Data Processing Agreement CoBoo

Version 1.0, last updated 13 November 2026

Parties

1. the organisation that uses the services of CoBoo, hereinafter: the Controller;
2. CoBoo, also trading as Lumyo, established in Hoogeveen, the Netherlands, registered with the Netherlands Chamber of Commerce under number 99516551, represented by Colin Suttner, hereinafter: the Processor.

The parties enter into this agreement because the Processor carries out phishing simulations for the Controller and provides access to the Lumyo awareness training (the Main Agreement: the accepted quotation together with the general terms and conditions of CoBoo). In doing so, the Processor processes personal data of the Controller's employees.

Article 1. Definitions

Terms such as personal data, processing, data subject, personal data breach and sub-processor have the meaning given in the General Data Protection Regulation (GDPR). Employees are the persons the Controller registers for a simulation or training.

Article 2. Subject matter and instructions

1. The Processor processes personal data only on behalf of and on the documented instructions of the Controller, and only to perform the Main Agreement. The Main Agreement and this agreement together constitute those instructions.
2. The Processor does not use the personal data for its own purposes. The Processor may use anonymised totals that cannot be traced to any person or client to improve the service.
3. If the Processor considers an instruction to infringe the GDPR, it informs the Controller immediately.
4. Which data, of whom, for what purpose and for how long is set out in Annex 1.

Article 3. Purpose and legal basis

1. The purpose of the processing is to measure and improve employees' resilience against phishing, through simulated phishing emails, reporting and training.
2. The Controller determines the legal basis (usually legitimate interest), informs employees in general terms about the programme in advance, and consults the works council where required.
3. Results are reported per department by default. Reporting per employee takes place only at the Controller's express written request, in which case the Controller is responsible for using it with care. Results are not used for sanctions against individual employees, unless the Controller has its own legal basis for doing so.

Article 4. Obligations of the Processor

1. The Processor processes only the personal data required for the service (data minimisation).

2. Anything an employee enters on a simulated login or form page is not stored. The Processor records only that something was entered, never passwords or other entered values.
3. Where reasonable, the Processor assists the Controller with a data protection impact assessment (DPIA) and a prior consultation of the supervisory authority.

Article 5. Confidentiality

Everyone at the Processor with access to the personal data is bound by confidentiality. This does not apply where a statutory obligation to disclose exists; the Processor then informs the Controller of such a request in advance, unless the law prohibits this.

Article 6. Security

1. The Processor takes appropriate technical and organisational measures against loss and unlawful processing, taking into account the state of the art, the costs and the risks to employees.
2. The measures are set out in Annex 3. The Processor may adjust them, provided the level of security does not decrease.

Article 7. Sub-processors

1. The Controller gives general authorisation for the sub-processors listed in Annex 2.
2. The Processor notifies the Controller of a new or replacement sub-processor at least 30 days in advance. The Controller may object on reasonable grounds within that period; if the parties cannot agree, the Controller may terminate the Main Agreement for the part involving that sub-processor.
3. The Processor imposes the same obligations as in this agreement on its sub-processors and remains responsible to the Controller for them.

Article 8. Personal data breaches

1. The Processor notifies the Controller's contact person of a personal data breach without undue delay and in any case within 24 hours of discovering it.
2. The notification includes, as far as known: what happened, which data and how many employees are affected, the likely consequences and the measures taken or proposed. Information not yet known follows as soon as it is.
3. The Controller decides whether the breach is reported to the supervisory authority and to employees; the Processor assists.

Article 9. Rights of data subjects

If the Processor receives a request from an employee (such as access, rectification or erasure), it forwards the request to the Controller and does not handle it itself. The Processor assists the Controller within a reasonable time in responding to such requests.

Article 10. Transfers outside the EEA

The Processor stores the personal data within the European Economic Area. Transfers outside it, including by a sub-processor, take place only on a valid basis under Chapter V of the GDPR, such as an

adequacy decision or the standard contractual clauses of the European Commission.

Article 11. Audits

1. On request, the Processor provides the Controller with the information needed to demonstrate compliance with this agreement.
2. The Controller may have an audit carried out at most once a year, with at least 30 days' notice, by an independent expert bound by confidentiality. The costs are borne by the Controller, unless the audit shows that the Processor materially fails to comply with this agreement.

Article 12. Term, retention and deletion

1. This agreement runs for as long as the Main Agreement, and thereafter for as long as the Processor still holds personal data of the Controller.
2. After the Main Agreement ends, the Processor retains the personal data, including results per employee, for no more than 12 months, so that the baseline, trend and charts, also per employee, continue if the client returns within that period. The Controller may at any time request earlier deletion or return of the data in a common file format.
3. After that period, the Processor deletes the personal data, including at sub-processors and from backups once these are overwritten, and confirms this in writing on request. Anonymised totals are not covered by this.

Article 13. Liability

1. The liability provisions in the general terms and conditions of CoBoo apply to the Processor's liability under this agreement, including the maximum per calendar year set out there.
2. That maximum applies to all claims under this agreement and the Main Agreement together; this agreement has no separate or higher maximum.
3. The Processor is not liable for damage or fines resulting from an instruction of the Controller, or from the Controller's failure to meet its own obligations under the GDPR, such as informing employees.
4. A fine imposed on the Controller by the supervisory authority is borne by the Processor only to the extent it results directly from a failure of the Processor itself, and within the limits of paragraphs 1 and 2.
5. These limitations do not apply in the event of intent or deliberate recklessness on the part of the Processor.

Article 14. Final provisions

1. In the event of conflict between this agreement and the Main Agreement, this agreement prevails as far as the processing of personal data is concerned.
2. Amendments apply only after the Controller has accepted them as described under Acceptance.
3. This agreement is governed by Dutch law. Disputes are submitted to the competent court in the district of Noord-Nederland.
4. This English version is a translation. In the event of any difference, the Dutch version prevails.

Acceptance

1. This agreement is concluded when an authorised representative of the Controller accepts it electronically when the account is created, before the first processing. The parties acknowledge that this electronic acceptance counts as a written signature (Article 28(9) GDPR and Article 6:227a of the Dutch Civil Code).
2. On acceptance, the Processor records: the name and position of the person accepting, the organisation, the date and time, and the version of this agreement. The Processor includes these details in the document and sends it to the Controller by email. That emailed document is the applicable agreement.
3. In the event of an amendment, the Controller receives an email with the new version and accepts it by logging in and agreeing again. Until then, the previous version continues to apply. If an amendment is not accepted within 30 days, either party may terminate the Main Agreement.

This agreement is accepted in the client portal; the organisation, the name and position of the signatory, and the date and time are recorded at that point.

Version: 1.0, 13 November 2026

Annex 1. Specification of the processing

Data subjects: employees of the Controller who take part in a simulation or training. Special categories of personal data (such as health data) and national identification numbers are not processed.

Component	Personal data	Purpose
Participant list	First and last name, email address, position (optional), department, site or country, language	Sending emails in the right language, breakdown by department or country
Phishing simulation	Per employee with date and time: email received, opened, link clicked, something entered (only the fact, not what), email reported	Measuring resilience, baseline, follow-up measurement and trend
Technical data on a click	IP address, browser and operating system, approximate location derived from the IP address	Distinguishing real clicks from automated scans by mail servers
Lumyo awareness training	Account (username, encrypted password), modules completed with date, knowledge test scores, certificates	Providing training, tracking progress and certificates
Reporting	Totals per department; per employee only on written request	Report to the Controller

Retention period: for as long as the Main Agreement runs, and thereafter no more than 12 months (Article 12).

Contact persons: Controller: the contact person designated by the Controller on acceptance. Processor: CoBoo, contact@coboo.nl.

Annex 2. Sub-processors

The phishing software (Gophish) and the Lumyo platform run on a server owned by the Processor in the Netherlands; no hosting provider is involved.

Sub-processor	Activity	Data	Location
Mailgun (Sinch)	Sending the simulated phishing emails	Email address, name, email content, delivery status	EU region (account on the EU environment)

Mailgun stores the message data of a domain in the EU region only within that region. Mailgun belongs to a US group (Mailgun Technologies, Inc., part of Sinch). Any access from the US is covered by the certification of Mailgun Technologies, Inc. under the EU-U.S. Data Privacy Framework; otherwise transfers are covered by the standard contractual clauses of the European Commission. The basis and conditions are set out in the Sinch data processing agreement.

Annex 3. Security measures

- Access: only the Processor itself has access to the personal data; no other persons are involved.
- Login: two-factor authentication on all management environments: the server, Gophish, the Lumyo platform and the Mailgun account.
- Encryption: all connections over HTTPS (TLS); storage and backups encrypted.
- Backups: regular backups, which are cleared along with the data after the retention period in Article 12.
- Updates: the operating system and software are kept up to date and security updates are installed promptly.
- Data minimisation: passwords and other values entered on simulation pages are never stored.
- Separation: data of different clients is kept separate and used only for that client.