



GDPR Compliance Statement

Annex to the Data Processing Agreement

How HorecaMelder, its customers and its sub-processors (including OpenAI) together meet the requirements of the General Data Protection Regulation (EU) 2016/679 and the Dutch GDPR Implementation Act (UAVG).

Provider: Co Lo Network Holding B.V., Oude Loosdrechtseweg 214, Chamber of Commerce (KvK) 32088644, the Netherlands · **Service:** HorecaMelder (horecamelder.nl) · **Contact:** info@horecamelder.nl

Version: 4 October 2026 · **Applies to:** Data Processing Agreement (Verwerkersovereenkomst) version 3 October 2026 and Privacy Notice (Privacyverklaring) version 4 October 2026

1. Purpose of this document

This annex explains, in one place, how the legal documents of HorecaMelder fit together and how the service complies with the GDPR. It is meant to be presented together with:

- the **HorecaMelder Data Processing Agreement** (Dutch original, with an English courtesy translation), between each customer and Co Lo Network Holding B.V.;
- the **OpenAI Data Processing Addendum**, executed between Co Lo Network Holding B.V. and OpenAI in October 2026, which governs OpenAI's role as sub-processor;
- the **General Terms and Conditions** (Algemene voorwaarden) and the **Privacy Notice** (Privacyverklaring) as published on horecamelder.nl.

The Dutch versions of the published documents are the legally binding texts. English translations are provided for convenience; in case of a discrepancy, the Dutch text prevails.

2. What a data processing agreement is

Under Article 28 GDPR, an organisation that has another party process personal data on its behalf must lay down binding written terms with that party. That contract is the **data processing agreement** (DPA). It records what data is processed and why, that the processor only acts on instructions, the security measures, confidentiality, the use of sub-processors, assistance with data subject requests and data breaches, audits, and what happens to the data when the service ends.

HorecaMelder has two such contracts in a chain:

Party	GDPR role	Contract that covers it
The customer (hospitality business using HorecaMelder)	Controller (Art. 4(7))	Decides why and how incidents are recorded. Accepts the HorecaMelder DPA when ordering or in the account settings; acceptance is logged with date and version.
Co Lo Network Holding B.V. (HorecaMelder)	Processor (Art. 4(8))	HorecaMelder Data Processing Agreement (Art. 28(3)).

OpenAI	Sub-processor (Art. 28(2) and (4))	OpenAI Data Processing Addendum (executed October 2026), imposing equivalent obligations on OpenAI, including the EU Standard Contractual Clauses for transfers outside the EEA.
Other sub-processors (hosting, e-mail, messaging, payments)	Sub-processors	Their own processing terms, listed in the annex of the HorecaMelder DPA (see section 7).

For HorecaMelder's own customer administration (accounts, invoices, sign-up requests), Co Lo Network Holding B.V. acts as a **controller**. That processing is described in the Privacy Notice and is not covered by the DPA.

3. The processing in brief

Element	Description
Purpose	Recording incidents in hospitality venues (refusals, violence, drugs, weapons, intoxication, first aid, work accidents and similar), producing written reports, and the related compliance registers: shift log, work accident register (Dutch Working Conditions Act, art. 9), aftercare for staff, individual venue bans, documents, certificates and contacts with police and municipality.
Data subjects	Staff and users of the customer; guests and other persons involved in an incident; contact persons of the customer.
Personal data	Names, e-mail addresses and phone numbers of users; incident notes and reports; physical descriptions of persons involved and, where needed, names; the nature of injuries of staff (no medical details); staff certificates and badge numbers; shift data.
Special and criminal data	Incident records may concern (suspected) criminal offences (Art. 10 GDPR). The customer processes these for its own protection and that of its staff, within Article 33 UAVG. The service does not ask for special categories (Art. 9); input guidance and the AI instructions exclude origin, ethnicity and similar characteristics from descriptions.
Legal basis	Determined by the customer as controller, typically legitimate interest (Art. 6(1)(f)) for safety and order, and legal obligation (Art. 6(1)(c)) for the work accident register and occupational health and safety duties.

4. Use of AI and the role of OpenAI

When a staff member chooses "**Maak verslag met AI**" (create report with AI), HorecaMelder sends to the OpenAI API: the staff member's notes, the incident category and related answers, the venue name, the role and name of the reporter and the time. The same applies when a manager uses AI to word a follow-up note. OpenAI returns a draft text that the staff member checks and confirms; the AI takes no decisions about persons (Art. 22 GDPR does not apply).

- **No training:** under OpenAI's API terms, data sent through the API is not used to train OpenAI's models.
- **Minimisation:** only the fields needed to write the report are sent; no e-mail addresses, phone numbers, ID document numbers or account data.
- **Local fallback:** if OpenAI is unavailable, the report is produced by an AI model running on HorecaMelder's own server in the EU, without data leaving the server.

- **Public data only for regulations:** OpenAI is also used to summarise public municipal bye-laws (APV); these contain no personal data.
- **Transfer:** OpenAI may process data in the United States. The transfer relies on the safeguards in the executed OpenAI Data Processing Addendum (EU Standard Contractual Clauses, Art. 46 GDPR).

5. Technical and organisational measures (Art. 32)

Measure	Implementation
Encryption in transit	HTTPS/TLS on all connections, HSTS with preload, HTTP redirected to HTTPS.
Encryption at rest	Incident notes, reports, descriptions, names, ban details, aftercare notes and archived PDF reports are encrypted field by field with AES-256-GCM before they reach the database.
Access control	Role-based access: reporting staff can only write (and see active bans at their own venue); managers see their own venue; owners see their organisation. The platform operator has no read access to customers' incidents. Revoking a role takes effect immediately.
Integrity	Incidents are append-only: they cannot be changed or deleted; corrections are added as separate, attributed amendments.
Logging	Audit log of creation, viewing, export and download of incidents and registers.
Hosting and network	Hosting in Denmark (EU) at Webdock; web application firewall in front of the service; origin locked to the firewall; database on an internal network without internet access; hardened SSH, automatic security updates.
Backups	Daily encrypted database backups (AES-256), key kept outside the server; restore tested.
Application security	Security headers (CSP, X-Frame-Options, nosniff, Referrer and Permissions Policy), login throttling, server-side permission checks on every action.

6. Retention (Art. 5(1)(e))

Data	Retention
Personal data in incidents and archived reports	Automatically anonymised after 3 years; the anonymised record remains for statistics.
Individual venue bans (max. 12 months)	Name, description and notes wiped 30 days after the ban ends; record deleted after 6 months.
Aftercare notes about staff	Wiped one year after the task was completed.
Secured camera footage (held by the customer)	The service reminds the customer to delete it once the incident is handled (Dutch DPA guidance: normally max. 4 weeks).

Retention runs automatically every night and is audit-logged.

7. Sub-processors

Sub-processor	Purpose	Location
---------------	---------	----------

Webdock.io ApS	Hosting of application and database	Denmark (EU)
OpenAI	Drafting reports with AI (no training on customer data)	United States (executed OpenAI DPA, SCCs)
MXroute	Sending e-mail (invoices, reminders)	Possibly outside the EU (see Privacy Notice)
Bird (MessageBird B.V.)	Alerts by SMS or WhatsApp to owners and managers	Netherlands (EU)
Stripe	Payments (customer data only, no incident data)	EU and United States

Customers are informed in advance of new or replacement sub-processors and may object within 14 days (DPA art. 6).

8. GDPR requirements and how they are met

Requirement	How it is met	Status
Art. 28 Processor contract	HorecaMelder DPA, accepted per customer with version and date.	In place
Art. 28(4) Sub-processor contracts	Executed OpenAI DPA and the processing terms of the other sub-processors.	In place
Art. 13/14 Transparency	Privacy Notice on horecamelder.nl (version 4 October 2026), covering all processing including the shift log, work accident register, aftercare, venue bans, documents and certificates; informing staff and guests on site is the customer's responsibility (supported by the knowledge base).	In place
Art. 5(1)(c) Data minimisation	Structured choices instead of free text; staff picked from the team, not typed; no medical details; guidance against sensitive descriptors.	In place
Art. 5(1)(e) Storage limitation	Automatic retention per data type (section 6).	In place
Art. 10 GDPR / Art. 33 UAVG Criminal data	Processing for the customer's own protection; bans never shared between organisations (sharing requires a permit from the Dutch DPA).	In place
Art. 15-21 Data subject rights	Requests forwarded to the customer; owners can view the data and export reports and registers as PDF; erasure or correction on the customer's instruction is carried out by the processor (DPA art. 7).	In place
Art. 25 Privacy by design	Encryption, role separation, append-only log, anonymisation by default.	In place
Art. 32 Security	Section 5.	In place
Art. 33/34 Data breaches	Processor notifies the customer within 36 hours of discovery (DPA art. 8), enabling the 72-hour notification to the Dutch DPA.	In place
Art. 30 Records of processing	This annex and the DPA describe the processing and can serve as the processor's record.	In place
Art. 35 DPIA	Systematic processing of criminal data may require a DPIA by the customer; the processor assists (DPA art. 9) and provides this annex as input.	In place

9. Status and follow-up

As of 4 October 2026 all contractual and transparency requirements above are in place: the HorecaMelder DPA, the executed OpenAI Data Processing Addendum, and the updated Privacy Notice. The following points are recommended good practice and are reviewed periodically:

- A model DPIA that customers can adopt for incident registration involving criminal data.
- A periodic review of the DPA and this annex by a privacy lawyer.
- A documented maximum retention period for the encrypted off-site backups.

This document describes the situation on 4 October 2026 and is provided for information. It is not legal advice. Binding texts: the Dutch originals of the Data Processing Agreement, General Terms and Conditions and Privacy Notice as published on horecamelder.nl.