Copla

Terms and Conditions

Version	Effective	Contact
1.5	2026-10-13	legal@copla.com

Contents

01	Copla Terms and Conditions	Version 1.5 · 2026-10-13
02	RoI Special Terms	Last update: 2026-03-17 · Version 1.1
03	MTP Register Special Terms	Last update: 2026-08-25 · Version 1.0
04	Incident Register Special Terms	Last update: 2026-03-17 · Version 1.0
05	EBA Register Special Terms	Last update: 2026-03-23 · Version 1.0
06	CoreGuardian Special Terms	Last update: 2026-03-23 · Version 1.0
07	Consulting Special Terms	Last update: 2026-03-23 · Version 1.0
08	Vendriq Special Terms	Last update: 2026-03-23 · Version 1.0

09	Managed Vendor Risk Management Special Terms	
10	Copla Service Level Agreement (SLA)	Version 1.0 · 2026-03-23
11	Copla Data Processing Agreement	Last update: 2026-08-25 · Version 2.1
12	Annex I to the DPA	Version 1.5 · 2026-10-13
13	Annex II to the DPA	Version 1.5 · 2026-10-13

Copla Terms and Conditions

Version 1.5 2026-10-13

1. General Provisions. Scope

1.1. These Terms, as well as the documents referenced herein, such as the applicable Special Terms (including, as applicable, the RoI Special Terms, CG Special Terms, IR Special Terms, EBA Special Terms, MTP Special Terms, Vendriq Special Terms, MVRM Special Terms, and/or Consulting Special Terms), the DPA, the Copla Service Order Form (“OF”), the onboarding plan (“OP”), and the SLA, apply to the contractual relationship between Copla and its clients on the provision of the Services (as described hereinafter). For the avoidance of doubt, CISO as a Service (CISOaaS) and Internal Audit (IA) services are governed by separate agreements and are not subject to these Terms.

1.2. Terms used in the Agreement are defined in these Terms, the applicable Special Terms, the DPA, the SLA, or the OF.

1.3. Any entity that is directly or indirectly controlled, managed, or jointly controlled by the Client ("Client Affiliate") and wishes to receive services under the Agreement must either (i) be specified in the OF and must adhere to the terms of the Agreement (in which case any reference to "Client" in the Agreement refers to the relevant Client Affiliate); or (ii) enter into a separate agreement with terms substantially similar to those set out in the Agreement. If a Client Affiliate is specified in the OF, the Client is responsible for any action or inaction of the relevant Client Affiliate that breaches the Agreement.

1.4. **Documents forming the Agreement.** The Terms, the applicable Special Terms, the DPA, and the SLA form part of the Agreement either by being attached to the OF or by being incorporated into it by reference at the link specified in the OF. They apply in the version identified in the OF and in force as at the Effective Date. Copla shall keep that version accessible to the Client at a stable address for the term of the Agreement and for six (6) years thereafter, and shall on request and at no charge provide the Client with a copy in a durable medium. Any subsequent version applies only in accordance with Chapter 3. If a document is not accessible

at the link specified in the OF at the time of signature, the version most recently provided to the Client in a durable medium shall apply. Where a document is attached to the OF, the attached version applies.

2. Services

2.1. Copla offers technology-enabled compliance automation services using the Copla or partner systems, add-ons, and platforms (“Copla Platform” or “Platform”), as detailed in the applicable Special Terms (hereinafter collectively and individually referred to as “Service” or “Services”). The specific features, functionalities, and scope of each Service are described in the applicable Special Terms. By signing the OF, the Client agrees to adhere to the Agreement.

2.2. Conclusion of the Agreement. The Agreement is concluded when the Client accepts the OF issued by Copla. The Client may accept by signing the OF (by handwritten or electronic signature), by confirming its acceptance in writing (including by email or other electronic means), or by paying the first invoice issued under the OF or using the Services after receiving it. Where both parties sign the OF, the Agreement is concluded on the date of the later signature. In every other case, Copla is deemed to have signed the OF it issued and no signature by Copla is required. The Agreement is then concluded on the date the Client’s acceptance first reaches Copla or, for acceptance by payment or use, on the date of payment or first use, whichever is earlier. Copla is not bound by an OF it withdrew before acceptance or whose stated validity period has expired. An acceptance that adds to or changes the OF is not an acceptance unless Copla confirms it in writing. Each form of acceptance has the same effect as a signature. Any reference in the Agreement to signing or signature, including to a signed OF, includes acceptance of the OF in any manner set out in this clause, and any reference to the date of signature means the date on which the Agreement is concluded under this clause. On conclusion, the documents listed in the OF form part of the Agreement in accordance with clause 1.4, whether or not they are physically attached to the OF, and the Client accepts the Agreement in full. Any deviations from or supplements to these Terms apply only if Copla has expressly agreed to them in writing in a document forming part of the Agreement.

2.3. The scope of Services agreed upon by the parties is specified in the OF and the OP. Services may have technical limitations or be limited in scope, as specified in the applicable Special Terms, OF, OP, and/or SLA. Service levels, availability commitments, and support terms are governed by the SLA.

2.4. Copla has the right to entrust another entity to provide all or part of the Services under this Agreement. Any subcontracting agreement entered into or granted by Copla does not release Copla from any of its obligations under this Agreement, and any act or omission of a Copla subcontractor is considered an act or omission of Copla under this Agreement.

2.5. Services operate at all hours, but there may be periods of Service unavailability. Copla makes every effort to ensure that Services are available in accordance with the availability commitments set out in the SLA.

2.6. Upon conclusion of the Agreement and the Client adhering to these Terms, Copla will provide the Client with access to the Platform to use the Services.

2.7. The specific Special Terms that apply to the Client depend on the Service(s) subscribed to under the OF. The following Special Terms are applicable to the respective Copla products and services: (i) RoI Special Terms – applicable to Clients using the RoI product; (ii) CoreGuardian Special Terms – applicable to Clients using the CoreGuardian product; (iii) Incident Register Special Terms – applicable to Clients using the Incident Register product; (iv) EBA Register Special Terms – applicable to Clients using the EBA Register product; (v) Consulting Special Terms – applicable to Clients receiving Consulting services; (vi) MTP Special Terms – applicable to Clients using the MTP Register product; (vii) Vendriq Special Terms – applicable to Clients using the Vendriq product; (viii) MVRM Special Terms – applicable to Clients subscribing to the Managed Vendor Risk Management Service. Where a Client subscribes to multiple products or services, all applicable Special Terms apply concurrently. In the event of a conflict between these Terms and any applicable Special Terms, the Special Terms shall prevail with respect to the subject matter they govern. Special Terms which do not correspond to a Service subscribed to under the OF form no part of the Agreement, impose no obligations on either party, and confer no rights on either party. The Services for which a price is stated in the OF determine which Special Terms apply, and no Special Terms apply by reason only of the Client being subject to the regulatory regime or framework they address.

2.8. **Data Retention and Return on Termination.** Upon expiry or termination of the Agreement or of a Client's access to any Service, for any reason, the Client shall be provided with a grace period of thirty (30) days during which it may export all Client Data and output files generated through the applicable Service. During this period, Copla shall ensure access to and the return of all Client Data in a structured, commonly used, and machine-readable format. In the event of discontinuation of Copla's business operations, insolvency, or resolution, Copla (or its liquidator or legal successor) shall equally guarantee access, recovery, and return of all Client Data during the same grace period.

2.9. **Deletion of Client Data.** Following expiry of the grace period referred to in clause 2.8, Copla shall delete or anonymise all Client Data associated with the terminated Service, unless retention is required by applicable law or the DPA. Prior to any permanent deletion or anonymisation of Client Data, Copla shall provide the Client with at least thirty (30) days' prior written notice, confirming that the Client Data remains available for export and requesting the Client's confirmation that it has no further objections to deletion. The specific data return and deletion obligations applicable to individual Services may be further detailed in the applicable Special Terms; in the event of conflict, the Special Terms shall prevail.

2.10. **Exit Assistance.** Upon expiry or termination of the Agreement or of access to any Service, Copla shall provide the Client with reasonable transition assistance upon request, for a period of up to sixty (60) days following the effective date of termination. Such assistance shall include making available relevant data schemas, configuration documentation, and reasonable technical support to facilitate the migration of Client Data to a successor system or provider. Exit assistance shall be provided at rates agreed in advance and shall not be unreasonably withheld or delayed. Copla shall take no action that would impair or hinder the Client's ability to migrate its data or transition to an alternative solution.

2.11. **Third-Party Audit and Assessment Services.** In addition to the Services, Copla may make available to the Client external audit, certification, assessment, attestation, or testing services ("**Audit Services**"). The Audit Services are provided and performed exclusively by the independent third-party audit or assessment firm identified in the OF ("**Auditor**"). Copla does not perform, conduct, supervise, review, verify, or control the Audit Services, does not issue any certificate, opinion, report, or attestation, is not a certification body, and assumes no responsibility for the Audit Services or for any act or omission of the Auditor.

2.12. The Auditor's own terms and conditions, made available at the link or in the document specified in the OF ("**Auditor Terms**"), govern the performance of the Audit Services and establish a direct legal relationship between the Client and the Auditor. By signing the OF, the Client confirms that it has reviewed and accepts the Auditor Terms, understands that it thereby enters into a separate legal relationship with the Auditor, and acknowledges that Copla is not a party to that relationship. Where the Auditor requires a separate engagement letter or contract, the Client shall enter into it directly with the Auditor. In the event of any conflict, the Auditor Terms shall prevail in respect of the performance of the Audit Services, and the Agreement shall prevail in respect of the Services and of invoicing and payment.

2.13. The Client acknowledges that the Auditor acts independently and that neither Copla nor the Client may influence the Auditor's scoping decisions, findings, opinion, or certification decision. The Auditor may decline, suspend, qualify, or withdraw any certification or opinion. No such outcome constitutes a defect in or failure of the Services, a breach of the Agreement by Copla, or grounds for withholding or reclaiming the fees payable for the Services.

2.14. Copla will invoice the Client for the Audit Services and the Client shall pay Copla in accordance with Chapter 7. Payment made to Copla discharges the Client's corresponding payment obligation in respect of the Audit Services to the extent of the amount paid. Fees for the Audit Services are as stated in the OF and are not subject to clause 7.6 or clause 7.7. COPLA ASSUMES NO LIABILITY AND NO RESPONSIBILITY WHATSOEVER IN RESPECT OF THE FEES FOR THE AUDIT SERVICES. Once the Auditor has commenced work, fees for the Audit Services are non-refundable, and Copla shall not be required to refund, credit, reimburse, discount, or otherwise bear any fee, cost, or expense charged for the Audit Services, whether or not the Audit Services are performed, are performed defectively or late, or result in any certification or other outcome. Any claim for the repayment, reduction, or reimbursement of fees for the Audit Services shall be brought by the Client directly against the Auditor under the Auditor Terms. The Client shall not withhold, set off, or deduct any such amount against any sum payable to Copla under the Agreement.

2.15. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, COPLA MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND IN RESPECT OF THE AUDIT SERVICES, INCLUDING AS TO THEIR QUALITY, TIMELINESS, SCOPE, ACCURACY,

INDEPENDENCE, OR THE ACHIEVEMENT OF ANY CERTIFICATION OR OTHER OUTCOME, AND COPLA ASSUMES NO RESPONSIBILITY AND SHALL HAVE NO LIABILITY WHATSOEVER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), FOR BREACH OF STATUTORY DUTY, IN RESTITUTION, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THE AUDIT SERVICES, THE FEES FOR THE AUDIT SERVICES, THE AUDITOR TERMS, OR ANY ACT OR OMISSION OF THE AUDITOR, INCLUDING ANY DELAY, NON-PERFORMANCE, DEFECTIVE OR NEGLIGENT PERFORMANCE, REFUSAL, SUSPENSION, QUALIFICATION OR WITHDRAWAL OF A CERTIFICATION, BREACH OF CONFIDENTIALITY, OR REGULATORY OR SUPERVISORY CONSEQUENCE. ALL CLAIMS IN CONNECTION WITH THE AUDIT SERVICES SHALL BE BROUGHT BY THE CLIENT DIRECTLY AGAINST THE AUDITOR UNDER THE AUDITOR TERMS. Copla shall, at the Client's request, provide reasonable assistance in raising such a claim with the Auditor.

2.16. If any exclusion in clause 2.15 is held to be unenforceable in whole or in part, Copla's aggregate liability in respect of the Audit Services shall not exceed one thousand (1,000) euros, shall in no circumstances extend to the repayment or reimbursement of any fee for the Audit Services, and clause 10.1 (exclusion of indirect loss) shall continue to apply. Any such liability counts towards, and is not in addition to, the aggregate cap in clause 10.2. Nothing in clauses 2.15 or 2.16 excludes liability which cannot be excluded or limited under applicable law.

3. Amendments

3.1. Copla may occasionally amend the Agreement to reflect technical progress in services and to ensure continuous compliance with applicable mandatory laws (including, but not limited to, applicable data protection laws) ("Amendments"). Information about such Amendments will be provided by Copla within a reasonable period (but no later than thirty (30) days before the planned effective date of the change). The amended Terms will come into effect upon being published on Copla's website and/or being notified to the Client by email, as specified in the OF. The Client acknowledges and agrees that using any Service after the effective date of the Amendments implies that the Client agrees with the Amendments. It is the Client's duty and responsibility to familiarize themselves with the Amendments.

3.2. If the Amendments negatively affect the Client's reasonable interests and it is no longer reasonable to expect the Client to adhere to the amended Agreement, the Client, having thoroughly described such impact, may terminate the Agreement.

4. Representations and Warranties

4.1. The Client is responsible for any use of the login information for the Copla Platform. The Client must provide correct, accurate, up-to-date, and comprehensive data in their account on the Copla Platform (“Access Data”). Except as provided in Chapter 13 (Assignment), the Client’s account may not be transferred or otherwise conveyed unless agreed to in writing by Copla. The Client shall immediately inform Copla of any misuse or unauthorized use of their Access Data or Client account and is responsible for their account on the Copla Platform. Copla has the right to temporarily block the Client’s access to the Copla Platform and prevent the Client from using the Services if Copla reasonably believes there are signs of misuse of the Access Data. Access will be restored to the Client as soon as such suspicions are removed and/or additional security measures are implemented (e.g., change of Access Data).

4.2. The Client is always responsible for the accuracy and correctness of their settings and information provided on the Copla Platform.

4.3. The Client acknowledges and agrees that they may have to adhere to certain third-party service provider policies, which will be presented in the Copla Platform’s user interface (hereinafter referred to as "UI"), sent to the Client’s specified email, and/or presented to the Client at the time of ordering such third-party services.

4.4. In using the Services, the Client may not (i) copy, decompile, reverse-engineer, or otherwise alter all or part of the Copla Platform, Services, accessible technical specifications and documentation (hereinafter referred to as "Copla Material") or create derivative works (except as permitted by law); (ii) use the Services in violation of applicable laws or transmit content (including data) that is illegal or infringes any intellectual property rights or other rights of third parties; and (iii) interfere with the operation or security of the Services and the Copla Platform. Notwithstanding the foregoing, Copla Material may be copied to the extent necessary to use the Services.

4.5. Each Party represents and warrants that (i) it is and will be duly authorized to enter into and perform the Agreement; (ii) it can legally receive and/or provide Services under this Agreement; (iii) it will perform Services diligently, in compliance with all applicable laws and industry standards; (iv) the Services provided comply with applicable laws; and (v) there are no ongoing (or imminent) legal actions, claims, or court proceedings against it that would have a substantial negative impact on its ability to perform its obligations under the Agreement.

4.6. Each Party represents and warrants that it understands that the Services, where applicable, are of an advisory or informational nature. Copla's recommendations, outputs, and reports are provided based on the best available industry standards and information provided by the Client, and Copla does not guarantee specific business, technical, or compliance outcomes. The Client is solely responsible for evaluating, implementing, or acting upon any recommendations or outputs provided through the Services. The specific scope of Copla's responsibilities and any applicable disclaimers in connection with a particular Service are set out in the applicable Special Terms.

5. Data Collection, Processing, and Storage

5.1. Certain personal data of the Client will be processed while using the services. In doing so, Copla acts only as authorized by the Client in the Agreement and the DPA. Copla implements and maintains technical and organizational measures related to the security of Personal Data processing.

6. Licenses and Restrictions

6.1. The Client agrees that Copla owns and retains all rights, title, and interest in the Services (or lawfully uses rights granted by third parties), including all software, databases, and other aspects and technologies related to the Copla Platform, any enhancements, modifications, or derivative works thereof, any material provided by Copla to the Client through the Copla Platform, such as through relevant user interfaces (UI) or other means, and all intellectual property rights therein. Subject to the terms of this Agreement, Copla grants the Client a limited, non-exclusive, non-transferable, revocable right and license to use the Services solely for activities related to this Agreement during its term. All rights not expressly granted here are reserved to Copla or third parties owning rights in parts of the Services or

Platform. The Client must use the Copla Platform only according to the instructions provided by Copla and Copla's standard security procedures, about which Copla will inform the Client.

6.2. The parties agree that the Client shall have the right to use certain material (documentation provided during the provision of Services) obtained in the course of providing Services even after the expiration of the Agreement. However, the parties agree that such use shall be solely for the Client's needs and shall not be resold or otherwise transferred to third parties.

6.3. The Client shall not allow (and shall not permit any third party to): (a) copy or duplicate the Services; (b) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code, object code, or underlying structure, ideas, or algorithms of the Services; (c) modify or create derivative works based on the Services; (d) rent, lease, distribute, sublicense, resell, pledge, transfer or otherwise convey rights to the Services; or (e) remove or otherwise alter any proprietary notices or labels from the Services or any part thereof. Furthermore, the Client may not resell the Services.

6.4. Copla has the right to use all data collected in the course of providing Services or related to them: (a) to fulfill its obligations under this Agreement; (b) to optimize and improve its services; (c) for analysis. If any part of the data belongs to the Client, the Client grants Copla a non-exclusive, royalty-free license valid for the duration of the Agreement to use all such data for the purposes stated in the preceding sentence.

7. Payment

7.1. The fees, their application, and calculation method are described in the OF or on the Copla website.

7.2. All agreed fees for Services do not include value-added tax, digital, and all other taxes. The Client assumes full responsibility for the payment of all applicable taxes from their funds.

7.3. Copla shall invoice the fees for the Services in advance at the billing frequency stated in the OF, for example monthly, quarterly, or annually, and, where the OF states none, monthly in advance. Where a fee is expressed as a monthly amount, each invoice covers that amount multiplied by the number of months in the billing

period. Each invoice is issued no later than ten (10) calendar days after the start of the billing period it covers. Charges that arise during a billing period, including for additional Services, are invoiced monthly in arrears unless the OF states otherwise.

7.4. The Client shall pay invoices into Copla's bank account specified in the invoice or OF, adhering to the payment terms set in the OF. Payment terms are calculated from the date of invoice issuance and presentation to the Client. Non-payment of any Copla invoice according to the payment terms is a material breach of the Agreement.

7.5. In the event of late payment of amounts according to issued invoices, Copla has the right to suspend the provision of Services until payment is received and to charge interest at a rate of two (2) percent per month or the highest rate permitted by law, whichever is lower. The Client will also be responsible for all reasonable costs incurred by Copla in collecting any overdue amounts from the Client and/or Client Affiliate(s).

7.6. Copla may increase the fees for the Services once per each twelve (12) month period of the Agreement by up to ten percent (10%), effective as of each anniversary of the Effective Date specified in the OF. Copla shall notify the Client of any such increase at least thirty (30) days in advance of its effective date. The increased fees shall apply automatically from the effective date unless otherwise agreed in writing by the parties.

7.7. **Committed Term Pricing.** Where the Initial Term specified in the OF is three (3) years or longer, clause 7.6 shall not apply during the Initial Term and the fees for the Services shall remain fixed for the duration of the Initial Term. In consideration of that price commitment, if the Agreement is terminated before the end of the Initial Term (i) by the Client for convenience or for any reason other than those set out in the following sentence, or (ii) by Copla under clause 11.2 or 11.3 as a result of the Client's breach, the Client shall pay an early termination charge equal to fifty percent (50%) of the fees that would have fallen due for the remainder of the Initial Term. No early termination charge is payable where the Client terminates under clause 3.2, under clause 11.2 as a result of Copla's material breach or insolvency, or under an express right of termination granted to the Client in the applicable Special Terms. The early termination charge shall be invoiced on the effective date of termination and paid in accordance with the payment terms

specified in the OF. The parties agree that the charge reflects the discount granted to the Client in consideration of the committed term and is not a penalty. Clause 7.6 shall apply to each renewal term following expiry of the Initial Term.

7.8. **Commercial terms.** All commercial terms of the Agreement, including fees, rates, discounts, volumes, bands, tiers, included quantities, term lengths, review dates, and payment terms, are set out exclusively in the OF. The Terms and the Special Terms are published by Copla, apply to all Clients, and contain no Client-specific commercial terms. No amount is payable by the Client unless it is set out in the OF or subsequently agreed in writing between the parties, and no Service, deliverable, or activity is included in the fees unless the OF or the applicable Special Terms state that it is included. In the event of any conflict between the OF and any other document forming part of the Agreement in respect of a commercial term, the OF prevails, notwithstanding clause 2.7.

8. Indemnification

8.1. The Client shall indemnify and ensure that Copla will be held harmless from all claims, as well as interests, penalties, reasonable legal and other professional expenses and costs, arising from or related to (i) the Client's breach of obligations under the applicable DPA or applicable data protection laws; and/or (ii) the Client's infringement of Copla and/or third-party intellectual property rights.

9. Disclaimer

9.1. EXCEPT AS EXPRESSLY STATED IN THE AGREEMENT, NEITHER PARTY MAKES ANY REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, STATUTORY, OR IMPLIED. THE SERVICE IS PROVIDED STRICTLY ON AN "AS IS" AND "AS AVAILABLE" BASIS. UNLESS OTHERWISE STATED IN THE AGREEMENT, COPLA MAKES NO REPRESENTATIONS OR WARRANTIES (AND EXPRESSLY DISCLAIMS ANY SUCH REPRESENTATIONS OR WARRANTIES) THAT (I) USE OF THE SERVICE WILL BE SECURE, TIMELY, UNINTERRUPTED OR ERROR-FREE OR OPERATE IN COMBINATION WITH ANY OTHER HARDWARE, SOFTWARE, SYSTEM OR DATA; (II) THE SERVICE WILL MEET CLIENT'S REQUIREMENTS OR EXPECTATIONS; (III) ANY DATA OR REPORTS PROVIDED THROUGH THE SERVICE WILL BE ACCURATE, RELIABLE OR WITHOUT LOSS; OR (IV) ANY SPECIFIC OUTCOME OR RESULT WILL BE ACHIEVED THROUGH USE OF THE SERVICES. ADDITIONAL PRODUCT-

SPECIFIC DISCLAIMERS MAY BE SET OUT IN THE APPLICABLE SPECIAL TERMS. EACH PARTY EXPRESSLY DISCLAIMS ANY OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, STATUTORY, OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, TITLE, MERCHANTABILITY, COURSE OF PERFORMANCE OR USAGE OF TRADE.

10. Limitation of Liability

10.1. EXCEPT AS EXPRESSLY STATED IN THIS SECTION (AND EXCEPT WHERE OTHERWISE PROHIBITED BY LAW IN THE APPLICABLE JURISDICTION), NO PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT LOSSES OR DAMAGE SUFFERED BY THE OTHER PARTY, INCLUDING LOST PROFITS (OR SAVED FUNDS), LOSS OF BUSINESS OPPORTUNITIES, ANY ERRORS OR INTERRUPTION OF USE, LOSS OF DATA OR TECHNOLOGY, INACCURACY OR DESTRUCTION, LOSS OF GOODWILL OR REPUTATIONAL DAMAGE, WHETHER ARISING UNDER CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER BASIS.

10.2. SUBJECT TO THIS CLAUSE, THE TOTAL LIABILITY OF COPLA TO THE CLIENT ARISING UNDER THE AGREEMENT, TORT (INCLUDING NEGLIGENCE) OR OTHER CAUSES THROUGHOUT THE TERM OF THE AGREEMENT SHALL BE LIMITED TO THE GREATER OF: (I) ONE THOUSAND (1,000) EUROS OR (II) THE FEES PAID BY THE CLIENT TO COPLA FOR THE LAST TWELVE (12) MONTH PERIOD PRIOR TO THE OCCURRENCE OF THE EVENT GIVING RISE TO THE CLAIM, PROVIDED THAT IN NO EVENT SHALL COPLA'S TOTAL LIABILITY EXCEED TWENTY THOUSAND (20,000) EUROS IN AGGREGATE.

10.3. THE EXCLUSIONS AND LIMITATIONS SET FORTH IN THIS SECTION AND ELSEWHERE IN THE AGREEMENT SHALL APPLY TO THE EXTENT PERMITTED BY LAW, BUT NEITHER PARTY SHALL LIMIT ITS LIABILITY FOR: (I) DEATH OR PERSONAL INJURY CAUSED BY ITS OR ITS OFFICERS', EMPLOYEES', CONTRACTORS' OR REPRESENTATIVES' NEGLIGENCE WHILE ACTING IN THE COURSE OF THEIR DUTIES; (II) FRAUD OR FRAUDULENT MISREPRESENTATION; (III) PAYMENTS UNDER SECTION 7 (PAYMENTS); OR (IV) ANY OTHER LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

10.4. NOTWITHSTANDING ANY OTHER PROVISION OF THIS CHAPTER 10, COPLA ASSUMES NO RESPONSIBILITY AND SHALL HAVE NO LIABILITY IN RESPECT OF THE AUDIT SERVICES, AS SET OUT IN CLAUSE 2.15. ANY LIABILITY WHICH

CANNOT BE EXCLUDED IS LIMITED IN ACCORDANCE WITH CLAUSE 2.16.

11. Term and Termination

11.1. Unless terminated earlier under the Agreement, the term of the Agreement is specified in the OF ("Initial Term") from the effective date indicated in the OF. Either party may notify the other in writing of the termination of the contract at least 30 (thirty) days before the end of the term. If the Client does not terminate the Agreement at the end of the Initial Term, the Agreement is automatically extended for the same period (the number of such term extensions is unlimited, except where the Client terminates the Agreement in the manner specified therein).

11.2. If a party (i) materially breaches the Agreement and, if such breach is curable, fails to remedy the breach within thirty (30) days of written notice thereof; or (ii) becomes insolvent or ceases its operations, the other party may terminate the Agreement immediately, having notified the other party in writing.

11.3. Copla may immediately and without prior notice suspend or terminate the Client's or Client Affiliate's access to the Copla Platform and Services if, in Copla's reasonable opinion, the Client or Client Affiliate materially breaches the Agreement.

12. Confidential Information

12.1. In the course of providing and receiving services under the Agreement, each party may become privy to the other party's confidential information (hereinafter referred to as "Confidential Information"), including but not limited to specifications, business methods, marketing strategies, pricing, and terms of the Agreement. Confidential Information also means Copla Material and technical documentation that Copla may provide and share with the Client or Client Affiliates throughout the term of the Agreement.

12.2. Information is not considered confidential if it (i) is already known to the recipient or its affiliates without any obligation to keep it confidential; (ii) is or becomes publicly known due to the recipient's or its affiliates' wrongful acts; (iii) is received by the recipient from a third party without any confidentiality restrictions; (iv) is independently developed by the recipient or its affiliates; (v) is disclosed by the disclosing party to third parties without any confidentiality obligations or due to a

valid order, condition, regulation, or law, including in response to a valid legal process, such as a court summons, provided that the responding party informs the party disclosing the Confidential Information at least ten (10) days before such response, including the submission of the legal process (such as a court summons); or (vi) is confirmed to be disclosed with prior written consent of the disclosing party.

12.3. Each party, without the prior written consent of the other party, shall not (i) transfer or otherwise make available any of the other party's Confidential Information to any third party, except to its affiliates, agents, directors, employees, and authorized representatives who need to know such information; provided that the recipient obligates these affiliates, agents, directors, employees, and authorized representatives to adhere to confidentiality obligations at least as strict as those specified in this section; or (ii) use the other party's Confidential Information for any commercial, industrial, or other purposes, except for the use or provision of Services; or (iii) copy, adapt, or otherwise reproduce the other party's Confidential Information, except as necessary to provide Services under the Agreement. All Confidential Information (including all copies or extracts thereof) remains the property of the disclosing party. Upon request by the disclosing party, the recipient shall: a) return such material to the disclosing party or b) destroy and confirm in writing that it has been destroyed.

13. Assignment

The Client may not assign, sublicense, or transfer the Agreement, the Client's account on the Copla Platform, or any right or obligation under the Agreement without Copla's consent. Any assignment, transfer, or attempt to assign or transfer in violation of this section shall be null and void and of no effect. Copla and its subsequent successors may assign, delegate, sublicense, or otherwise transfer the Agreement or any rights or obligations under it, in whole or in part, to any person or entity.

14. Marketing Rights

The Client grants Copla permission to use its name and logo in Copla's sales and marketing materials. The Client may revoke this permission at any time by emailing legal@copla.com.

15. Force Majeure

Neither party shall be liable for delay or failure to perform under the Agreement due to events beyond that party's control ("Force Majeure"). Such Force Majeure events include, but are not limited to, lightning, flood, hurricane, tornado, fire, war, terrorism, decisions or inaction by government authorities, and new legislation. Any party claiming a Force Majeure event shall notify the other party of the occurrence of the Force Majeure event. If Force Majeure circumstances continue for more than thirty (30) days, the party claiming such circumstances shall have the right to terminate the Agreement immediately, notifying the other party in writing. If the Client exercises its right to terminate the Agreement under this section, it shall promptly pay Copla all applicable fees that have accrued, are due, and are payable to Copla under the terms of the Agreement up to the date of such termination.

16. Notices

16.1. Copla may provide notices to the Client, at Copla's discretion, to the email address specified in the OF, or by posting in the Client's account on the Platform, which the Client has access to. The Client must ensure that the email address and any other contact information provided to Copla are updated and correct throughout the term of the Agreement. Changes in the Client's contact information (including email address for invoices) should be sent to the designated Copla representative. The Client may contact Copla via email as specified in the OF.

17. Other Terms

If it is determined that any provision of the Agreement is unenforceable and/or contrary to law, such provision shall be interpreted in a manner that most closely matches the parties' intentions, while the other provisions remain in effect.

18. Applicable Law and Jurisdiction

The Agreement is governed by the laws of the Republic of Lithuania. The Client and Copla agree to the jurisdiction and venue of the courts of the Republic of Lithuania.

RoI Special Terms

Last update: 2026-03-17 Version 1.1

These **RoI Special Terms** apply to the use of the DORA RoI Product (as defined below) and form a legally binding Agreement between the Client and Copla, in addition to the Terms.

In the event of any conflict or inconsistency between these RoI Special Terms and the Terms, these RoI Special Terms shall prevail in respect of the Product described herein.

1. Definitions

Unless otherwise defined herein, capitalized terms shall have the meaning ascribed to them in the Terms.

- **DORA RoI Product** means the web-based SaaS application, a web-based SaaS tool that helps financial entities meet their DORA Registry of Information ("RoI") obligations under **Regulation (EU) 2022/2554** ("DORA"). The Product guides users through structured data entry across all required ICT third-party service relationships — covering contractual details, service criticality, provider profiles, and sub-outsourcing chains — and generates a compliant, regulator-ready export of the 16 CSV tables required for NCA submission.
- **RoI** refers to the Registry of Information as mandated under Articles 28 and 29 of DORA and associated guidance issued by the European Supervisory Authorities (ESAs).
- **Client** means a financial entity subject to RoI reporting obligations under DORA and legally entitled to use the Product for regulatory compliance purposes.

2. Scope of Product

2.1 The Product is intended exclusively for professional use by Clients regulated under DORA for the purpose of compiling and maintaining ICT third-party risk information, including but not limited to:

- Company structure, branches, and arrangements;
- ICT third-party service provider profiles and service mapping;

- Contractual data, including service criticality, pricing, audit arrangements, and contingency providers.

2.2 The Product generates a structured export of 16 CSV-formatted tables intended for import into national competent authority (NCA) systems. The Client is solely responsible for validating, submitting, and maintaining such exports in accordance with applicable regulatory requirements.

3. Regulatory Use Limitation

3.1 The Product is made available solely for lawful use in compliance with DORA and related ICT risk management obligations.

3.2 Copla does not guarantee regulatory compliance or legal sufficiency of the information submitted via the Product and does not provide legal or supervisory advice in connection with RoI content or DORA obligations. Copla guarantees that:

a) the Product shall include all data fields and reporting templates as mandated by the regulators and applicable legislation;

b) the Product's export functionality will generate files in the proper technical format required by regulators

c) Provider shall update any technical specifications of Product without delay to reflect any changes in regulatory reporting requirements.

4. Data Input and Responsibility

4.1 The Client remains fully responsible for the accuracy, completeness, and timeliness of all data entered into the Product.

4.2 Copla will not be liable for any failure by the Client to comply with RoI reporting deadlines or requirements, nor for any regulatory action taken against the Client as a result of incorrect or incomplete data entry.

5. Data Access and Confidentiality

5.1 Subject to applicable law, all data submitted to the Product and all output files remain the sole property of the Client.

5.2 Copla shall process such data strictly in accordance with its role as service provider and in line with applicable data protection and confidentiality obligations.

5.3 Copla shall not access, transmit, or disclose such data to third parties, unless authorized by the Client or required by applicable law or supervisory authority.

6. Security and Availability

6.1 Copla shall implement reasonable and proportionate technical and organizational measures to ensure availability, integrity, and resilience of the Product, consistent with its obligations under DORA and applicable security standards.

6.2. Copla shall:

(a) Provide assistance to the Client in the event of an ICT incident related to the Product at no additional cost.

(b) Grant the Client, its appointed auditors, and any relevant National Competent Authority (NCA) or other supervisory authority (including the European Supervisory Authorities) full rights of access, inspection, and audit of Copla's business premises, systems, processes, and data records related to the Product and its delivery. Such access shall be provided: (i) on reasonable prior written notice for scheduled audits; and (ii) without prior notice where required by a supervisory authority or in the event of a suspected serious incident. Copla shall cooperate fully and at no additional cost with any such audit or inspection, including by making relevant personnel available and providing copies of documentation upon request.

(c) Ensure that ICT services are hosted and data is processed exclusively within the European Economic Area (EEA). Copla confirms that the primary ICT services and data storage are provided from Frankfurt, Germany. In accordance with DORA Art. 30(2)(b), Copla shall notify the Client at least thirty (30) days in advance of any planned changes to the locations of data processing or storage, or any changes to sub-processors involved in the delivery of the Product.

6.3. Incident Notification: Copla shall notify the Client without undue delay, and in any event within 24 hours, of any ICT-related incident or security breach that may affect the availability, integrity, or confidentiality of the Client's Registry of Information data.

7. Termination and Data Retention

7.1 Upon termination of the Client's Subscription Plan or access to the Product or in the event of discontinuation of Copla's business operations, insolvency, or resolution, the Client shall be provided with a thirty (30) day grace period to export all data and output files. During this period, Copla (or its liquidator/legal successor) guarantees access, recovery, and return of all personal and non-personal data in an easily accessible, structured, and machine-readable format.

7.2 After expiry of the grace period, Copla shall delete or anonymize all Client Data associated with the Product, unless retention is required by law or the Terms. Before any permanent deletion or anonymization of data, Copla shall send a written notice to the Client at least thirty (30) days in advance, confirming that the data is ready for final export and that the Client has no further objections to the deletion.

8. Jurisdiction and Applicability

8.1 These RoI Special Terms apply only to Clients who are obligated to maintain a Registry of Information under DORA and who subscribe to the DORA RoI Product.

8.2 These terms do not apply to the use of any other Copla Services.

9. General

9.1 All matters not expressly governed by these RoI Special Terms shall be subject to the Terms.

9.2 The RoI Special Terms may be updated from time to time in accordance with the change procedure defined in the Terms.

9.3. Right to Audit: The Client or an appointed third party may conduct an audit of Copla's ICT security measures once per year or upon a suspected breach.

9.4. Copla undertakes to notify the Client of any Product updates or revisions that affect the data fields or export functionality, ensuring they do not disrupt our historical data or compliance status.

10. Subcontracting

10.1 Copla shall not subcontract or delegate to any third party the performance of any part of the Product or its underlying ICT services without the prior written consent of the Client. Where the Client provides consent, Copla shall: (a) ensure that any subcontractor is bound by contractual obligations no less protective than those set out in these RoI Special Terms and the Terms, including in relation to data confidentiality, security, and audit rights; and (b) remain fully liable to the Client for the performance of any subcontracted obligations.

10.2 Copla shall maintain and make available to the Client upon request an up-to-date list of all subcontractors and sub-processors engaged in the delivery of the Product, including their names, registered addresses, and the nature of services provided. Copla shall notify the Client in writing at least thirty (30) days in advance of any intended change to its subcontractors, and the Client shall have the right to object to any such change on reasonable grounds. Where the Client objects, the parties shall work in good faith to resolve the matter; if no resolution is reached, the Client may terminate the Agreement with no penalty.

11. Business Continuity and Exit Provisions

11.1 Copla shall maintain and regularly test a documented business continuity plan ("BCP") and disaster recovery plan ("DRP") for the Product, consistent with the requirements of DORA and applicable ICT risk management standards. Copla shall make a summary of such plans available to the Client upon request, and shall notify the Client within ten (10) business days of any material change to the BCP or DRP.

11.2 In the event of a significant disruption to the Product, Copla shall: (a) activate its BCP and DRP without undue delay; (b) notify the Client within four (4) hours of the disruption; (c) provide regular status updates at least every eight (8) hours until service is restored; and (d) provide a written root-cause analysis and remediation report within fifteen (15) business days following restoration of service.

11.3 Exit and Transition Assistance: Upon expiry or termination of these RoI Special Terms for any reason, in addition to the data return obligations, Copla shall: (a) provide reasonable transition assistance to the Client or any replacement provider nominated by the Client for a period of up to ninety (90) days following the effective date of termination, at the Client's request and at rates agreed in

advance; (b) ensure that no action is taken that would impair or hinder the Client's ability to migrate its data or continue its DORA reporting obligations; and (c) co-operate with the Client's reasonable requests to transfer configurations, data schemas, and documentation to facilitate continuity of service.

12. Termination for Regulatory Non-Compliance

12.1 Notwithstanding any other termination provisions in these RoI Special Terms or the Terms, the Client shall have the right to terminate this Agreement with immediate effect, by written notice to Copla, if: (a) Copla's acts or omissions cause or materially risk a breach by the Client of its obligations under DORA or any applicable regulatory requirement; (b) a competent supervisory authority or resolution authority directs or recommends that the Client terminate the arrangement with Copla; (c) Copla suffers an insolvency event, appointment of an administrator, or ceases to carry on business; or (d) Copla materially and persistently fails to remedy a breach of these RoI Special Terms within ten (10) business days of written notice from the Client.

12.2 Where the Client exercises its right of immediate termination under clause 12.1, no termination fee, break penalty, or other financial consequence shall be payable by the Client.

MTP Register Special Terms

Last update: 2026-08-25 Version 1.0

These **MTP Register Special Terms** ("**MTP Special Terms**") apply to the use of the MTP Register Product (as defined below) and form a legally binding Agreement between the Client and Copla, in addition to the Terms.

In the event of any conflict or inconsistency between these MTP Special Terms and the Terms, these MTP Special Terms shall prevail in respect of the Product described herein, in accordance with clause 2.7 of the Terms.

These MTP Special Terms apply where the OF identifies the MTP Register as a Service subscribed to by the Client. Where the Client also subscribes to other Copla products, the corresponding Special Terms (including, as applicable, the RoI Special Terms, the IR Special Terms, and the EBA Special Terms) apply concurrently in accordance with clause 2.7 of the Terms.

1. Definitions

Unless otherwise defined herein, capitalised terms shall have the meaning ascribed to them in the Terms, the OF, the DPA, or the SLA.

- **FCA** means the United Kingdom Financial Conduct Authority; **PRA** means the Prudential Regulation Authority; and **BoE** means the Bank of England.
- **PS26/2** means FCA Policy Statement PS26/2 (Operational incident and third party reporting), published on 18 March 2026 following Consultation Paper CP24/28, together with the rules it introduces into the FCA Handbook (including SUP 15.19 and SUP 16.33), the accompanying Finalised Guidance FG26/3 and FG26/4, and any successor, amending, or replacement rules, guidance, or reporting templates. The rules introduced by PS26/2 come into force on 18 March 2027.
- **Material Third Party Arrangement** or **MTPA** means a third party arrangement which meets the definition of a material third party arrangement in the FCA Handbook, as further explained in FG26/4.
- **MTP Register** means the register of Material Third Party Arrangements which an in-scope firm is required to maintain and to submit to the FCA annually under PS26/2.

- **Reference Date** means 31 December of the calendar year to which an MTP Register submission relates, being the date as at which the register is required to be accurate.
- **Submission Window** means the period of ninety (90) calendar days from the date on which the FCA opens the annual reporting window for submission of the MTP Register.
- **Reporting Templates** means the register template and the separate notification template published by the FCA under PS26/2 and FG26/4, and any successor or replacement templates.
- **Product** means the web-based SaaS application branded as **MTP Register**, a tool that assists firms regulated in the United Kingdom in identifying, assessing, recording, and maintaining information on their third party arrangements, in preparing notifications of new or significantly changed Material Third Party Arrangements, and in generating a structured, regulator-ready export of the annual MTP Register in the format required by the Reporting Templates.
- **Client** means a firm which is subject to the third party reporting requirements introduced by PS26/2 (including, as applicable, enhanced scope SM&CR firms, banks, building societies, designated investment firms, Solvency II firms, CASS large firms, authorised electronic money institutions and authorised payment institutions, and consolidated tape providers) and which is legally entitled to use the Product for regulatory compliance purposes.
- **Client Data** means all information, documentation, and data submitted, uploaded, or generated by the Client or its authorised users within the Product, including third party profiles, materiality assessments, contractual data, notifications, and register entries and exports.
- **Subscription Plan** means the plan selected by the Client under the applicable OF, which determines the modules, features, and usage limits available to the Client under these MTP Special Terms.

2. Scope of Product

2.1 The Product is intended exclusively for professional use by Clients subject to PS26/2 for the purpose of compiling, assessing, and maintaining information on their third party arrangements, including but not limited to:

- identification of third party arrangements and assessment of materiality against the definition in the FCA Handbook and the factors set out in FG26/4, Chapter 3, including capture of the reasoning and evidence supporting each determination;
- structured data collection on third party providers and arrangements, including provider identity and identifiers, the products and services provided, contractual terms and key dates, locations of service provision and data storage, sub-contracting chains and external dependencies, intra-group arrangements, and substitutability and exit arrangements;
- mapping of Material Third Party Arrangements to the Client's important business services for the purposes of SYSC 15A;
- preparation of notifications of new Material Third Party Arrangements and of significant changes to existing arrangements;
- maintenance of the MTP Register on an ongoing basis and preparation of the annual submission as at the Reference Date.

2.2 The Product generates structured exports in the format of the Reporting Templates. Consistent with FG26/4, the register export and the notification export are generated as separate outputs serving different purposes. The Client is solely responsible for validating, submitting, and maintaining such exports in accordance with applicable regulatory requirements.

2.3 The Product does not constitute a direct interface with the FCA, the PRA, the BoE, or any other authority. All notifications and register submissions must be made by the Client through the relevant official channels, including the shared reporting portal operated by the regulators.

2.4 Where the Client is a dual-regulated firm, the Product supports the preparation of a single set of data capable of supporting one submission to the FCA and the PRA in accordance with PS26/2 and PRA Policy Statement PS7/26. The Client remains solely responsible for determining which regulatory requirements apply to it.

2.5 The Product retains a point-in-time record of the MTP Register as at each Reference Date, together with a versioned audit trail of changes to Client Data, so as to enable the Client to evidence the accuracy of its submission and to respond to supervisory enquiries.

2.6 The specific modules and features available to the Client depend on the Subscription Plan selected in the OF. Service levels, availability commitments, and support response times are governed by the SLA.

3. Regulatory Use Limitation

3.1 The Product is made available solely for lawful use in connection with the Client's obligations under PS26/2 and related operational resilience, outsourcing, and third party risk management requirements, including SYSC 8 and SYSC 15A.

3.2 Copla does not guarantee regulatory compliance or legal sufficiency of the information maintained, notified, or submitted via the Product, and does not provide legal or supervisory advice in connection with PS26/2 obligations. Copla guarantees that:

a) the Product shall include all data fields and reporting structures mandated by the FCA rules and the Reporting Templates applicable to Material Third Party Arrangements and to the MTP Register;

b) the Product's export functionality will generate files in the technical format required by the FCA for notifications and for the annual register submission, to the extent such formats are published and in force;

c) Copla shall update the Product without undue delay to reflect any change in the applicable rules, guidance, technical standards, or Reporting Templates, and shall in any event ensure that the Product supports the requirements in force from 18 March 2027 in advance of that date.

3.3 Any materiality assessment, classification, scoring, or recommendation generated or supported by the Product constitutes decision support only. All determinations as to whether a third party arrangement is material, and all notification and submission decisions, remain the sole responsibility of the Client.

4. Data Input and Responsibility

4.1 The Client remains fully responsible for the accuracy, completeness, and timeliness of all data entered into the Product, including all information relating to its third party providers, contractual arrangements, materiality assessments, and dependencies.

4.2 The Client is solely responsible for observing the regulatory timescales applicable to it, including notifying the FCA of new or significantly changed Material Third Party Arrangements sufficiently early in its decision-making process, and submitting its MTP Register within the Submission Window, accurate as at the Reference Date.

4.3 Copla shall not be liable for any failure by the Client to comply with notification or reporting deadlines or requirements, nor for any regulatory action, supervisory measure, or sanction taken against the Client as a result of incorrect, incomplete, or untimely data entry, notification, or submission.

4.4 The Client shall ensure that all data entered into the Product is consistent with its actual third party arrangements and is maintained and updated on an ongoing basis to reflect any change.

5. Data Access and Confidentiality

5.1 Subject to applicable law, all Client Data submitted to the Product and all output files remain the sole property of the Client.

5.2 Copla shall process such data strictly in accordance with its role as service provider and in line with applicable data protection and confidentiality obligations, including the UK GDPR, the Data Protection Act 2018, and the DPA.

5.3 Copla shall not access, transmit, or disclose such data to third parties, unless authorised by the Client or required by applicable law or a supervisory authority. Where Copla is required by law to disclose Client Data, it shall, to the extent legally permitted, notify the Client in advance.

6. Security and Availability

6.1 Copla shall implement reasonable and proportionate technical and organisational measures to ensure the availability, integrity, confidentiality, and resilience of the Product, consistent with applicable security standards and with the operational resilience expectations applicable to the Client under SYSC 15A.

6.2 Copla shall:

(a) provide assistance to the Client in the event of an ICT or operational incident related to the Product at no additional cost, including such information as the Client reasonably requires in order to assess whether the incident is reportable under PS26/2 and FG26/3;

(b) grant the Client, its appointed auditors, and the FCA, the PRA, the BoE, and any other relevant supervisory or resolution authority full rights of access, inspection, and audit of Copla's business premises, systems, processes, and data records related to the Product and its delivery, on reasonable prior written notice for scheduled audits, or without prior notice where required by a supervisory authority or in the event of a suspected serious incident; Copla shall cooperate fully and at no additional cost with any such audit, inspection, or information request;

(c) ensure that the Product is hosted and Client Data is processed exclusively within the European Economic Area (EEA) or the United Kingdom, Copla confirming that the primary ICT services and data storage are provided from Frankfurt, Germany, and notify the Client at least thirty (30) days in advance of any planned change to the locations of data processing or storage, or to any sub-processors involved in the delivery of the Product.

6.3 Incident Notification: Copla shall notify the Client without undue delay, and in any event within twenty-four (24) hours, of any ICT-related incident or security breach that may affect the availability, integrity, or confidentiality of the Client's MTP Register data. Such notification shall include sufficient information to enable the Client to assess and, where required, to discharge its own operational incident reporting obligations under PS26/2.

6.4 Copla confirms that, as at the date of these MTP Special Terms, it has not been designated as a critical third party under the critical third parties regime in the Financial Services and Markets Act 2000 (as amended). Copla shall notify the Client without undue delay if it becomes so designated.

7. Support for the Client's Own Reporting Obligations

7.1 The Parties acknowledge that Copla's provision of the Product may itself constitute a third party arrangement of the Client and may, depending on the Client's own materiality assessment, constitute a Material Third Party Arrangement

requiring notification to the FCA and inclusion in the MTP Register submitted by the Client.

7.2 Copla shall provide to the Client, at no additional cost, all information within its control which the Client reasonably requires in order to notify the arrangement and to complete the Reporting Templates in respect of Copla, including: Copla's legal entity name, registered address, registration number, and legal entity identifier (where held); a description of the products and services provided; the contractual start date, term, and notice periods; the countries and locations from which the services are provided and in which Client Data is stored; details of Copla's sub-contractors and sub-processors and of any onward chain of external dependency; the assurance, certification, and audit reports held by Copla; and information relevant to substitutability, exit, and business continuity.

7.3 Copla shall provide the information referred to in clause 7.2 within ten (10) business days of the Client's written request, and shall notify the Client of any change to that information within thirty (30) days and in any event in sufficient time to enable the Client to notify a significant change to the arrangement to the FCA.

7.4 Copla shall cooperate promptly and at no additional cost with any request for information, clarification, or engagement made by the FCA, the PRA, or the BoE in connection with the arrangement, and shall support the Client in responding to any such request.

7.5 Copla shall not act, or omit to act, in a manner which it knows or ought reasonably to know would prevent the Client from complying with SYSC 8, SYSC 15A, or the requirements introduced by PS26/2.

8. Termination and Data Retention

8.1 Upon termination of the Client's Subscription Plan or access to the Product, or in the event of discontinuation of Copla's business operations, insolvency, or resolution, the Client shall be provided with a thirty (30) day grace period to export all Client Data and output files, in accordance with clause 2.8 of the Terms. During this period, Copla (or its liquidator or legal successor) guarantees access, recovery, and return of all personal and non-personal data in a structured, commonly used, and machine-readable format.

8.2 After expiry of the grace period, Copla shall delete or anonymise all Client Data associated with the Product in accordance with clause 2.9 of the Terms, unless retention is required by applicable law or the DPA. Before any permanent deletion or anonymisation of Client Data, Copla shall provide the Client with at least thirty (30) days' prior written notice, confirming that the data remains available for export and requesting the Client's confirmation that it has no further objections to the deletion.

8.3 The Product shall enable the Client to export and retain each submitted MTP Register, together with the underlying materiality assessments and audit trail, for the period for which the Client is required to retain such records under applicable regulatory requirements.

9. Jurisdiction and Applicability

9.1 These MTP Special Terms apply only to Clients which are subject to third party reporting requirements under PS26/2 and which subscribe to the MTP Register Product under the OF.

9.2 These MTP Special Terms do not apply to the use of any other Copla products or services.

9.3 The Agreement is governed by the law specified in Chapter 18 of the Terms, unless the Parties expressly agree otherwise in the OF. Nothing in these MTP Special Terms limits or excludes any power or right of the FCA, the PRA, or the BoE arising under applicable law.

9.4 Save as set out in clauses 6.2(b) and 9.3, a person who is not a party to the Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms.

10. General

10.1 All matters not expressly governed by these MTP Special Terms shall be subject to the Terms.

10.2 These MTP Special Terms may be updated from time to time in accordance with the amendment procedure set out in Chapter 3 of the Terms.

10.3 Right to Audit: The Client or an appointed third party may conduct an audit of Copla's ICT security measures relevant to the Product once per calendar year, at any time following a suspected or actual security breach affecting Client Data, or where required by a supervisory authority.

10.4 Copla undertakes to notify the Client of any Product update or revision affecting the data fields, reporting structures, or export functionality required for PS26/2 compliance, ensuring that such updates do not disrupt historical Client Data or previously submitted registers. Copla shall not deploy material changes to the export functionality during a Submission Window without the Client's prior agreement, save where required in order to correct an error or to comply with a regulatory requirement.

10.5 These MTP Special Terms shall be read in conjunction with the Terms, the OF, the DPA, and the SLA, which together constitute the Agreement.

11. Subcontracting

11.1 Copla shall not subcontract or delegate to any third party the performance of any part of the Product or its underlying ICT services without the prior written consent of the Client. Where the Client provides consent, Copla shall: (a) ensure that any subcontractor is bound by contractual obligations no less protective than those set out in these MTP Special Terms and the Terms, including in relation to data confidentiality, security, and audit rights; and (b) remain fully liable to the Client for the performance of any subcontracted obligations.

11.2 Copla shall maintain and make available to the Client upon request an up-to-date list of all subcontractors and sub-processors engaged in the delivery of the Product, including their names, registered addresses, the nature of the services provided, and the countries from which those services are provided, in a form which enables the Client to record the onward chain of dependency in its MTP Register. Copla shall notify the Client in writing at least thirty (30) days in advance of any intended change to its subcontractors, and the Client shall have the right to object to any such change on reasonable grounds, including where the change would require the Client to notify a significant change to the FCA. Where the Client objects, the Parties shall work in good faith to resolve the matter; if no resolution is reached, the Client may terminate the Agreement with no penalty.

12. Business Continuity and Exit Provisions

12.1 Copla shall maintain and regularly test a documented business continuity plan ("BCP") and disaster recovery plan ("DRP") for the Product, consistent with applicable ICT risk management standards and with the operational resilience expectations applicable to the Client. Copla shall make a summary of such plans available to the Client upon request, and shall notify the Client within ten (10) business days of any material change to the BCP or DRP.

12.2 In the event of a significant disruption to the Product, Copla shall: (a) activate its BCP and DRP without undue delay; (b) notify the Client within four (4) hours of the disruption; (c) provide regular status updates at least every eight (8) hours until service is restored; and (d) provide a written root-cause analysis and remediation report within fifteen (15) business days following restoration of service.

12.3 Copla shall use all reasonable endeavours to ensure the availability of the Product throughout each Submission Window and shall not schedule planned maintenance during a Submission Window where this could reasonably be expected to prejudice the Client's ability to submit its MTP Register on time.

12.4 Exit and Transition Assistance: Upon expiry or termination of these MTP Special Terms for any reason, in addition to the data return obligations set out in Chapter 8 and in clauses 2.8 to 2.10 of the Terms, Copla shall: (a) provide reasonable transition assistance to the Client or to any replacement provider nominated by the Client for a period of up to ninety (90) days following the effective date of termination, at the Client's request and at rates agreed in advance; (b) ensure that no action is taken which would impair or hinder the Client's ability to migrate its data or to continue to discharge its notification and MTP Register reporting obligations under PS26/2; and (c) co-operate with the Client's reasonable requests to transfer configurations, data schemas, and documentation in order to facilitate continuity of service.

13. Termination for Regulatory Non-Compliance

13.1 Notwithstanding any other termination provisions in these MTP Special Terms or the Terms, the Client shall have the right to terminate this Agreement with immediate effect, by written notice to Copla, if: (a) Copla's acts or omissions cause or materially risk a breach by the Client of its obligations under PS26/2 or any other applicable regulatory requirement; (b) the FCA, the PRA, the BoE, or any

other competent supervisory or resolution authority directs or recommends that the Client terminate the arrangement with Copla; (c) Copla suffers an insolvency event, appointment of an administrator, or ceases to carry on business; or (d) Copla materially and persistently fails to remedy a breach of these MTP Special Terms within ten (10) business days of written notice from the Client.

13.2 Where the Client exercises its right of immediate termination under clause 13.1, no termination fee, break penalty, or other financial consequence shall be payable by the Client.

Incident Register Special Terms

Last update: 2026-03-17 Version 1.0

These **Incident Register Special Terms** apply to the use of the DORA Incident Register Product (as defined below) and form a legally binding agreement between the Customer and Copla (the “Provider”), in addition to the Provider’s General Terms and Conditions (“General Terms”).

In the event of any conflict or inconsistency between these Incident Register Special Terms and the General Terms, these Incident Register Special Terms shall prevail in respect of the Product described herein.

1. Definitions

Unless otherwise defined herein, capitalized terms shall have the meaning ascribed to them in the General Terms.

- **Product** means the web-based SaaS application branded as **DORA Incident Register**, made available by the Provider to facilitate the input, management, classification, and export of major ICT-related incident data as required under **Regulation (EU) 2022/2554** (“DORA”).
- **Incident Register** refers to the register of ICT-related incidents and significant cyber threats that financial entities are required to maintain pursuant to Article 19 of DORA and associated guidance issued by the European Supervisory Authorities (ESAs).
- **Major ICT Incident** means an ICT-related incident of a significant nature as classified in accordance with the criteria established under Articles 18 and 19 of DORA and the relevant regulatory technical standards (RTS) issued by the ESAs.
- **Incident Report** means the initial, intermediate, and final reports required to be submitted to the national competent authority (NCA) as prescribed under Article 19 of DORA.
- **Customer** means a financial entity subject to DORA incident reporting obligations under DORA and legally entitled to use the Product for regulatory compliance purposes.

2. Scope of Product

2.1 The Product is intended exclusively for professional use by Customers regulated under DORA for the purpose of recording, classifying, and reporting ICT-related incidents, including but not limited to:

- Incident recording and structured data entry aligned with DORA reporting templates;
- Classification based on DORA severity criteria and applicable RTS thresholds;
- Generation and export of initial, intermediate, and final Incident Reports in the format mandated by the relevant NCA;
- Maintenance of a searchable and auditable internal Incident Register.

2.2 The Product generates structured, regulator-ready Incident Reports and supporting documentation for submission to the relevant NCA. The Customer is solely responsible for validating, submitting, and maintaining such reports in accordance with applicable regulatory requirements and prescribed timelines.

2.3 The Product does not constitute legal advice and does not replace the Customer's own obligation to assess, classify, and report incidents in accordance with DORA and relevant RTS.

3. Regulatory Use Limitation

3.1 The Product is made available solely for lawful use in compliance with DORA and related ICT incident reporting and management obligations.

3.2 The Provider does not guarantee regulatory compliance or legal sufficiency of the information submitted via the Product and does not provide legal or supervisory advice in connection with incident content or DORA obligations. The Provider guarantees that:

a) the Product shall include all data fields and reporting templates as mandated by the applicable legislation and regulators, including all three phases of reporting (initial, intermediate, and final) as required under DORA Article 19;

b) the Product's export functionality will generate Incident Reports in the proper technical format and structure required by the relevant NCA;

c) the Provider shall update any technical specifications of the Product without delay to reflect any changes in regulatory reporting requirements, including changes arising from updated ESA guidance or revised RTS.

4. Data Input and Responsibility

4.1 The Customer remains fully responsible for the accuracy, completeness, and timeliness of all data entered into the Product, including the correct classification of incidents as major ICT incidents in accordance with DORA.

4.2 The Provider will not be liable for any failure by the Customer to comply with DORA incident reporting deadlines or requirements, nor for any regulatory action taken against the Customer as a result of incorrect, incomplete, or late data entry.

4.3 The Customer acknowledges that statutory reporting deadlines under DORA (including the initial report within 4 hours of classification and the final report within 1 month) are the Customer's sole responsibility, and the Product is a tool to facilitate — but not substitute — such reporting.

5. Data Access and Confidentiality

5.1 Subject to applicable law, all data submitted to the Product and all output files remain the sole property of the Customer.

5.2 The Provider shall process such data strictly in accordance with its role as service provider and in line with applicable data protection and confidentiality obligations.

5.3 The Provider shall not access, transmit, or disclose such data to third parties, unless authorised by the Customer or required by applicable law or supervisory authority.

5.4 Given the sensitive and time-critical nature of incident data, the Provider shall ensure that all data submitted by the Customer is stored and processed exclusively within the European Economic Area (EEA) and is protected by appropriate encryption at rest and in transit.

6. Security and Availability

6.1 The Provider shall implement reasonable and proportionate technical and organisational measures to ensure availability, integrity, and resilience of the Product, consistent with its obligations under DORA and applicable security standards.

6.2 Given that the Product is used in connection with time-sensitive regulatory reporting, the Provider shall make best efforts to maintain service availability at all times, and shall notify the Customer without undue delay of any planned or unplanned outages that may affect the Customer's ability to submit Incident Reports within regulatory deadlines.

6.3. The Provider shall:

(a) Provide assistance to the Customer in the event of an incident related to the Product at no additional cost.

(b) Grant the Customer and its National Competent Authority (NCA) full rights of access, inspection, and audit to the Provider's business premises and data records related to the Service.

(c) Ensure that ICT services are hosted and data is processed exclusively within the European Economic Area (EEA). The Provider confirms that the primary ICT services and data storage are provided from Frankfurt, Germany. In accordance with DORA Art. 30(2)(b), the Provider shall notify the Customer at least thirty (30) days in advance of any planned changes to the locations of data processing or storage, or any changes to sub-processors involved in the delivery of the Product.

6.4. Incident Notification: The Provider shall notify the Customer without undue delay, and in any event within 24 hours, of any ICT-related incident or security breach that may affect the availability, integrity, or confidentiality of the Customer's incident register data.

7. Termination and Data Retention

7.1 Upon termination of the Customer's Subscription Plan or access to the Product or in the event of discontinuation of the Provider's business operations, insolvency, or resolution, the Customer shall be provided with a thirty (30) day grace period to

export all data and output files. During this period, the Provider (or its liquidator/legal successor) guarantees access, recovery, and return of all personal and non-personal data in an easily accessible, structured, and machine-readable format.

7.2 After expiry of the grace period, the Provider shall delete or anonymise all Customer Data associated with the Product, unless retention is required by law or the General Terms. Before any permanent deletion or anonymisation of data, the Provider shall send a written notice to the Customer at least thirty (30) days in advance, confirming that the data is ready for final export and that the Customer has no further objections to the deletion.

7.3 The Customer acknowledges that applicable law or regulatory requirements may impose independent retention obligations on incident data. Nothing in these terms limits or waives the Customer's own statutory data retention obligations under DORA or any other applicable law.

8. Jurisdiction and Applicability

8.1 These Incident Register Special Terms apply only to Customers who are obligated to maintain and submit an ICT incident register under DORA and who subscribe to the DORA Incident Register Product.

8.2 These terms do not apply to the use of any other Copla products or services, including the DORA RoI Product, which is governed by its own separate Special Terms.

9. General

9.1 All matters not expressly governed by these Incident Register Special Terms shall be subject to the General Terms.

9.2 The Incident Register Special Terms may be updated from time to time in accordance with the change procedure defined in the General Terms. The Provider shall provide the Customer with at least thirty (30) days' prior written notice of any material changes. If the Customer does not agree with the proposed changes, the Customer shall have the right to terminate the Agreement by providing written notice to the Provider before the changes take effect.

9.3. Right to Audit: The Customer or an appointed third party may conduct an audit of the Provider's ICT security measures once per year or upon a suspected breach, with a minimum of five (5) business days' prior written notice.

9.4. The Provider undertakes to designate responsible persons to participate in ICT security awareness programmes and digital resilience training provided by the Customer, if required and requested by the Customer.

9.5. The Provider undertakes to notify the Customer of any Product updates or revisions that affect the data fields, classification logic, or export functionality, ensuring they do not disrupt historical incident data or the Customer's compliance status.

9.6. These Incident Register Special Terms shall be read in conjunction with, and are supplementary to, the RoI Special Terms where the Customer subscribes to both the DORA RoI Product and the DORA Incident Register Product. In the event of conflict between the two sets of Special Terms, the Incident Register Special Terms shall prevail in respect of incident reporting.

EBA Register Special Terms

Last update: 2026-03-23 Version 1.0

These **EBA Register Special Terms** apply to the use of the EBA Register Product (as defined below) and form a legally binding Agreement between the Client and Copla, in addition to the Terms.

In the event of any conflict or inconsistency between these EBA Register Special Terms and the Terms, these EBA Register Special Terms shall prevail in respect of the Product described herein.

1. Definitions

Unless otherwise defined herein, capitalised terms shall have the meaning ascribed to them in the Terms.

- **Product** means the web-based SaaS application branded as **EBA Register**, a tool that assists financial entities subject to DORA in collecting, structuring, and maintaining the information required to support the European Banking Authority's (EBA's) and the European Supervisory Authorities' (ESAs') oversight register of critical ICT third-party service providers (**CTPP Register**) under **Regulation (EU) 2022/2554** ('DORA'). The Product enables the Client to manage and maintain the required data on its ICT third-party service providers, map them against the applicable DORA criticality and materiality criteria, and prepare the structured information required for submission or reporting to the relevant supervisory authority.
- **EBA Register** refers to the register of critical ICT third-party service providers established and maintained by the European Supervisory Authorities (ESAs) pursuant to Article 28(3) of DORA, and any associated reporting, notification, or data-submission obligations imposed on financial entities thereunder.
- **Client** means a financial entity subject to DORA and legally entitled to use the Product for regulatory compliance purposes.
- **Client Data** means all information, documentation, and data submitted or uploaded by the Client or its authorised users to the Product.

2. Scope of Product

2.1 The Product is intended exclusively for professional use by Clients regulated under DORA for the purpose of identifying, assessing, and maintaining information on their ICT third-party service providers relevant to the EBA Register obligations, including but not limited to:

- identification and classification of ICT third-party service providers against DORA criticality and materiality thresholds;
- structured data collection on ICT provider relationships, contractual arrangements, and service dependencies;
- mapping of ICT services to the applicable DORA regulatory categories and reporting fields;
- preparation and maintenance of data required for supervisory reporting or submission in connection with the EBA Register.

2.2 The Client is solely responsible for validating, submitting, and maintaining all data and reports in accordance with the applicable regulatory requirements and any instructions issued by the competent supervisory authority or the ESAs.

2.3 The Product does not constitute a direct interface with any supervisory authority system. Any data submission to a competent authority or the ESAs must be carried out by the Client through the relevant official channels.

3. Regulatory Use Limitation

3.1 The Product is made available solely for lawful use in connection with the Client's obligations under DORA and related ICT risk management and supervisory reporting requirements.

3.2 Copla does not guarantee regulatory compliance or legal sufficiency of the information maintained or submitted via the Product, and does not provide legal or supervisory advice in connection with EBA Register obligations. Copla guarantees that:

a) the Product shall include all data fields and reporting structures as mandated by DORA and the applicable technical standards and guidelines issued by the ESAs in respect of the EBA Register;

b) the Product's data export and reporting functionality will generate outputs in the technical format required by the relevant competent authority or the ESAs, to the extent such formats are published and in force;

c) Copla shall update the Product without undue delay to reflect any changes in regulatory reporting requirements, technical standards, or data templates applicable to the EBA Register.

4. Data Input and Responsibility

4.1 The Client remains fully responsible for the accuracy, completeness, and timeliness of all data entered into the Product, including all information relating to its ICT third-party service providers, contractual arrangements, and service classifications.

4.2 Copla shall not be liable for any failure by the Client to comply with EBA Register reporting deadlines or requirements, nor for any regulatory action, supervisory measure, or sanction taken against the Client as a result of incorrect, incomplete, or untimely data entry or submission.

4.3 The Client shall ensure that all data entered into the Product is consistent with its actual ICT third-party arrangements and that it is maintained and updated on an ongoing basis to reflect any changes.

5. Data Access and Confidentiality

5.1 Subject to applicable law, all data submitted to the Product and all output files remain the sole property of the Client.

5.2 Copla shall process such data strictly in accordance with its role as service provider and in line with applicable data protection and confidentiality obligations, including the Data Processing Agreement.

5.3 Copla shall not access, transmit, or disclose such data to third parties, unless authorised by the Client or required by applicable law or supervisory authority.

6. Security and Availability

6.1 Copla shall implement reasonable and proportionate technical and organisational measures to ensure the availability, integrity, and resilience of the Product, consistent with its obligations under DORA and applicable security standards.

6.2 Copla shall:

- (a) provide assistance to the Client in the event of an ICT incident related to the Product at no additional cost;
- (b) grant the Client, its appointed auditors, and any relevant competent supervisory authority or the ESAs full rights of access, inspection, and audit of Copla's business premises, systems, processes, and data records related to the Product and its delivery, on reasonable prior written notice for scheduled audits, or without prior notice where required by a supervisory authority or in the event of a suspected serious incident; Copla shall cooperate fully and at no additional cost with any such audit or inspection;
- (c) ensure that ICT services are hosted and data is processed exclusively within the European Economic Area (EEA), and notify the Client at least thirty (30) days in advance of any planned changes to the locations of data processing or storage or to any sub-processors involved in the delivery of the Product.

6.3 Incident Notification: Copla shall notify the Client without undue delay, and in any event within twenty-four (24) hours, of any ICT-related incident or security breach that may affect the availability, integrity, or confidentiality of the Client's EBA Register data.

6.4 Service availability commitments and support response times are set out in the Service Level Agreement ('SLA'), which forms part of the Agreement.

7. Termination and Data Retention

7.1 Upon termination of the Client's Subscription Plan or access to the Product, or in the event of discontinuation of Copla's business operations, insolvency, or resolution, the Client shall be provided with a thirty (30) day grace period to export all Client Data and output files. During this period, Copla (or its liquidator or legal successor) guarantees access, recovery, and return of all personal and non-personal data in a structured, commonly used, and machine-readable format.

7.2 After expiry of the grace period, Copla shall delete or anonymise all Client Data associated with the Product, unless retention is required by applicable law or the Terms. Before any permanent deletion or anonymisation of Client Data, Copla shall provide the Client with at least thirty (30) days' prior written notice, confirming that the data remains available for export and requesting the Client's confirmation that it has no further objections to the deletion.

8. Jurisdiction and Applicability

8.1 These EBA Register Special Terms apply only to Clients who are subject to ICT third-party risk reporting and EBA Register-related obligations under DORA and who subscribe to the EBA Register Product.

8.2 These terms do not apply to the use of any other Copla products or services.

9. General

9.1 All matters not expressly governed by these EBA Register Special Terms shall be subject to the Terms.

9.2 These EBA Register Special Terms may be updated from time to time in accordance with the amendment procedure set out in the Terms.

9.3 Right to Audit: The Client or an appointed third party may conduct an audit of Copla's ICT security measures relevant to the Product once per calendar year, or at any time following a suspected or actual security breach affecting Client Data.

9.4 Copla undertakes to notify the Client of any Product updates or revisions that affect the data fields, reporting structures, or export functionality required for EBA Register compliance, ensuring that such updates do not disrupt historical Client Data or previously prepared compliance records.

10. Subcontracting

10.1 Copla shall not subcontract or delegate to any third party the performance of any part of the Product or its underlying ICT services without the prior written consent of the Client. Where the Client provides consent, Copla shall: (a) ensure that any subcontractor is bound by contractual obligations no less protective than those

set out in these EBA Register Special Terms and the Terms, including in relation to data confidentiality, security, and audit rights; and (b) remain fully liable to the Client for the performance of any subcontracted obligations.

10.2 Copla shall maintain and make available to the Client upon request an up-to-date list of all subcontractors and sub-processors engaged in the delivery of the Product, including their names, registered addresses, and the nature of services provided. Copla shall notify the Client in writing at least thirty (30) days in advance of any intended change to its subcontractors, and the Client shall have the right to object to any such change on reasonable grounds. Where the Client objects, the parties shall work in good faith to resolve the matter; if no resolution is reached, the Client may terminate the Agreement with no penalty.

11. Business Continuity and Exit Provisions

11.1 Copla shall maintain and regularly test a documented business continuity plan ("BCP") and disaster recovery plan ("DRP") for the Product, consistent with the requirements of DORA and applicable ICT risk management standards. Copla shall make a summary of such plans available to the Client upon request, and shall notify the Client within ten (10) business days of any material change to the BCP or DRP.

11.2 In the event of a significant disruption to the Product, Copla shall: (a) activate its BCP and DRP without undue delay; (b) notify the Client within four (4) hours of the disruption; (c) provide regular status updates at least every eight (8) hours until service is restored; and (d) provide a written root-cause analysis and remediation report within fifteen (15) business days following restoration of service.

11.3 Exit and Transition Assistance: Upon expiry or termination of these EBA Register Special Terms for any reason, in addition to the data return obligations set out in Section 7, Copla shall: (a) provide reasonable transition assistance to the Client or any replacement provider nominated by the Client for a period of up to ninety (90) days following the effective date of termination, at the Client's request and at rates agreed in advance; (b) ensure that no action is taken that would impair or hinder the Client's ability to migrate its data or continue its EBA Register and DORA reporting obligations; and (c) co-operate with the Client's reasonable requests to transfer configurations, data schemas, and documentation to facilitate continuity of service.

12. Termination for Regulatory Non-Compliance

12.1 Notwithstanding any other termination provisions in these EBA Register Special Terms or the Terms, the Client shall have the right to terminate this Agreement with immediate effect, by written notice to Copla, if: (a) Copla's acts or omissions cause or materially risk a breach by the Client of its obligations under DORA or any applicable regulatory requirement relating to the EBA Register; (b) a competent supervisory authority or resolution authority directs or recommends that the Client terminate the arrangement with Copla; (c) Copla suffers an insolvency event, appointment of an administrator, or ceases to carry on business; or (d) Copla materially and persistently fails to remedy a breach of these EBA Register Special Terms within ten (10) business days of written notice from the Client.

12.2 Where the Client exercises its right of immediate termination under clause 12.1, no termination fee, break penalty, or other financial consequence shall be payable by the Client.

CoreGuardian Special Terms

Last update: 2026-03-23 Version 1.0

These **CG Special Terms** apply to the use of the CG Product (as defined below) and form a legally binding Agreement between the Client and Copla, in addition to the Terms. In the event of any conflict or inconsistency between these CG Special Terms and the Terms, these CG Special Terms shall prevail in respect of the Product described herein.

1. Definitions

Unless otherwise defined herein, capitalized terms shall have the meaning ascribed to them in the Terms.

- **CG Product** means the web-based SaaS compliance automation application branded as **CoreGuardian**, a platform that assists organizations in assessing, managing, and maintaining compliance with one or more of the following regulatory and security frameworks: **NIS 2** (Directive (EU) 2022/2555), **DORA** (Regulation (EU) 2022/2554), **PCI DSS**, and **ISO 27001**. The Product operates through a web-based interface and an integrated chatbot (the "Assistant"), and provides compliance assessments, control gap analysis, task management, evidence storage, policy generation, and compliance dashboards.
- **Framework(s)** means one or more of the regulatory or security frameworks supported by the Product, as selected by the Client under the applicable Order Form, currently including NIS 2, DORA, PCI DSS, and ISO 27001.
- **Client** means an organization legally entitled to use the Product for internal compliance management purposes under the Agreement.
- **Client Data** means all information, evidence, documentation, and data submitted or uploaded by the Client or its authorized users to the Product.
- **Assistant** means the AI-assisted chatbot feature integrated into the Product that supports compliance assessment, evidence collection, awareness training delivery, and automated policy preparation.

2. Scope of Product

2.1 The Product is intended for professional use by Clients seeking to assess and manage their compliance posture against the selected Framework(s). The Product provides, in particular:

- a compliance assessment engine that evaluates the Client's current status against the controls and requirements of the selected Framework(s);
- an ICT risk management feature enabling the Client to identify, assess, and track ICT-related risks in the context of the applicable Framework(s);
- automated identification of control gaps and generation of prioritized remediation tasks for the Client to address;
- an evidence repository where the Client may store and associate documentation with specific controls;
- an AI-assisted chatbot (the "Assistant") that supports compliance workflows, including conducting interactive assessments, collecting evidence, delivering awareness training to the Client's personnel, and gathering the information required to automatically prepare draft policies applicable to the selected Framework(s);
- compliance dashboards providing the Client with a real-time, visual representation of its compliance level across selected Framework(s) and individual control domains.

2.2 The Product generates draft outputs, including policy documents and compliance reports, based on information provided by the Client. Such outputs are made available to the Client through the Platform interface and are intended to assist the Client's compliance processes. The Client remains solely responsible for reviewing, validating, and implementing all outputs in accordance with applicable requirements.

2.3 The scope of Frameworks and features available to the Client depends on the Subscription Plan selected in the applicable OF. Copla may add support for additional frameworks over the term of the Agreement; material changes to supported Frameworks will be communicated to the Client in advance.

3. Service Limitations and Disclaimer

3.1 The Product is made available solely for the Client's internal compliance management purposes. It does not constitute legal, regulatory, audit, or professional advisory services.

3.2 Copla does not guarantee that use of the Product will result in the Client achieving, maintaining, or demonstrating compliance with any Framework. The Client is solely responsible for its own compliance obligations and for the decisions it makes based on the Product's outputs.

3.3 Copla shall use reasonable efforts to ensure that the Product reflects the current requirements of each supported Framework and will update the Product without undue delay following any material change to a supported Framework's requirements.

4. Client Responsibilities and Data Input

4.1 The Client is solely responsible for the accuracy, completeness, and timeliness of all information and Client Data entered into the Product, including all responses provided to the Assistant and evidence uploaded to the evidence repository.

4.2 The quality and accuracy of the Product's assessments, gap analyses, policy drafts, and dashboard outputs depend on the accuracy and completeness of the information provided by the Client. Copla shall not be liable for any inaccuracies in outputs that result from incomplete, incorrect, or misleading Client Data or inputs.

4.3 The Client shall ensure that its authorized users are appropriately trained to use the Product and that use of the Product complies with all applicable internal policies, legal requirements, and confidentiality obligations.

5. Security and Availability

5.1 Copla shall implement reasonable and proportionate technical and organizational security measures to ensure the availability, integrity, and confidentiality of the Product and Client Data, consistent with applicable security standards.

5.2 Service availability commitments and support response times are set out in the Service Level Agreement ("SLA"), which forms part of the Agreement.

6. Applicability

6.1 These CG Special Terms apply only to Clients who subscribe to the CG Product.

6.2 These terms do not apply to the use of any other Copla Services.

7. General

7.1 All matters not expressly governed by these CG Special Terms shall be subject to the Terms.

7.2 These CG Special Terms may be updated from time to time in accordance with the amendment procedure set out in the Terms.

7.3 Copla shall notify the Client of any Product updates that materially affect the compliance assessment logic, supported Framework requirements, or evidence repository functionality, ensuring that such updates do not disrupt historical compliance data or evidence records stored in the Product.

Consulting Special Terms

Last update: 2026-03-23 Version 1.0

These **Consulting Special Terms** apply to the provision of information security consulting services by Copla (as described below) and form a legally binding Agreement between the Client and Copla, in addition to the Terms.

In the event of any conflict or inconsistency between these Consulting Special Terms and the Terms, these Consulting Special Terms shall prevail in respect of the Services described herein.

1. Definitions

Unless otherwise defined herein, capitalised terms shall have the meaning ascribed to them in the Terms.

Consulting Services means the information security advisory and consulting services provided by Copla specialists to the Client, as specified in the OF. Consulting Services may include, without limitation, advice on information security policies, risk assessments, security controls, regulatory requirements, and related matters. Consulting Services do not constitute CISO-as-a-Service or any ongoing management, operational, or executive security function.

Deliverables means any written reports, recommendations, assessments, or other outputs produced by Copla in the course of providing Consulting Services, as specified in the OF.

Hourly Rate means the fee per hour of Consulting Services provided, as agreed by the parties in the OF.

2. Scope of Services

2.1 Copla shall provide the Consulting Services to the Client on the terms set out in these Consulting Special Terms and the OF. The specific subject matter, scope, estimated hours, and any agreed Deliverables shall be set out in the OF or in a written statement of work agreed by the parties.

2.2 The flow and specific scope of each individual consulting engagement are agreed on a per-project basis. Unless the parties agree otherwise in the OF, the scope, objectives, and estimated effort for each engagement shall be confirmed between the parties by email or other written communication prior to commencement of work. Such confirmation constitutes a binding instruction to proceed and forms part of the Agreement. Copla shall not be obliged to commence work on any engagement until such confirmation has been received.

2.3 Consulting Services are provided on an advisory basis only. Copla's specialists will provide recommendations and guidance on the specific information security matters referred to them by the Client. The Client remains solely responsible for all decisions made and actions taken on the basis of Copla's advice.

2.4 Consulting Services do not include any ongoing management responsibility, executive security function, or operational authority over the Client's systems, processes, or personnel. Nothing in these Consulting Special Terms shall be construed as creating an employment, agency, or partnership relationship between Copla's specialists and the Client.

3. Fees and Billing

3.1 Consulting Services are billed at the Hourly Rate specified in the OF. Time shall be recorded by Copla in increments agreed in the OF, and Copla shall provide the Client with a summary of hours spent upon request or with each invoice.

3.2 Copla shall invoice the Client for Consulting Services in accordance with the payment terms set out in the OF and the Terms. Unless otherwise agreed in the OF, invoices shall be issued monthly in arrears for all hours rendered during the preceding calendar month.

3.3 If the estimated hours set out in the OF are likely to be exceeded, Copla shall notify the Client in advance. Additional hours beyond any agreed estimate shall require the Client's written approval before being incurred, unless the OF expressly provides otherwise.

3.4 Travel, accommodation, and other out-of-pocket expenses reasonably incurred in the provision of Consulting Services shall be reimbursed by the Client at cost, provided such expenses have been approved by the Client in advance.

4. Confidentiality and Deliverables

4.1 All Deliverables produced by Copla in the course of providing Consulting Services are provided for the Client's internal use only and shall be treated as Confidential Information under the Terms. The Client shall not share Deliverables with third parties without Copla's prior written consent.

4.2 Subject to full payment of all fees due, Copla grants the Client a non-exclusive, non-transferable licence to use the Deliverables for its internal information security purposes during the term of the Agreement.

4.3 Copla retains all intellectual property rights in any methodologies, frameworks, tools, and know-how used or developed in the course of providing Consulting Services. Nothing in these Consulting Special Terms shall be construed as a transfer of such intellectual property rights to the Client.

5. Advisory Nature and Disclaimer

5.1 Consulting Services are of an advisory nature. Copla's recommendations are based on the information provided by the Client and the professional judgement of Copla's specialists at the time of provision. Copla does not guarantee any specific security outcome, regulatory approval, or compliance result arising from the implementation of its advice.

5.2 The quality and relevance of Consulting Services depend on the accuracy and completeness of the information provided by the Client. Copla shall not be liable for any advice given on the basis of inaccurate, incomplete, or misleading information provided by the Client.

5.3 Consulting Services do not constitute legal, regulatory, or audit advice. Where legal, regulatory, or audit expertise is required, the Client should engage appropriately qualified professionals.

6. Client Responsibilities

6.1 The Client shall provide Copla with timely access to the personnel, systems, documentation, and information reasonably required for the provision of Consulting Services. Delays caused by the Client's failure to provide such access may affect the agreed timeline and may result in additional fees.

6.2 The Client is solely responsible for evaluating Copla's recommendations and for any decision to implement or disregard such recommendations. Copla shall not be liable for any loss or damage arising from the Client's implementation of, or failure to implement, Copla's advice.

7. Term and Termination

7.1 The engagement for Consulting Services shall commence on the date specified in the OF and shall continue until the earlier of: (a) completion of the scope set out in the OF; or (b) termination in accordance with these Consulting Special Terms or the Terms.

7.2 Either party may terminate the provision of Consulting Services on not less than fourteen (14) days' written notice to the other party. Upon termination, the Client shall pay Copla for all Consulting Services rendered up to and including the effective date of termination, together with any approved expenses incurred.

7.3 Copla may suspend or terminate the provision of Consulting Services with immediate effect if the Client fails to pay any invoice in accordance with the Terms.

8. General

8.1 All matters not expressly governed by these Consulting Special Terms shall be subject to the Terms.

8.2 These Consulting Special Terms may be updated from time to time in accordance with the amendment procedure set out in the Terms.

8.3 These Consulting Special Terms apply only to Clients who engage Copla for Consulting Services under a signed OF referencing these terms. They do not apply to the use of any other Copla product or platform-based service.

Vendriq Special Terms

Last update: 2026-03-23 Version 1.0

These **Vendriq Special Terms** apply to the use of the Vendriq Product (as defined below) and form a legally binding Agreement between the Client and Copla, in addition to the Terms.

In the event of any conflict or inconsistency between these Vendriq Special Terms and the Terms, these Vendriq Special Terms shall prevail in respect of the Product described herein.

1. Definitions

Unless otherwise defined herein, capitalised terms shall have the meaning ascribed to them in the Terms.

- **Product** means the web-based SaaS third-party management platform branded as **Vendriq**, which enables organisations to manage the full lifecycle of their third-party vendor relationships, including vendor selection and onboarding, risk evaluation, contract lifecycle management, performance monitoring, compliance oversight, and business continuity planning. The Product operates through a web-based interface accessible to the Client's authorised users.
- **Client** means the organisation legally entitled to use the Product for the purposes of managing its third-party vendor relationships under the Agreement.
- **Client Data** means all information, documentation, and data submitted, uploaded, or generated by the Client or its authorised users within the Product, including vendor profiles, contracts, questionnaire responses, performance records, and risk assessments.
- **Vendor** means any third-party supplier, service provider, or contractor whose information the Client manages within the Product.
- **Subscription Plan** means the plan selected by the Client under the applicable OF, which determines the modules, features, and usage limits available to the Client under these Vendriq Special Terms.

2. Scope of Product

2.1 The Product is intended for professional use by organisations seeking to centralise, automate, and manage their third-party vendor relationships across the full vendor lifecycle. Subject to the Subscription Plan, the Product includes the following feature areas:

- **Vendor selection and onboarding:** configurable onboarding workflows that automate documentation collection, route approvals to the appropriate stakeholders, trigger background and credit checks, and notify relevant parties — all without manual email coordination. Multi-stakeholder approval workflows and built-in communication threads maintain a full audit trail across procurement, legal, finance, and operations. Vendor questionnaires may be deployed to collect structured information during onboarding.
- **Vendor risk evaluation and recommendations:** centralised vendor profiles aggregating contacts, contracts, certifications, spend history, and risk tier in a single location accessible to authorised stakeholders. The Product provides visibility into each vendor's supply chain and generates recommendations on how identified risks should be handled.
- **Contract lifecycle and SLA management:** tracking of key contract dates, payment terms, SLAs, and renewal windows across all vendor relationships. The Product surfaces expiring contracts in advance and routes them to the designated owner for renegotiation, termination, or substitute vendor selection. Spend and contract data is made available to support renegotiation decisions.
- **Performance and cost monitoring:** configurable KPIs — including delivery timeliness, SLA adherence, quality scores, cost, and responsiveness — are tracked per vendor and aggregated into living scorecards. Spend data is consolidated across vendors, categories, and business units and visualised in dashboards that surface duplicate vendors, maverick spend, and consolidation opportunities.
- **Risk and compliance oversight:** automated tracking of vendor compliance certifications (including SOC 2, ISO 27001, insurance, and GDPR compliance), with flagging of upcoming expirations. The Product assigns risk tiers to vendors based on spend level, data access, and geography, and supports integration with third-party risk data feeds for real-time risk alerts.

- **Business continuity and exit planning:** identification of substitute vendors based on service category and risk profile, enabling the Client to maintain and demonstrate audit-ready contingency plans for each critical vendor relationship.

2.2 The specific modules and features available to the Client depend on the Subscription Plan selected in the applicable OF. Copla may introduce additional modules and features over the term of the Agreement; material changes to included functionality will be communicated to the Client in advance.

2.3 The Product is a tool to support the Client's vendor management processes. The Client remains solely responsible for all decisions made in relation to its vendor relationships, including vendor selection, onboarding, risk treatment, contract execution, and termination.

3. Service Limitations and Disclaimer

3.1 The Product is made available for the Client's internal vendor management purposes. It does not constitute legal, financial, regulatory, or audit advisory services.

3.2 Risk assessments, recommendations, and risk tier assignments generated by the Product are based on the data and information provided by the Client and, where applicable, third-party data feeds. Copla does not guarantee the accuracy, completeness, or timeliness of third-party data. The Client is solely responsible for evaluating and acting on any risk information or recommendations produced by the Product.

3.3 The Product does not execute contracts, commit the Client to any vendor arrangement, or take any action on the Client's behalf. All outputs — including risk recommendations, scorecards, and contingency plans — are informational and require the Client's independent review and decision.

3.4 Copla shall use reasonable efforts to ensure that the Product's functionality reflects current industry practices for third-party risk management and will update the Product without undue delay in response to material changes in applicable regulatory or technical requirements.

4. Client Responsibilities and Data Input

4.1 The Client is solely responsible for the accuracy, completeness, and currency of all Client Data entered into or uploaded to the Product, including all vendor information, contract data, questionnaire responses, and performance records.

4.2 The quality of the Product's risk assessments, scorecards, compliance alerts, and contingency planning outputs depends on the accuracy and completeness of the Client Data. Copla shall not be liable for any inaccuracies in outputs that result from incomplete, incorrect, or outdated Client Data.

4.3 The Client is responsible for ensuring that its use of the Product — including the collection and processing of vendor information within the Product — complies with all applicable laws, including data protection legislation. Where the Client processes personal data of its vendors' personnel within the Product, the Client acts as data controller for such processing.

4.4 The Client shall ensure that its authorised users are appropriately trained and that access credentials are not shared or transferred to unauthorised parties.

5. Data Access and Confidentiality

5.1 Subject to applicable law, all Client Data submitted to or generated within the Product remains the sole property of the Client.

5.2 Copla shall process Client Data strictly in accordance with its role as service provider and in line with applicable data protection legislation and the Data Processing Agreement.

5.3 Copla shall not access, use, transmit, or disclose Client Data to third parties, except where required for the operation and maintenance of the Product, authorised by the Client, or required by applicable law.

5.4 Copla may use aggregated, anonymised, and non-attributable data derived from the Product for the purposes of product improvement, benchmarking, and analytics, provided that such use does not enable the identification of the Client or any individual vendor.

6. Security and Availability

6.1 Copla shall implement reasonable and proportionate technical and organisational security measures to ensure the availability, integrity, and confidentiality of the Product and Client Data, consistent with applicable security standards.

6.2 Copla shall notify the Client without undue delay, and in any event within twenty-four (24) hours, of any security incident or breach that may affect the availability, integrity, or confidentiality of Client Data.

6.3 Service availability commitments and support response times are set out in the Service Level Agreement ('SLA'), which forms part of the Agreement.

7. Termination and Data Retention

7.1 Upon expiry or termination of the Client's Subscription Plan or access to the Product, the Client shall be provided with a thirty (30) day grace period during which it may export all Client Data and output files in a structured, commonly used, and machine-readable format. In the event of discontinuation of Copla's business operations, insolvency, or resolution, Copla (or its liquidator or legal successor) shall guarantee access, recovery, and return of all Client Data during the same grace period.

7.2 Following expiry of the grace period, Copla shall delete or anonymise all Client Data associated with the Product, unless retention is required by applicable law or the Terms. Copla shall provide the Client with at least thirty (30) days' prior written notice before any permanent deletion or anonymisation, confirming that the data remains available for export.

8. Applicability

8.1 These Vendriq Special Terms apply only to Clients who subscribe to the Vendriq Product.

8.2 These terms do not apply to the use of any other Copla products or services.

9. General

9.1 All matters not expressly governed by these Vendriq Special Terms shall be subject to the Terms.

9.2 These Vendriq Special Terms may be updated from time to time in accordance with the amendment procedure set out in the Terms.

9.3 Copla shall notify the Client of any Product updates that materially affect core vendor management functionality, ensuring that such updates do not cause loss of or irreversible changes to Client Data without prior notice.

9.4 Right to Audit: The Client or an appointed third party may, upon reasonable prior written notice, conduct an audit of Copla's security measures relevant to the Product once per calendar year, or at any time following a suspected or actual security breach affecting Client Data.

10. Subcontracting

10.1 Copla shall not subcontract or delegate to any third party the performance of any material part of the Product or its underlying infrastructure without prior written notice to the Client. Where Copla engages subcontractors, it shall: (a) ensure that any subcontractor is bound by contractual obligations no less protective than those set out in these Vendriq Special Terms and the Terms, including in relation to data confidentiality, security, and audit rights; and (b) remain fully liable to the Client for the performance of any subcontracted obligations.

10.2 Copla shall maintain and make available to the Client upon request an up-to-date list of all subcontractors and sub-processors engaged in the delivery of the Product. Copla shall notify the Client in writing at least thirty (30) days in advance of any intended material change to its subcontractors, and the Client shall have the right to object to any such change on reasonable grounds.

11. Termination for Material Breach

11.1 Without prejudice to any other termination rights under the Terms, the Client shall have the right to terminate this Agreement with immediate effect, by written notice to Copla, if: (a) Copla materially and persistently fails to remedy a breach of these Vendriq Special Terms within fifteen (15) business days of written notice from the Client; or (b) Copla suffers an insolvency event, appointment of an administrator, or ceases to carry on business.

11.2 Where the Client exercises its right of immediate termination under clause 11.1, no termination fee, break penalty, or other financial consequence shall be payable by the Client.

Managed Vendor Risk Management Special Terms

Last update: 2026-09-29

Version 1.0

These **MVRM Special Terms** apply to the use of the Managed Vendor Risk Management Service (as defined below) and form a legally binding Agreement between the Client and Copla, in addition to the Terms.

In the event of any conflict or inconsistency between these MVRM Special Terms and the Terms, these MVRM Special Terms shall prevail in respect of the Service described herein.

The Service is delivered using the Vendriq Product. The Vendriq Special Terms apply to the Client's use of that Product, and in the event of conflict these MVRM Special Terms prevail in respect of the Service.

1. Definitions

Unless otherwise defined herein, capitalised terms shall have the meaning ascribed to them in the Terms.

- **Service** means the managed vendor risk management service described in Chapter 2, performed by Copla for the Client using the Vendriq Product.
- **Vendriq Product** means the Copla vendor risk management platform, as defined in the Vendriq Special Terms.
- **Managed Vendor** means a third-party supplier of the Client which is recorded and maintained in the Vendriq Product as part of the Service. Each separate contractual arrangement between the Client and a supplier counts as one Managed Vendor.
- **Vendor Portfolio** means all Managed Vendors within the scope of the Service at a given time.
- **Vendor Count** means the number of Managed Vendors covered by the Fee, as stated in the OF.

- **Included Onboardings** means the number of additional vendors, beyond the Vendor Count, for which Copla charges no onboarding charge, as stated in the OF. The monthly amount under clause 5.4 still applies to them.
- **Risk Tier** means the classification of a Managed Vendor as routine, important, or critical, assigned by Copla under clause 2.1 and signed off by the Client under clause 3.2.
- **Framework** means any legal, regulatory, contractual, or industry framework against which the Client's third-party arrangements are assessed, as agreed by the parties and recorded in the OF or in the discovery report.
- **Additional Services** means any work which is not described in Chapter 2 or otherwise stated to be included in the Fee.
- **Fee** means the recurring fee for the Service specified in the OF.
- **Business Day** means a day other than a Saturday, Sunday, or public holiday in the Republic of Lithuania.

2. Scope of the Service

2.1 Within five (5) weeks of the Effective Date, or within such other period as the OF states, Copla shall deliver: a vendor inventory baseline across the Vendor Portfolio within the Vendriq Product; a Risk Tier for each Managed Vendor, supported by a written rationale stating the tier assigned, the inputs used, the assumptions made, and the recommended monitoring cadence; a criticality mapping of the Client's vendor arrangements against the applicable Frameworks; questionnaire templates configured for the Client's vendor types; an approval workflow configured to the Client's sign-off process; and a discovery report summarising the starting position, gaps, and priorities.

2.2 Thereafter Copla shall deliver, on a continuing basis: onboarding and due diligence for the Included Onboardings, comprising a completed due diligence questionnaire, collected documentation, an approval routing log, an initial Risk Tier with written rationale, and a complete vendor profile in the Vendriq Product; periodic automated monitoring across the Vendor Portfolio, including certification and insurance expiry tracking, breach and adverse media signals, and security ratings; quarterly re-assessment of each Managed Vendor with tier changes flagged and explained; a quarterly concentration view by provider, geography, and service type; contract lifecycle tracking with alerts ahead of renewal dates, notice

periods, and other contractual deadlines; a monthly status report to the Client's designated distribution list; a monthly working session with the Client's team of approximately sixty (60) minutes; a short quarterly feedback session with the Client on the operation of the Service; and a quarterly review of approximately ninety (90) minutes, delivered as a presentation and written memorandum.

2.3 The cadences stated in clause 2.2 are the service levels for the Service. Monitoring is carried out at those cadences and is not real-time surveillance. The concentration view is informational and does not constitute any assessment, determination, or filing which the Client is required to make itself.

2.4 The quarterly review covers the Service and the Vendor Portfolio only. It does not assess the Client's wider compliance framework or any obligation of the Client beyond vendor risk management.

2.5 Copla performs the Service for the Client but does not act as the Client's agent and has no authority to bind the Client, to select, instruct, negotiate with, or terminate any vendor, or to execute any document on the Client's behalf, unless the Client authorises it in writing on each occasion.

2.6 Copla may change the methods, tooling, and internal processes by which it delivers the Service, provided that the deliverables and cadences set out in clauses 2.1 and 2.2 are maintained.

2.7 The depth of due diligence, the evidence required, and the frequency and intensity of monitoring and re-assessment differ according to Risk Tier. A vendor tiered as critical receives the most detailed assessment and the most frequent review, a vendor tiered as important an intermediate level, and a vendor tiered as routine a proportionate baseline assessment. The approach applied to each Risk Tier is set out in the discovery report delivered under clause 2.1.

3. Client Responsibilities and Retained Decisions

3.1 The Client remains responsible at all times for its own compliance with all laws, regulations, and Frameworks applicable to it. The Service supports the Client's vendor risk management activities but does not assume, transfer, or discharge any obligation, function, or accountability of the Client.

3.2 The following decisions are reserved to the Client: vendor selection and final approval; risk appetite and risk treatment decisions, whether to accept, mitigate, transfer, or avoid a risk; contract negotiation and execution; vendor termination; final sign-off of each Risk Tier; the determination of which of the Client's functions or vendors are critical or important; and the content, accuracy, and submission of any report, register, filing, or notification the Client is required to make.

3.3 All assessments, tiers, analyses, and recommendations produced through the Service are advisory. Nothing produced under these MVRM Special Terms constitutes legal, financial, audit, or regulatory advice.

3.4 The Client shall give Copla timely access to the personnel, systems, documentation, and vendor information reasonably required for the Service. Copla is not responsible for any delay, gap, or inaccuracy in the Service to the extent it results from the Client's failure to provide such access. Where the Client has failed to provide access for more than ten (10) Business Days after written request, Copla may suspend the affected element of the Service without liability, and the Fee remains payable in full.

4. Risk Tiering and Evaluation Method

4.1 Copla shall assign a proposed Risk Tier to each Managed Vendor using the evaluation method set out in this Chapter. The Risk Tier determines the depth of due diligence and the monitoring cadence applied under Chapter 2, and the rate charged for any additional vendor under clause 5.4.

4.2 In evaluating a Managed Vendor, Copla shall assess at least the following factors: (a) the importance of the service to the Client's operations and to the continuity of its business services; (b) whether the service supports a function which the Client has identified as critical or important; (c) whether the vendor accesses, processes, or stores Client data, and the volume and sensitivity of that data, including personal data; (d) the nature and extent of any access to the Client's systems, including privileged, remote, or persistent access; (e) the requirements applicable to the arrangement under any applicable Framework; (f) substitutability, being the availability of alternative providers and the estimated time and cost of replacement; (g) concentration and dependency, including intra-group arrangements and the vendor's own sub-contracting chain; (h) the countries from which the service is provided and in which data is stored; (i) financial exposure,

including contract value and the cost of failure; and (j) the vendor's security posture and assurance position, including certifications held, assurance reports available, and known incident history.

4.3 Each factor is scored on a documented scale and the scores are aggregated to produce a proposed Risk Tier of routine, important, or critical. The scoring scale, the weighting of individual factors, and the thresholds between Risk Tiers are recorded in the discovery report delivered under clause 2.1 and are available to the Client in the Vendriq Product. Where the Client operates its own risk taxonomy, the parties may agree at the outset to map the Risk Tiers to it, and that mapping shall be recorded in the discovery report.

4.4 Copla shall submit each proposed Risk Tier to the Client with a written rationale stating the tier proposed, the factors and inputs relied on, the assumptions made, and the recommended monitoring cadence. The Client signs off the Risk Tier in accordance with clause 3.2.

4.5 Copla shall re-evaluate each Managed Vendor at least quarterly, and in addition on the occurrence of a trigger event, being a material change in the service provided, an incident affecting the vendor, adverse media or a change in the vendor's assurance position, a change in the location of provision or in the vendor's sub-contractors, a change in an applicable Framework, or the renewal or material variation of the vendor contract. Where a re-evaluation produces a different proposed Risk Tier, clause 4.4 applies to it.

4.6 Copla may update the evaluation method from time to time to reflect changes in applicable Frameworks, supervisory expectations, or established practice. Copla shall notify the Client at least thirty (30) days before any material change to the factors, weightings, or thresholds takes effect. A change to the evaluation method does not apply retrospectively to a Risk Tier already signed off, and takes effect for a Managed Vendor at its next re-evaluation.

4.7 Where the Client and Copla do not agree on a Risk Tier, the Client's determination prevails in accordance with clause 3.2, and Copla shall record the difference and its own proposed Risk Tier in the Vendriq Product. Clause 5.6 governs the effect of a disputed Risk Tier on charging.

5. Vendors Covered, Fee, and Continuation

5.1 The OF states the number of Managed Vendors covered by the Service (the Vendor Count) and the Fee for that Vendor Count. The Fee covers the Service for those Managed Vendors for the term. The Fee includes the Client's use of the Vendriq Product while the Service is provided.

5.2 Copla first carries out the setup described in clause 2.1 for the Managed Vendors within the Vendor Count. When the setup is complete, Copla notifies the Client in writing.

5.3 Within thirty (30) days of that notice the Client may choose, by written notice to Copla, one of two options: (a) Copla continues to provide the Service under these MVRM Special Terms for the remainder of the term; or (b) the Client manages its vendors itself using the Vendriq Product. If the Client chooses option (b), the Service ends thirty (30) days after the Client's notice or at the end of the third (3rd) month after the Effective Date, whichever is later, and the Fee stops from that date. No Fee paid in advance for any period after that date is refunded; instead, the Client may use the Vendriq Product until the end of the period already paid for without further charge. From the end of that period, the Client's use of the Vendriq Product is governed by the Vendriq Special Terms alone, at the rate stated in the OF for the Vendriq Product or, if none is stated, at Copla's standard rate. If the Client gives no notice, option (a) applies.

5.4 The Client may add Managed Vendors at any time. Each Managed Vendor added beyond the Vendor Count is charged, in addition to the Fee, the monthly amount stated in the OF for its Risk Tier, from the first day of the month after onboarding until it is removed from the Vendor Portfolio. Removal takes effect at the end of the month in which the Client gives written notice. An onboarding charge stated in the OF is payable once for each additional vendor, except for vendors covered by the Included Onboardings. Before onboarding, Copla confirms the proposed Risk Tier, the monthly amount, and any onboarding charge to the Client in writing, and the Client may withdraw the request at that point without charge.

5.5 The Fee does not reduce if the number of Managed Vendors falls below the Vendor Count.

5.6 A Risk Tier is assigned on risk grounds alone under Chapter 4 and is never set by reference to price. Where the Client disputes a proposed Risk Tier, the higher tier applies for charging until the dispute is resolved, and any difference is then credited or invoiced.

5.7 Amounts charged under clause 5.4 are additional Fees for additional Services. They do not count towards the annual fee increase limit in the Terms (clause 7.6 of the Terms), which continues to apply to the monthly amounts stated in the OF.

6. Additional Services

6.1 Only the activities described in Chapter 2 are included in the Fee. No other activity is included, whether or not it relates to vendor risk management.

6.2 Onboarding of additional vendors is charged as set out in clause 5.4.

6.3 The following are available on request and are quoted before work begins: contract compliance review, being a review of a vendor contract against GDPR, DORA, and information security requirements, identifying missing or weak provisions and, where gaps exist, providing draft addendum language, recommended changes, or a draft data processing agreement for the Client's legal team to review, adapt, and execute; vendor shortlisting, being a list of candidate vendors in a category specified by the Client with a surface-level check on each; vendor exit recommendations, being a transition plan for a vendor the Client has decided to leave; and executive reports outside the standard monthly and quarterly cycle.

6.4 A contract compliance review is limited to the scope stated and is not a legal review. Final legal review, negotiation, and execution remain with the Client's legal advisers. Vendor shortlisting does not include a recommendation as to which vendor to select, and the Client conducts all evaluations and negotiations. Execution of any vendor transition remains with the Client.

6.5 Additional Services are performed only on the Client's written request or written approval of a quote, and are charged at the rates set out in the OF or, where no rate is stated, at Copla's standard rates in force at the time. Where Copla provides advisory work beyond the scope of these MVRM Special Terms, the Consulting Special Terms apply to that work.

7. Service Governance and Support for the Client's Regulatory Obligations

7.1 The functions and services provided under the Service are described in Chapter 2 and in the OF. Subcontracting is permitted only on the conditions set out in Chapter 10.

7.2 The Service is provided from, and Client Data is processed and stored within, the European Economic Area. Copla confirms that the primary locations of service provision and data storage are the Dublin metropolitan area, Republic of Ireland, and Vilnius, Lithuania, and shall notify the Client not less than thirty (30) days before any intended change to the countries in which the Service is provided or Client Data is processed or stored.

7.3 Copla shall maintain provisions on the availability, authenticity, integrity, and confidentiality of data, including personal data, in accordance with Chapter 9, the DPA, and applicable data protection law.

7.4 In the event of insolvency, resolution, or discontinuation of Copla's business operations, or on termination of the Agreement for any reason, the Client shall be ensured access to, recovery of, and return of all personal and non-personal data processed for it, in an easily accessible, structured, commonly used, and machine-readable format, in accordance with Chapter 12 and clauses 2.8 to 2.10 of the Terms.

7.5 Service levels and cadences for the Service are set out in Chapter 2 and the OF. Service availability commitments and support response times for the Vendriq Product are set out in the SLA.

7.6 Copla shall assist the Client at no additional cost where an incident connected with the Service occurs, in accordance with Chapter 9.

7.7 Copla shall cooperate fully with any competent authority, supervisory authority, or resolution authority of the Client, and with any person appointed by them, and shall not charge the Client for that cooperation.

7.8 In addition to any other right of termination, the Client may terminate the Service where: (a) Copla is in significant breach of applicable law, regulation, or the Agreement; (b) circumstances arise which materially and demonstrably affect Copla's ability to perform the Service in accordance with the Agreement, including material adverse changes affecting the arrangement or the situation of Copla; (c)

weaknesses are evidenced in Copla's risk management, in particular in the way it ensures the availability, authenticity, integrity, or confidentiality of data; or (d) a competent authority of the Client can no longer effectively supervise the Client as a result of the arrangement. Before terminating on any of these grounds the Client shall give Copla written notice specifying the ground relied on and the facts supporting it, and shall allow Copla thirty (30) days to remedy the matter, unless the matter is incapable of remedy, a competent authority requires earlier termination, or waiting would cause the Client to breach a regulatory requirement. Where Copla remedies the matter within that period the right to terminate under this clause lapses in respect of that matter. Termination under this clause takes effect on the notice the Client specifies and no termination fee is payable.

8. Additional Provisions for Critical or Important Functions

8.1 Where the Service supports a function which the Client has identified as critical or important, or which is otherwise subject to enhanced regulatory requirements under an applicable Framework, the remainder of this Chapter applies. The Client shall inform Copla in writing of any such identification, and Copla shall give effect to this Chapter within thirty (30) days of being informed. Where the OF records that this Chapter applies at the Effective Date, the obligations in this Chapter are included in the Fee. Where the Client notifies Copla after the Effective Date, the parties shall seek to agree an adjustment to the Fee reflecting the additional obligations; failing agreement within thirty (30) days, Copla shall nonetheless give effect to this Chapter and the additional work is chargeable as Additional Services at Copla's standard rates in force at the time.

8.2 The parties shall agree full service level descriptions for the Service with precise quantitative and qualitative performance targets, so that the Client can monitor the Service effectively and require corrective action without undue delay where those targets are not met.

8.3 Copla shall notify the Client without undue delay of any development that might have a material impact on its ability to provide the Service in line with the agreed service levels.

8.4 Copla shall implement and test business contingency plans and shall maintain security measures, tools, and policies providing an appropriate level of security for the Service. Testing shall be carried out at least annually and Copla shall provide a

summary of the results to the Client on request.

8.5 Copla shall participate and cooperate fully in threat-led penetration testing carried out by or on behalf of the Client, including pooled testing. Copla shall bear its own costs of participating in one such exercise in any period of twenty-four (24) months. Participation in further exercises within that period, and any effort exceeding five (5) person-days in respect of a single exercise, is chargeable as Additional Services at Copla's standard rates in force at the time.

8.6 The Client may monitor Copla's performance on an ongoing basis, which entails: (a) unrestricted rights of access, inspection, and audit for the Client, for a third party appointed by the Client, and for a competent authority; (b) the right to take copies of relevant documentation on site where taking such copies is critical to the Client's operations; (c) the right to require Copla to cooperate fully during on-site inspections and audits; and (d) an obligation on Copla to provide details of the scope, the procedures to be followed, and the frequency of such inspections and audits. Copla shall bear its own costs of one audit or inspection in each calendar year, and of any inspection carried out or required by a competent authority, however many such inspections occur. Where the Client, or a third party appointed by it, carries out further audits in the same calendar year, or where Copla's cooperation in respect of audits in a calendar year exceeds five (5) person-days in aggregate, the Client shall reimburse Copla's reasonable and documented costs of that additional cooperation, charged at Copla's standard rates in force at the time. Copla shall notify the Client before such costs are incurred and shall not withhold, delay, or condition any access, inspection, or audit right on payment. Each party otherwise bears its own costs.

8.7 On expiry or termination of the Service, other than termination by Copla for the Client's material breach or non-payment or termination arising from Copla's insolvency or cessation of business, or an ending of the Service under clause 5.3(b), Copla shall observe a transition period of six (6) months, or such longer period as the Client reasonably requires up to a maximum of twelve (12) months, during which Copla shall continue to provide the Service on the same terms so as to reduce the risk of disruption at the Client and to allow the Client to migrate to another provider or to an in-house solution. The Client shall specify the length of the transition period it requires not less than thirty (30) days before the Service would otherwise end; failing that, the transition period is six (6) months. The Fee payable during the transition period is the Fee in force immediately before the

Service would otherwise have ended, invoiced monthly in advance. Work requested by the Client for the purposes of transition which falls outside Chapter 2 is chargeable as Additional Services. The transition period is for the purposes of this clause only and does not extend the term of the Agreement for any other purpose. Copla may suspend the transition period where the Client fails to pay any undisputed amount when due.

9. Security, Availability, and Incident Assistance

9.1 Copla shall implement and maintain appropriate technical and organisational measures to ensure the availability, authenticity, integrity, confidentiality, and resilience of the Service and of Client Data, consistent with applicable security standards.

9.2 Copla shall notify the Client without undue delay, and in any event within twenty-four (24) hours, of any incident or security breach affecting the Service or Client Data, and shall provide information sufficient to enable the Client to classify the incident and to meet its own reporting obligations.

9.3 Copla shall assist the Client at no additional cost in connection with any incident connected with the Service, including assistance with investigation, containment, root-cause analysis, and the preparation of any report the Client is required to make.

9.4 Copla confirms that, as at the date on which these MVRM Special Terms take effect and so far as Copla is aware, it has not been designated as a critical third-party service provider under any regime applicable to it, and shall notify the Client without undue delay if it becomes so designated.

10. Subcontracting

10.1 Copla shall not subcontract the Service or any material part of it without the Client's prior written consent, which shall not be unreasonably withheld or delayed. Where Chapter 8 applies, Copla shall notify the Client in advance of any intended subcontracting of material parts of the Service, and the Client may object before it takes effect.

10.2 Copla shall ensure that each subcontractor is bound by obligations no less protective than those in these MVRM Special Terms and the Terms, including as to confidentiality, security, data location, and rights of access, inspection, and audit, and shall remain fully liable to the Client for the performance of any subcontracted obligation.

10.3 Copla shall maintain and make available to the Client on request an up-to-date list of the subcontractors and sub-processors engaged in delivering the Service, including their names, registered addresses, the services provided, and the countries from which those services are provided. Copla shall give the Client at least thirty (30) days' written notice of any intended change, and the Client may object on reasonable grounds.

11. Term, Renewal, and Termination

11.1 The term of the Service is governed by Chapter 11 of the Terms, save as stated in this clause. The Service commences on the Effective Date and continues for the Initial Term specified in the OF. Unless the OF states that the Service expires at the end of the Initial Term, the Service extends automatically for successive periods equal to the Initial Term unless a party gives notice of termination in the manner and within the period set out in clause 11.1 of the Terms.

11.2 Copla's rates in force at the time of an extension apply to that extension period. Copla shall notify the Client of the rates applicable to the next period not less than forty-five (45) days before the end of the then-current term, so that the Client may exercise its right of termination under clause 11.1 of the Terms if it does not accept them. A change of rate taking effect on extension is not an in-term increase, and clause 7.6 of the Terms does not apply to it; clause 7.6 continues to apply to any increase taking effect during a term.

11.3 The parties shall review the Service together at least once every six (6) months, covering the Vendor Portfolio, the Service delivered, and any adjustment of scope either party wishes to propose.

11.4 The Client may terminate the Service on the grounds set out in clause 7.8, or may end the Service under clause 5.3(b), in each case with no termination fee, and either party may terminate under clause 11.2 of the Terms. Any other termination by the Client before the end of the then-current term does not relieve the Client of its obligation to pay the Fee for the remainder of that term, and no prepaid Fee is

refundable. The early termination charge in clause 7.7 of the Terms does not apply to the Service, and this clause applies instead of it; clause 7.7 of the Terms otherwise applies. The Fee for the remainder of the term reflects the personnel and capacity Copla reserves for the Service for the full term.

12. Data Retention, Exit, and Return of Data

12.1 During the term Copla retains and processes Client Data for as long as is necessary to provide the Service.

12.2 On expiry or termination of the Service for any reason, Copla shall provide the Client with a complete export of the Client Data held in the Vendriq Product in connection with the Service, including vendor profiles, questionnaire responses, collected documentation, Risk Tiers and their rationales, monitoring history, and reports, in a structured, commonly used, and machine-readable format, within thirty (30) days of the effective date of termination.

12.3 Copla shall retain Client Data for ninety (90) days following the effective date of termination and shall delete or anonymise it at the end of that period, unless retention is required by applicable law or the DPA. Clause 2.9 of the Terms applies to that deletion.

12.4 Copla may retain indefinitely, and use for the purposes of maintaining and improving its vendor reference data, factual information about a supplier which does not identify the Client and does not reveal the existence or the terms of any relationship between the Client and that supplier. Such information is limited to the supplier's legal name, legal entity identifier and other public registration identifiers, registered address, corporate group details, publicly available certifications and their validity periods, and comparable publicly available or supplier-provided attributes of the supplier as an organisation. It does not include personal data, and it does not include the Client's assessments, Risk Tiers, questionnaire responses, contracts, reports, or any other Client Data.

12.5 Where Chapter 8 applies, the transition period in clause 8.7 applies. Otherwise Copla shall provide transition assistance for up to sixty (60) days following the effective date of termination, at rates agreed in advance.

12.6 Copla shall not act, or omit to act, in a manner which would impair the Client's ability to continue its vendor risk management activities during or after the transition.

13. Case Studies and Marketing Materials

13.1 Copla's use of the Client's name and logo in sales and marketing materials is governed by Chapter 14 of the Terms.

13.2 In addition, Copla may prepare a case study relating to the Service. Copla shall provide the draft to the Client and shall not publish or otherwise disclose it without the Client's prior written approval, which shall not be unreasonably withheld or delayed.

13.3 No Confidential Information of the Client, no name of a Managed Vendor, and no assessment, Risk Tier, or report generated through the Service shall be disclosed in any case study or marketing material without the Client's express prior written approval.

14. Applicability

14.1 These MVRM Special Terms apply only to Clients who subscribe to the Service under the OF.

14.2 These terms do not apply to the use of any other Copla product or service. Where the Client receives any other service from Copla under a separate agreement, that service is governed by that agreement, and these MVRM Special Terms neither extend nor limit its scope.

15. General

15.1 All matters not expressly governed by these MVRM Special Terms shall be subject to the Terms.

15.2 These MVRM Special Terms may be updated from time to time in accordance with the amendment procedure set out in the Terms.

15.3 Where the OF expressly states that a provision of these MVRM Special Terms is varied, supplemented, or disapplied, the OF prevails to the extent stated, notwithstanding clause 2.7 of the Terms. This clause does not permit the OF to

vary or disapply Chapter 3, Chapter 4, clauses 7.7 and 7.8, clause 8.6, Chapter 9, Chapter 10, or Chapter 12, each of which applies to every Client in all cases.

Copla Service Level Agreement (SLA)

Version 1.0 2026-03-23

1. Service Level Targets (SLAs)

1.1. Service Availability

Copla shall use **commercially reasonable efforts** to achieve a Service Availability of **99.0%** per calendar month.

- **Measurement:** Service availability shall be measured as the percentage of time the production environment is operational and accessible to the Client, excluding the Exclusions set out in Section 1.5.

1.2. Incident Response and Resolution

Copla shall use **commercially reasonable efforts** to meet the following targets for Incident Management, with acknowledgement and resolution targets defined by severity:

Severity Level	Description	Acknowledgement Target	Resolution / Workaround Target
Severity 1 – Critical	Complete service outage or severe degradation affecting all users; no immediate workaround.	2 hour	24 hours
Severity 2 – High	Major functionality impaired; partial outage affecting many users; workaround exists but is not sustainable.	5 hours	3 business days
Severity 3 – Medium	Non-critical degradation or functional issues impacting some users; workaround available.	1 business day	7 business days
Severity 4 – Low	Minor issues, cosmetic defects, non-urgent queries.	3 business days	As mutually agreed

1.3. Monitoring and Measurement

Copla shall internally monitor system availability and key performance indicators. Measurement methods shall be transparent and aligned with Copla's internal good industry practices.

1.4. Service Credits and Exclusive Remedy

If Copla fails to meet the Service Availability target set out in Section 1.1, the Client's **sole and exclusive financial remedy** shall be the following Service Credits:

- Availability below 99.0% but above 96.0% - **2%** monthly service credit
- Availability at or below 96.0% - **4%** monthly service credit

Service credits are applied to the next invoice and constitute the Client's **exclusive financial remedy** for Service Availability breaches, notwithstanding any other rights the Client may have regarding material breach of the Agreement.

1.5. Exclusions

SLAs shall not apply to failures or delays caused by:

(i) Client-side systems, connectivity, or misuse of the Services;

(ii) third-party services not under the direct management and control of Copla;

(iii) force majeure events; or

(iv) planned maintenance, provided Copla gives reasonable prior notice (typically 72 hours).

1.6. Support Hours and Business Hours

Customer Success and standard support services shall be provided during Business Hours, defined as Monday to Friday, from 09:00 to 18:00, Eastern European Time (EET/EEST), as applicable in Lithuania, excluding public holidays in Lithuania.

All acknowledgement and resolution targets set out in Section 1.2 shall be measured and apply only during Business Hours, unless expressly agreed otherwise in writing by the Parties.

Incidents reported outside Business Hours shall be deemed received at the start of the next Business Hour.

Copla Data Processing Agreement

Last update: 2026-08-25 Version 2.1

This Data Processing Agreement (“**DPA**”) is entered into between the Client and UAB Cyber upgrade (legal entity code 306422641, address Laičių str. 92, Laičių village, Elektrėnai, Lithuania (or "**Data Processor**") (hereinafter collectively referred to as "**Parties**").

WHEREAS

(A) the Client acts as a data controller;

(B) for the purposes of provision of automated compliance automation SaaS platform under the Services Agreement, the Data Processor shall process personal data on behalf of the Client hereunder;

(C) the Parties seek to implement a data processing arrangement that complies with the current legal regulatory requirements related to personal data processing;

(D) the Parties aim to establish their rights and obligations to ensure that the processing of personal data complies with the applicable personal data legislation, therefore:

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1. Unless otherwise defined in this DPA or the Services Agreement, terms and expressions written in capital letters in this DPA shall have the following meanings:

1.1.1. "**Company Personal Data**", "**Client Personal Data**" or "**Personal Data**" - any personal data processed on behalf of the Client by the Data Processor;

1.1.2. "**Sub-processor**" - any person appointed by or on behalf of the Data Processor to process Personal Data on behalf of the Client under this DPA;

1.1.3. "**Data Protection Laws**" - EU data protection laws and, where applicable, the data protection or privacy laws of any other country;

1.1.4. "**EEA**" - the European Economic Area;

1.1.5. "**GDPR**" - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

1.1.6. "**Data Transfer**" means:

1.1.6.1. the transfer of the Client's Personal Data from the Client to the Data Processor; or

1.1.6.2. further transfer of the Client's Personal Data from the Data Processor to a Sub-processor, or between the Processor and its affiliates;

1.1.7. "**Services**" - services provided by the Data Processor, more fully described in the Services Agreement.

1.2. Terms "**data controller**", "**data subject**", "**Member State**", "**personal data**", "**personal data breach**", "**processing**" , "**supervisory authority**" and others used in this DPA shall have the same meaning as in the GDPR.

2. Obligations of the Parties

2.1. The Client:

2.1.1. is responsible for ensuring that Personal Data is processed in accordance with the GDPR, Data Protection Laws and this DPA, including implementing appropriate technical and organizational security measures as required by Article 32 of the GDPR;

2.1.2. has the right and obligation to make decisions on the purposes and means of processing of Personal Data;

2.1.3. shall be responsible, among other, for ensuring that processing of Personal Data which is assigned to the Data Processor has legal basis;

2.1.4. is responsible for ensuring that data subjects are provided with all necessary information about the processing of their Personal Data, as required under GDPR and other applicable laws;

2.1.5. shall ensure that, when transferring Personal Data to the Data Processor, all relevant and accurate information regarding processing purposes, data categories, and any applicable restrictions or requirements is provided.

2.2. The Data Processor undertakes:

2.2.1. processes Personal Data only in accordance with the documented instructions issued by the Client except for the cases where this is required by the Data Protection Laws applicable to the Data Processor (in such cases Data Processor shall inform the Client of the legal requirement before processing, unless that law prohibits such information for reasons of substantial public interest);

2.2.2. shall immediately notify the Client if, in the opinion of the Data Processor, the Client's instructions are in conflict with the GDPR or other Data Protection Laws;

2.2.3. shall maintain records related to the activities of processing of Personal Data carried out on behalf of the Client.

2.3. In the event that the instructions of the Client by which the Personal Data are processed by the Data Processor are unlawful, the Client shall be liable for any damage caused to the Data Processor by such actions and shall indemnify the Data Processor for the direct losses incurred.

2.4. This DPA shall not release the Parties from other obligations applicable to them under the GDPR or other Data Protection Laws.

2.5. The Client entrusts the Data Processor to process the Company's Personal Data. The processed Personal Data is described in Annex II of this DPA.

3. Confidentiality

3.1. The Data Processor shall take reasonable measures to ensure the reliability of any employee, agent, or contractor of the Data Processor mentioned in the Services Agreement who may have access to the Company's Personal Data, in each case ensuring that access is strictly limited to those individuals who need to know and (or) have access to the relevant Company's Personal Data, as necessary for the purpose of the Services Agreement, and to comply with Data Protection Laws, ensuring that all such individuals are subject to confidentiality commitments or

professional or statutory confidentiality obligations. In case of discontinuation of employment relationship with the employee of the Data Processor, the access rights to the Client's Personal Data shall be revoked not later than on the last day of work.

3.2. The list of persons granted access to Personal Data shall be reviewed on a periodical basis, at least every 3 months. Following the afore-mentioned review, such access to Personal Data shall be suspended if such access is no longer necessary; thus, Personal Data cannot be accessible to such persons.

3.3. Upon the Client's request, the Data Processor shall demonstrate that the persons who are supervised by the Data Processor and to whom processing of Personal Data is assigned shall be subject to the obligation of confidentiality provided for in Section 3 of DPA.

3.4. Each Party must keep this DPA and information it receives about the other Party and its business in connection with this DPA confidential and may not use or disclose this confidential information without the prior written consent of the other Party, except where:

3.4.1. disclosure is required by law;

3.4.2. the relevant information is already publicly available;

3.4.3. disclosure is made to the Data Processor's affiliates and Sub-processors.

4. Security

4.1. The Data Processor shall implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risk for the Company's Personal Data. In assessing the appropriate level of security, the Data Processor shall primarily consider the risks that are presented by processing, particularly from a Personal Data breach. Depending on the appropriateness of the measures, they may be as follows:

4.1.1. the pseudonymisation and (or) encryption of Personal Data;

4.1.2. the ability to ensure the continues confidentiality, integrity, availability and resilience of processing systems and services;

4.1.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

4.1.4. a process for regular testing, inspecting and evaluating the technical and organizational security measures for ensuring the security of the processing.

4.2. The Data Processor acknowledges that it has obtained DIN EN ISO/IEC 27001:2022 certification. The used security measures are provided by request.

4.3. According to Article 32 of the GDPR, the Data Processor shall also – independently from the Client – evaluate the risks to the rights and freedoms of natural persons inherent in the processing activity entrusted to it by the Client and implement the measures to mitigate those risk. To this end, the Client shall provide the Data Processor with all information necessary for identification and assessment of such risk.

4.4. Furthermore, the Data Processor shall help the Client in ensuring compliance with the Client's obligation provided for in Article 32 of the GDPR inter alia providing the Client with information on technical and organisational security measures which have already been implemented by the Data Processor under Article 32 of the GDPR together with all other information necessary for the Client to comply with its obligation under Article 32 of the GDPR.

4.5. If, according to the assessment made by the Client, the mitigation of the identified risks requires further measures to be implemented by the Data Processor, the Client shall specify these additional measures, and the Data Processor shall implement additional measures. The Data Processor shall make available to the Client all information necessary to demonstrate compliance with its obligations as provided in this DPA.

5. Sub-processors

5.1. Data Sub-processors engaged by the Data Processor are disclosed in Annex I of this DPA. The Data Processor undertakes to ensure that they comply with the terms of this DPA. Prior to processing, the Data Processor shall inform the Sub-processor of the identity and contact details of the Client for which the Sub-processor processes Personal Data.

5.2. The Data Processor shall not engage a Sub-processor for performance of the processing carried out under this DPA without a prior general written authorisation of the Client. The Data Processor has the general written authorisation to engage

Sub-processors of the Client. The Data Processor shall notify the Client of any planned amendments related to engagement or replacement of Sub-processors in writing no later than 10 business days in advance, thus, enabling the Client to object to such amendments before engagement of the respective Sub-processor(s).

5.3. In the event that the Client does not agree to the inclusion of the sub-processor in the list referred to in the Annex I, the Data Processor shall have the right to terminate this DPA and the Services Agreement if the use of this type of the Sub-processor is necessary for the performance of such contract.

5.4. A separate authorization of the Client is not necessary when renewal of the data processing agreement with the Sub-processor is sought.

5.5. Upon request of the Client, a copy of the contract with a Sub-processor and subsequent amendments thereto, shall be provided to the Client, thus, enabling the Client to ensure that the Sub-processor was subject to the same data protection obligations as laid down by the DPA. The Data Processor shall notify the Client of any failure by the Sub-processor to fulfil its obligations under that contract or other legal act binding on Sub-processor. The Data Processor is not obliged to provide the provisions of the data processing agreement on the business-related issues which do not have an impact on the terms and conditions of the legal protection of Personal Data of the contract concluded with the Sub-processor.

5.6. The Data Processor shall agree on a third-party beneficiary clause with a Sub-processor (if any) providing that in case of bankruptcy of the primary Data Processor, the Client shall be entitled to enforce the data processing agreement directly against the Sub-processor engaged by the primary Data Processor and (or) issue direct instructions on processing, for example, instruct the Sub-processor to delete or return Personal Data.

5.7. The Data Processor shall be responsible for requiring that the Sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the DPA and the GDPR. If the Sub-processor fails to fulfil the Personal Data protection obligations, the primary Data Processor with which/whom data processing agreement is concluded shall remain fully liable towards the Client for fulfilment of the Sub-processor's obligations. This shall not affect the data

subjects' rights provided for in the GDPR, in particular, the rights provided for in Articles 79 and 82 of the GPDR in respect of the Client and the Data Processor including the rights in respect of the Sub-processors.

6. Data Subject Rights

6.1. In view of the nature of the processing, the Data Processor assists the Client in fulfilling its obligations to respond to requests to exercise data subject rights under the Data Protection Laws.

6.2. The Data Processor shall:

6.2.1. immediately inform the Client if it receives a request from a data subject; and

6.2.2. ensure that it does not respond to such a request except on the documented instructions of the Client or as required by Applicable Laws that apply to the Data Processor. In such a case, the Data Processor, to the extent permitted, informs the Client about such a requirement.

7. Personal Data Breach

7.1. The Data Processor shall notify the Client without undue delay after becoming aware of a Personal Data breach. The Data Processor shall notify the Client within 36 hours from the moment on which the Data Processor becomes aware of the Personal Data breach so that the Client could fulfil the Client's obligations to report the Personal Data breach to the competent supervisory authority in accordance with Article 33 of the GDPR.

7.2. The obligation to assist the Client to notify the competent supervisory authority of a Personal Data breach shall imply that the Data Processor must assist the Client to obtain the information specified below which, according to Article 33(3) of the GDPR, must be indicated in the Client's notification to the competent supervisory authority:

7.2.1. the nature of the Personal Data including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data concerned;

7.2.2. the likely consequences of the Personal Data breach;

7.2.3. the measures taken or proposed to be taken by the Client to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

7.2.4. any other relevant information which is or may be necessary for the Client when preparing the notification or responding to additional requests of the competent supervisory authority related to the Personal Data breach.

7.3. If the Data Processor fails to provide all information on the Personal Data breach to the Client or later additional information becomes evident, the Data Processor shall be obliged to without undue further delay but not later than within 24 hours from the moment of becoming aware of new information give an additional notification to the Client specifying all missing information.

7.4. Upon request of the Client, in addition to the information provided for in point 7.4 hereof, the Data Processor shall provide copies of the documents, for example, the documents justifying the carried-out actions, applied measures or carried out internal inspections and conclusions of the inspections.

8. Data Protection Impact Assessment and Consultations

8.1. The Data Processor provides reasonable assistance to the Client with any data protection impact assessments, and prior consultations with supervisory authorities, which the Client reasonably considers to be required under Articles 35 or 36 of the GDPR.

9. Deletion or Return of Company's Personal Data

9.1. Upon termination of this DPA, the Data Processor shall be obliged, at the choice of the Client to delete all Personal Data processed on behalf of the Client and demonstrate to the Client that it did this and (or) return all Personal Data to the Client and in any event delete the existing copies unless the Personal Data must be stored in accordance with the laws of the European Union or its Member State.

10. Audit Rights

10.1. Subject to this Section 10, the Data Processor shall, upon the Client's request, provide the Client with all information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted

by the Client or another auditor mandated by the Client concerning the processing of the Company's Personal Data. The Client agrees to bear the costs for such audit.

11. Data Transfer

11.1. The Data Processor shall be entitled to transfer Personal Data to third countries or international organisations only after receipt of the documented instructions of the Client and in accordance with the requirements of Chapter V of the GDPR.

11.2. If Personal Data must be transferred to third countries or international organisations in accordance with European Union or Member State law which must be complied with by the Data Processor although the Client has not given instructions to do this to the Data Processor, the Data Processor shall notify the Client of the afore-mentioned legal requirement prior to transfer of data unless such legal act prohibits communication of such information.

11.3. The Data Processor shall not be entitled to carry out the following actions without the documented instructions of the Client or the particular request under European Union or Member States law in accordance with this DPA:

11.3.1. to transfer Personal Data to a data controller or a data processor in a third country or in an international organisation;

11.3.2. to transfer processing of Personal Data to a sub-processor in a third country;

11.3.3. to allow the Data Processor to process personal data in a third country.

12. Applicable Law and Jurisdiction

12.1. This DPA is governed by the laws of the Republic of Lithuania.

12.2. The DPA shall take precedence over any similar provisions related to processing of Personal Data set out in other agreements between the Parties.

12.3. Any dispute arising under this DPA, which the Parties are unable to resolve amicably, shall be submitted to the exclusive jurisdiction of the courts of the Republic of Lithuania.

13. Final provisions

13.1. The terms and conditions of this DPA shall come into force from the date of signature of the Agreement.

13.2. Each Party shall appoint a person responsible for executing the DPA:

13.2.1. on behalf of the Client: as agreed on the Order Form;

13.2.2. on behalf of Data Processor: General Counsel, e-mail: privacy@copla.com.

13.3. If the provision of Services under the Services Agreement is terminated and Personal Data is deleted or returned to the Client in accordance with this DPA, the DPA may be terminated by written notice given by either Party.

13.4. Without prejudice to any provisions of the GDPR, if the Data Processor breaches its obligations hereunder, the Client shall be entitled to order the Data Processor to suspend Personal Data processing on a temporary basis till the latter complies with the DPA or this DPA is terminated. The Data Processor shall immediately notify the Client if it cannot perform its tasks as agreed in the DPA for any reason.

13.5. The Client shall be entitled to terminate the DPA if:

13.5.1. the Data Processor substantial or persistent breaches the DPA or its obligations under the GDPR;

13.5.2. the Data Processor fails to comply with the binding decision of the court or supervisory authority in relation to its obligations provided for in the DPA or the GDPR;

13.5.3. the processing of personal data by the Data Processor has been suspended by the Client pursuant to point 13.5.1 and (or) 13.5.2 of the DPA and compliance with this DPA is not restored within a 1 month following suspension.

Annex I to the DPA

Upon entry into force of the DPA, the Client shall allow to engage the following sub-processors:

Name of sub-processor, legal entity code or individual activity certificate number or business licence number	Address of the registered office and location	Provided service	Data Location
Amazon Web Services EMEA SARL	Avenue John F. Kennedy 38, LUXEMBOURG, 1855, LUXEMBOURG	Provision of cloud computing/storage platform	Dublin, Ireland
SFDC Ireland Ltd.	Salesforce Tower Dublin, North Dock, Dublin 1, D01 W2Y3, Ireland	Provision of Slack communication platform	Frankfurt, Germany
HubSpot Ireland Limited	Ground Floor, Two Dockland Central, Guild Street, Dublin 1, D01 K2C5, Ireland	Provision of customer relationship management and customer communication platform	Frankfurt, Germany
Google Ireland Ltd	Google Building Gordon House, Barrow St, Dublin, D04 E5W5, Ireland	Provision of cloud storage platform	Frankfurt, Germany
Anthropic Ireland, Limited, CRO No. 760497	6th Floor, South Bank House, Barrow Street, Dublin 4, IRELAND	Provision of AI/large language model processing services (API)	Dublin, Ireland (deployed in our AWS infrastructure)

Annex II to the DPA

Data subjects	Processed personal data	Retention period	Processing operations
Client's employees and representatives; Client's consultants/ contractors.	Name, surname, e-mail, Service usage data.	During the provision of the Services and 30 days after the end of the Services Agreement.	The Personal Data transferred will be processed in accordance with the DPA and may be subject to the following processing activities: storage and other processing necessary to provide, maintain, and update the Services provision of the Services provided to the Client; provision of customer support and technical support to the Client; disclosures in accordance with the Agreement, as compelled by law.