this Agreement shall be deemed to be a waiver of that right or in any way prejudice any right of Risk Ledger or the Organisation under this Agreement, and no waiver by Risk Ledger of any breach of this Agreement by the Organisation shall be considered as a waiver of any subsequent breach of the same or any other provision. Any waiver or relaxation whether partly or wholly of any of the terms or conditions of this Agreement shall be valid only if in writing and signed by or on behalf of Risk Ledger and shall apply only to a particular occasion and shall not be continuing and further shall not constitute a waiver or relaxation of any other terms or conditions of this Agreement.

20.8 The rights and remedies provided in this Agreement for Risk Ledger are cumulative and not exclusive of any rights and remedies provided by law.

20.9 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Agreement.

Appendix 1: Service level agreement

The following sections provide relevant details on service availability, monitoring of in-scope Services and related components.

1. **Service availability**

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

1.1 **Web-based Services**

Risk Ledger's web-based Services will be available for a minimum of 99.5% of time within each calendar month. Scheduled Maintenance shall be excluded from downtime calculations. "**Available**" for this purpose means that the Site is operating, and all basic functions are accessible.

1.2 **Email support**

Email support is provided during Working Hours. Emails received outside of Working Hours will be collected, however no action can be guaranteed until commencement of Working Hours on the next Business Day.

Support may be requested by email to support@riskledger.com.

1.3 **Triage and priority of support requests**

Risk Ledger will deal with support requests based on Risk Ledger's determination of priority. Priority is determined through a combination of impact and urgency, as described below. Support requests do not include new feature requests.

Priority 1	The issue or failure is causing immediate critical and significant impact on major business functions for the Organisation. There is no possible workaround.
Priority 2	• The issue or failure is causing critical and significant impact on major business functions, but there is a workaround available; or • The issue or failure will imminently cause critical and significant impact on major business functions for the Organisation. There is no possible workaround; or • The issue or failure is causing critical and significant impact on non-core business functions, and there is no possible workaround.
Priority 3	The issue or failure is causing an impact on non-core business activities for the Organisation, and a workaround is available.
Priority 4	The issue or failure has limited impact or the impact is minimal and a workaround will be provided within the next calendar month.

1.4 **Target response and resolution targets**

Risk Ledger aims to respond and to satisfactorily resolve 90% of issues submitted to it within the targeted time, as specified below.

Priority	Target response time – confirmation by email that issue has been received and assigned a priority	Target resolution time
1	4 Working Hours	12 Working Hours
2	4 Working Hours	24 Working Hours
3	7 Working Hours	10 Business Days
4	8 Working Hours	20 Business Days

Target response and resolution times referenced above will be measured from whichever is the later of:

- When Risk Ledger receives a support request and such information as the Organisation has in order for Risk Ledger to give the issue a priority; and
- If there is ambiguity of whether the issue lies with Risk Ledger's or the Organisation's systems, from when Risk Ledger's engineers have confirmed that the cause of the issue is within Risk Ledger's system perimeter.

1.5 **Exceptions**

When a support request requires information or support from an external vendor or more information from the Organisation, Risk Ledger may take longer than the above periods to resolve such issues. Such additional time will not be counted as part of the target resolution times.

2. **Scheduled maintenance**

Risk Ledger will endeavour to provide the following minimum levels of notice in respect of Scheduled Maintenance:

Maximum outage period	Minimum notice	Minimum notice
5 minutes		24 hours
10 minutes		2 Business Days
30 minutes		5 Business Days
More than 30 minutes		10 Business Days

Appendix 2: Data protection

1. **Data protection definitions**

1.1 References to a "**paragraph**" in this Appendix are to the relevant paragraph of this Appendix indicated. The following additional definitions apply in this Appendix:

(a) "**Appropriate Safeguards**" means such legally enforceable mechanism(s) for transfers of personal data as may be permitted under Data Protection Laws from time to time;

(b) "**C2C Transfer**" means a transfer of personal data on a Controller to Controller basis;

(c) "**C2P Transfer**" means a transfer of personal data on a Controller to Processor basis for the Data Importer to process such personal data on behalf of the Data Exporter;

(d) "**Controller**", "**Processor**", "**data subject**", "**personal data**" and "**processing**" shall have the meanings ascribed to them in the applicable Data Protection Laws;

(e) "**Data Exporter**" means a party that transfers personal data (acting as a Controller) to another party in accordance with this Agreement;

(f) "**Data Importer**" means a party that receives personal data (acting as a Controller or a Processor) from another party in accordance with this Agreement;

(g) "**Data Protection Laws**" means any applicable privacy and data protection law(s) including, if and where applicable, EU Data Protection Laws and UK Data Protection Laws;

(h) "**Data Subject Request**" means a request made by a data subject to exercise any rights of data subjects under Data Protection Laws;

(i) "**EU Adequacy Finding**" means a decision by the European Commission under Article 45 of the EU GDPR in relation to a country, territory or international organisation or one or more specified sectors ensures an adequate level of protection for personal data to which the EU GDPR applies;

(j) "**EU Data Protection Laws**" means:

(i) all EU regulations applicable (in whole or in in part) to the processing of personal data (such as Regulation (EU) 2016/679 (the "**EU GDPR**"));

(ii) the national laws of each EEA member state implementing any EU directive applicable (in whole or in part) to the processing of personal data (such as Directive 2002/58/EC (the "**e-Privacy Directive**")); and

(iii) any other national laws of each EEA member state applicable (in whole or in part) to the processing of personal data,

as amended or superseded from time to time;

(k) "**EU SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to EU GDPR;

(l) "**EU/UK Data Transfer Provisions**" means the terms that apply when a Data Exporter transfers personal data subject to the EU GDPR and/or the UK GDPR to a Data Importer, as set out in Annex 3 (*EU/UK Data Transfer Provisions*) to this Appendix;

(m) "**Minimum Security Measures**" means the security measures specified in Annex 2 (*Minimum Security Measures*) to this Appendix, as may be updated or reissued by Risk Ledger from time to time;

(n) "**Personal Data Breach**" means any breach of security relating to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any personal data processed under this Agreement in a party's capacity as Processor;

(o) "**Protected Data**" has the meaning given to it in paragraph 2.3 of this Appendix;

(p) "**Standard Contractual Clauses**" means:

(i) where the EU GDPR applies, the EU SCCs; and

(ii) where the UK GDPR applies, the UK SCCs;

(q) "**Sub-Processor**" means another processor engaged by Risk Ledger to carry out processing activities in respect of the Protected Data on behalf of the Organisation;

(r) "**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;

(s) "**UK Adequacy Finding**" means any regulations having effect under Article 45A of the UK GDPR providing that transfers of personal data to a country, territory, sector or international organisation are approved for the purposes of UK GDPR;

(t) "**UK Data Protection Laws**" means:

(i) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**");

(ii) the Data Protection Act 2018 ("**DPA 2018**");

(iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 as it continues to have effect under section 2 of the European Union (Withdrawal) Act 2018 ("**PECR**"); and

(iv) any other laws in force in the UK from time to time applicable (in whole or in part) to the processing of personal data;

as such may be amended or superseded from time to time; and

(u) "**UK SCCs**" means standard data protection clauses adopted pursuant to or permitted under Article 46 of UK GDPR.

2. **Compliance, Controller and Processor**

2.1 Each party shall process any personal data involved in the performance of this Agreement in compliance with:

(a) their respective obligations under the Data Protection Laws; and

(b) the terms of this Agreement.

2.2 Risk Ledger is a Controller with respect to Authorised Users' account details, usage information and the contents of logs. For information about how Risk Ledger processes and protects such information, please see its privacy notice at https://riskledger.com/privacy.

2.3 In order to request a third party to set up a supplier profile on the Site, an Authorised User may need to input the business contact details of a Participant's member of staff into the

Services ("**Protected Data**"). For Protected Data, details of which are set out in Annex 1B to this Appendix, the Organisation is the Controller and Risk Ledger is the Processor. The remainder of this Appendix applies in respect of the Protected Data.

2.4 The Organisation warrants and undertakes that:

(a) its Authorised Users will only input Protected Data into the Services to the minimum extent that is reasonably required for the Organisation to make proper use of the Services in accordance with this Agreement; and

(b) all Protected Data provided to Risk Ledger for processing pursuant to this Agreement shall comply in all respects, including in terms of its collection, storage and processing (which shall include the Organisation ensuring that any required fair processing information and all necessary consents have been given to and received from the data subjects), with the Data Protection Laws.

2.5 Nothing in this Agreement shall require Risk Ledger to check or monitor the accuracy or contents, or the Organisation's use of, Protected Data.

3. **Instructions and details of processing**

Insofar as Risk Ledger processes Protected Data on behalf of the Organisation, Risk Ledger:

3.1 unless required to do otherwise by Data Protection Laws, shall (and shall take steps to ensure that each person acting under its authority shall) process the Protected Data only on and in accordance with the Organisation's documented instructions as set out in this Appendix or as submitted by the Organisation in writing including via the Site or the Services, and updated from time to time in accordance with the terms of this Agreement (the "**Processing Instructions**");

3.2 if any applicable UK or EU member state law requires it to process Protected Data other than in accordance with the Processing Instructions, Risk Ledger shall notify the Organisation of any such requirement before undertaking such processing of the Protected Data (unless such applicable law prohibits such information on important grounds of public interest); and

3.3 shall inform the Organisation if Risk Ledger becomes aware of a Processing Instruction that, in Risk Ledger's opinion, infringe any Data Protection Laws, provided that this shall be without prejudice to paragraph 2.4 (*Compliance, Controller and Processor*) and, to the maximum extent permitted by mandatory law, Risk Ledger shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities arising from or in connection with any processing in accordance with the Organisation's Processing Instructions following the Organisation's receipt of that information.

4. **Technical and organisational measures**

Risk Ledger shall implement and maintain, at its cost and expense, the technical and organisational measures:

4.1 appropriate to the risk of processing, including the Minimum Security Measures set out in Annex 2 to this Appendix; and

4.2 taking into account the nature of the processing, to assist the Organisation insofar as is possible in the fulfilment of their obligations to respond to Data Subject Requests.

5. **Using staff and other processors**

5.1 The Organisation grants to Risk Ledger general authorisation to appoint Sub-Processors, and additional or replacement Sub-Processors. The Sub-Processors used by Risk Ledger are identified at https://riskledger.com/privacy. Risk Ledger will provide 30 days' advance notice of its intention to appoint a new (or replacement) Sub-Processor, and the Organisation may object to such appointment or change.

5.2 Where the Organisation objects to the proposed appointment of a Sub-Processor under paragraph 5.1, Risk Ledger shall consider the reasons for the objection and take appropriate steps to ensure that the proposed or appointment or change in Sub-Processors does not prevent Risk Ledger's implementation of appropriate technical and organisational measures relating to data processing.

5.3 Risk Ledger shall:

(a) prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract enforceable by Risk Ledger containing materially the same obligations as under this Agreement;

(b) ensure that each Sub-Processor complies with all such obligations; and

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

5.4 Risk Ledger shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential.

6. **Assistance with Organisation's compliance and data subject rights**

6.1 Risk Ledger shall refer to the Organisation all Data Subject Requests and any relevant notices and correspondence it receives from a Supervisory Authority in respect of data processed on behalf of the Organisation within three Business Days of receipt of the request.

6.2 Risk Ledger shall provide to the Organisation such reasonable assistance as the Organisation reasonably requires (taking into account the nature of processing and the information available to Risk Ledger) in ensuring compliance with the Organisation's obligations under Data Protection Laws (and the Organisation shall pay to Risk Ledger such costs as are reasonable in the circumstances) with respect to:

(a) security of processing;

(b) data protection impact assessments (as such term is defined in Data Protection Laws);

(c) prior consultation with a Supervisory Authority regarding high risk processing;

(d) responding to Data Subject Requests; and

(e) notifications to the Supervisory Authority and/or communications to data subjects by the Organisation in response to any Personal Data Breach.

7. **International data transfers**

7.1 Due to the international nature of supply chains, the Organisation agrees that Risk Ledger may transfer Protected Data to any country, provided all transfers by Risk Ledger of Protected Data shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws.

7.2 If the Organisation is based in, or is transferring to Risk Ledger personal data held by it in, an EEA member state, paragraphs 7.3 and 7.4 shall apply. For this purpose, the Organisation shall be the Data Exporter and Risk Ledger the Data Importer.

7.3 Where the Data Exporter performs a C2P Transfer of personal data to the Data Importer and the personal data is:

(a) Subject to the EU GDPR; and/or

(b) Subject to the UK GDPR,

the parties shall additionally comply with Part B (*C2P Transfers*) and Part C (*Supplemental EU/UK transfer requirements*) of the EU/UK Data Transfer Provisions.

7.4 Where the Data Exporter performs a C2C Transfer of personal data to the Data Importer and the personal data is:

(a) Subject to the EU GDPR; and/or

(b) Subject to the UK GDPR,

the parties shall additionally comply with Part A (*C2C Transfers*) and Part C (*Supplemental EU/UK transfer requirements*) of the EU/UK Data Transfer Provisions.

7.5 For any transfers of personal data between the Organisation and any other Participant via the Services involving an export of personal data from the EEA or the United Kingdom, where such transfer is not covered by another Appropriate Safeguard recognised in the Data Exporter's jurisdiction then, until such time as another Appropriate Safeguard becomes applicable:

(a) the Organisation shall put in place the relevant Standard Contractual Clauses between the Organisation and other Participant; and

(b) where the Data Importer is processing personal data protected under the UK GDPR outside the UK in a territory not at that time subject to a UK Adequacy Finding, then the Organisation shall ensure that the Data Importer complies with the terms of clauses 14 and 15 of the EU SCCs or the equivalent.

7.6 If an alternative Appropriate Safeguard becomes available, an update of these terms to replace either or both of the Standard Contractual Clauses referenced in the EU/UK Data Transfer Provisions with such alternative Appropriate Safeguard (as is appropriate to the scope of that Appropriate Safeguard) shall be deemed reasonable for the purposes of Clause 19.1 (*Amendments to the Terms of Service*) of this Agreement.

8. **Records, information and audit**

8.1 Risk Ledger shall, in accordance with Data Protection Laws, make available to the Organisation such information as is reasonably necessary to demonstrate Risk Ledger's compliance with its obligations under this Appendix, and allow for and contribute to audits, including inspections, by the Organisation (or, subject to paragraph 8.2, another auditor mandated by the Organisation) for this purpose, subject to the Organisation:

(a) being limited to one audit per year, except to the extent that the Data Protection Laws require more frequent audits;

(b) giving Risk Ledger reasonable prior notice of such information request, audit and/or inspection being required by the Organisation;

(c) ensuring that all information obtained or generated by the Organisation or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by the Data Protection Laws);

(d) ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to Risk Ledger's business and the business of its other customers; and

(e) paying Risk Ledger's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

8.2 If a third party is to conduct an audit under paragraph 8.1, the third party must be mutually agreed to by the Organisation and Risk Ledger (except if such third party is a Supervisory Authority). Risk Ledger will not unreasonably withhold its consent to a third party auditor requested by the Organisation. The third party must execute a written confidentiality agreement acceptable to Risk Ledger or otherwise be bound by a statutory or legal confidentiality obligation protective of Risk Ledger.

9. **Breach notification**

In respect of any Personal Data Breach, Risk Ledger shall, without undue delay:

9.1 notify the Organisation of the Personal Data Breach; and

9.2 provide the Organisation with details of the Personal Data Breach.

10. **Deletion or return of Organisation Data and copies**

Risk Ledger shall, at the Organisation's written request, either delete or return all the Protected Data to the Organisation in such form as the Organisation reasonably requests within a reasonable time after the earlier of:

10.1 The end of the provision of the relevant Services related to processing; or

10.2 Once processing by Risk Ledger of any Protected Data is no longer required for the purpose of Risk Ledger's performance of its relevant obligations under this Agreement,

and delete existing copies (unless storage of any Protected Data is required by applicable laws and, if so, Risk Ledger shall inform the Organisation of any such requirement).

Annex 1A: Information on Processor

Risk Ledger Limited is registered with the UK's Information Commissioner's Office ("**ICO**") with reference number ZA485622. References in this Appendix to Risk Ledger are to the Risk Ledger contracting entity determined in accordance with Clause 18 of the Agreement; where Risk Ledger Inc. is the contracting entity, Risk Ledger Ltd. operates the Services as a Sub-Processor.

Risk Ledger's Data Protection Policy is published here: https://riskledger.com/privacy.

For data protection matters please contact us by email at data@riskledger.com.

Annex 1B: Information on processing activities

Subject matter	Protected Data as defined in paragraph 2.3.
Duration of processing activities	For the length of this Agreement to facilitate the Organisation's use of the Services. Some Protected Data may be stored in encrypted

	backups for no longer than 1 month after the termination of this Agreement.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	Continuous.
Nature and purpose of the processing activities	To enable the Organisation and Participants to get into contact with each other in relation to the Services.
Types of personal data	Business contact details.
Categories of data subject	Members of staff of Participants and prospective Participants involved in the Organisation's third party risk management programme.

Annex 1C: Competent Supervisory Authority

For transfers made under the EU SCCs, the competent Supervisory Authority will be determined in accordance with clause 13 of the EU SCCs.

For transfers made under the UK SCCs, the competent Supervisory Authority will be the United Kingdom Information Commissioner's Office.

Annex 2: Minimum Security Measures

Measures of pseudonymisation and encryption of personal data	Data is encrypted at rest and in transit using AES-256 encryption.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Our system architecture is subject to regular penetration testing and we have a full information security programme implemented.
Measures to quickly restore the availability and access to personal data in the event of a physical or technical incident	We maintain a full IT disaster recovery process and business continuity process. This is tested annually. We follow a strict backup policy which includes both online and offline backups.
Regular verification, evaluation and assessment processes to determine the effectiveness of technical and organizational measures to ensure the security of the processing	We run regular vulnerability scans of our internal and external environment. We conduct regular penetration testing of our production application and hosting infrastructure.
Measures for user identification and authorisation	We enforce multifactor authentication on all user accounts. We enforce through technical means a policy of requiring exceeding a minimum complexity standard.
Measures for the protection of data during transmission	Data is encrypted at rest and in transit using AES-256 encryption. We enforce a TLS version of 1.2 or greater.
Measures for data protection during storage	Data is encrypted at rest and in transit using AES-256 encryption. Our data is stored within secure data centres with strong security controls.
Measures to ensure the physical security of the places where personal data is processed	Data is stored within our production environment that has strict physical security policies in place.

	Physical controls include CCTV, alarmed perimeters, and armed security.
Measures to ensure the recording of incidents	We use a gold standard logging solution that centralises all our events and logs from across our environment. These are monitored with automated alerts triggered if thresholds are met.
Measures to ensure system configuration, especially default configuration	System configuration is maintained by using a defined CI/CD pipeline (with security and quality testing built in) with infrastructure as code, subject to multiple approvals before deployment.
Internal IT governance and management measures and information security	We maintain a full ISMS covering a full suite of security policies and processes. Security is managed by our CEO with support from defined members of staff, with their roles documented.
Measures for the certification/guarantee of processes and products	Risk Ledger undertakes regular internal reviews of its security, and regular external reviews for certification against a variety of standards, including Cyber Essentials and ISO27001.
Measures to ensure data minimisation	We conduct regular reviews of the personal data we collect to ensure we have a need to collect it. This is further supported by us enforcing the principle of least privilege across the company.
Measures to ensure data quality	We enforce data validation on all input fields.
Measures to ensure limited data retention	All data is retained in line with our data retention schedule, which is enforced through technical means.
Measures to ensure accountability	We require all users to have their user account with a unique ID. We keep auditable logs of events and actions within the platform. We enforce multi-factor authentication on all user accounts.
Measures for allowing data portability and ensuring erasure	We have a defined process for ensuring data portability in line with our data protection requirements. Upon request, personal data is deleted from our platform using a secure delete script.

Annex 3: EU/UK Data Transfer Provisions

Part A: C2C Transfers

1. **C2C Transfers – EU GDPR**

Where the Data Importer is processing as a Controller personal data protected under the EU GDPR outside the EEA in a territory or sector not at that time subject to an EU Adequacy Finding then, the EU SCCs will be deemed entered into (and incorporated into this Agreement by this reference) between the transferring Data Exporter and that Data Importer in relation to that personal data and completed as follows:

1.1 Module One will apply;

1.2 in clause 7, the optional docking clause will not apply;

1.3 in clause 11, the optional language will not apply;

1.4 in clause 17, option 1 will apply, and the EU SCCs will be governed by Irish law;

1.5 in clause 18(b), disputes shall be resolved before the courts of Ireland;

1.6 in Annex I:

(a) Part A: with the information set out in Annex 4 to this Agreement;

(b) Part B: with the relevant Processing details set out in Annex 1B to this Agreement;

(c) Part C: in accordance with the criteria set out in clause 13(a) of the EU SCCs;

1.7 In Annex II: with the Minimum Security Measures, in the format set out in Annex 2 to this Agreement.

2. **C2C Transfers – UK GDPR**

Where the Data Importer is processing as a Controller personal data protected under the UK GDPR outside the UK in a territory or sector not at that time subject to a UK Adequacy Finding, then the UK SCCs will be deemed entered into (and incorporated into this Agreement by reference) between the transferring Data Exporter and that Data Importer in relation to that personal data and completed as follows:

2.1 Where the Data Exporter and Data Importer are lawfully permitted to rely on the EU SCCs for transfers of UK personal data subject to the completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

(a) The EU SCCS, completed as set out above in paragraph 1 (*C2C Transfers – EU GDPR*) of this Part A, shall also apply to transfers of such personal data, subject to sub-paragraph (b) below; and

(b) The UK Addendum shall be deemed executed between the transferring Data Exporter and the Data Importer, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such personal data.

2.2 If paragraph 2.1 does not apply, then the transferring Data Exporter and the Data Importer shall cooperate in good faith to implement appropriate safeguards for transfers of such personal data as required or permitted by UK GDPR without undue delay.

Part B: C2P Transfers

1. **C2P Transfers – EU GDPR**

Where the Data Importer is processing as a Processor personal data protected under the EU GDPR outside the EEA in a territory or sector not at that time subject to an EU Adequacy Finding then, the EU SCCs will be deemed entered into (and incorporated into this Agreement by this reference) between the transferring Data Exporter and that Data Importer in relation to that personal data and completed as follows:

1.1 Module Two will apply;

1.2 in clause 7, the optional docking clause will not apply;

1.3 in clause 9, option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in paragraph 5.1 of Appendix 2 to this Agreement;

1.4 in clause 11, the optional language will not apply;

1.5 in clause 17, option 1 will apply, the EU SCCs will be governed by Irish law;

1.6 in clause 18(b), disputes shall be resolved before the courts of Ireland;

1.7 in Annex I:

(a) Part A: with the information set out in Annex 4 to this Agreement;

(b) Part B: with the relevant Processing details set out in Annex 1B to this Agreement;

(c) Part C: in accordance with the criteria set out in clause 13(a) of the EU SCCs;

1.8 In Annex II: with the Minimum Security Measures, in the format set out in Annex 2 to this Agreement.

2. **C2P Transfers – UK GDPR**

Where the Data Importer is processing as a Processor personal data protected under the UK GDPR outside the UK in a territory or sector not at that time subject to a UK Adequacy Finding, then the UK SCCs will be deemed entered into (and incorporated into this Agreement by reference) between the transferring Data Exporter and that Data Importer in relation to that personal data and completed as follows:

2.1 Where the Data Exporter and Data Importer are lawfully permitted to rely on the EU SCCs for transfers of UK personal data subject to completion of a UK Addendum, then:

(a) The EU SCCS, completed as set out above in paragraph 1 (*C2P Transfers – EU GDPR*) of this Part B, shall also apply to transfers of such personal data, subject to sub-paragraph (b) below; and

(b) The UK Addendum shall be deemed executed between the transferring Data Exporter and the Data Importer, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such personal data.

2.2 If paragraph 2.1 does not apply, then the transferring Data Exporter and the Data Importer shall cooperate in good faith to implement appropriate safeguards for transfers of such personal data as required or permitted by UK GDPR without undue delay.

Part C: Supplemental EU/UK transfer requirements

The following additional terms shall also apply to the above-mentioned C2C Transfers and C2P Transfers:

1. If there is any conflict between this Agreement and the Standard Contractual Clauses applicable to the Data Exporter's transfer of personal data to a Data Importer, those Standard Contractual Clauses shall prevail.

2. Where the Data Importer is lawfully able to receive or process the relevant personal data under the EU-US Data Protection Framework (including the UK Extension thereto as appropriate), then:

2.1 that framework and any relevant extension shall automatically be deemed to apply to the transfer of personal data from the Data Exporter to the Data Importer from the EEA or the UK so long as it remains valid;

2.2 the relevant Standard Contractual Clauses shall no longer apply to that transfer; and

2.3 in the event that this eligibility is terminated or becomes invalid, or is no longer applicable to the Data Importer, then the Standard Contractual Clauses shall once again apply.

Annex 4 – List of parties

Data exporter(s)

Name	The Organisation, as defined in the Agreement.
Address	As provided by the Organisation at the time of registration on the Site.
Contact person's name, position and contact details	As provided by the Organisation at the time of registration on the Site.
Activities relevant to the data transferred under these clauses	To enable the Organisation and Participants to contact each other in relation to the Services.
Signature and date	This Annex 4 shall be deemed executed upon the Organisation entering into the Agreement.
Role (controller/processor)	Controller.

Data importer(s)

Name	The Risk Ledger contracting entity determined in accordance with Clause 18 of the Agreement.
Address	As stated in Clause 18.1 of the Agreement.
Contact person's name, position and contact details	Haydn Brooks, CEO. data@riskledger.com.
Activities relevant to the data transferred under these clauses	To enable the Organisation and Participants to contact each other in relation to the Services.
Signature and date	This Annex 4 shall be deemed executed upon the Organisation entering into the Agreement.
Role (controller/processor)	Risk Ledger is a processor in relation to Protected Data (as defined in the Agreement). Risk Ledger is a controller with respect to Authorised Users' (as defined in the Agreement) account details, usage information and the contents of logs.