Annex 1. Data Processing Agreement

Version 2.0 · 8 November 2026

This is a translation. In case of differences, the Dutch text prevails.

CONTENTS

Article 1. Subject matter
Article 2. Instructions
Article 3. Confidentiality
Article 4. Security
Article 5. Sub-processors
Article 6. Transfer outside the European Economic Area
Article 7. Rights of data subjects
Article 8. Personal data breaches
Article 9. Assistance and audits
Article 10. End of processing
Article 11. Liability and term
Annex A. Description of the processing
Annex B. Sub-processors
Annex C. Security measures

This data processing agreement forms part of the terms and conditions of mBino Services and applies when mBino Services (**Processor**) processes personal data on behalf of the Customer (**Controller**) when supplying the Services. Terms from the General Data Protection Regulation (GDPR), such as personal data, processing, data subject and personal data breach, have the meaning given in the GDPR. Other terms with a capital letter have the meaning given in the terms and conditions.

Article 1. Subject matter

1.1. Processor processes personal data only to the extent necessary to supply the Services, as described in the Agreement and in Annex A.

1.2. The Customer determines the purpose and means of the processing. The Customer warrants that the processing is lawful, that it has a legal basis, and that it informs the data subjects, such as its guests, customers, visitors and employees.

Article 2. Instructions

2.1. Processor processes the personal data only on the basis of the Customer's instructions In Writing. The Agreement, this data processing agreement and the settings that the Customer chooses in the Services count as instructions.

2.2. Processor may process personal data if a legal obligation requires this. It informs the Customer of this in advance, unless the law prohibits this.

2.3. If Processor considers that an instruction infringes the GDPR or other data protection rules, it notifies the Customer immediately.

Article 3. Confidentiality

3.1. Processor ensures that the persons who process the personal data are bound by confidentiality, and that only persons who need access for their work have access.

Article 4. Security

4.1. Processor takes appropriate technical and organisational measures to secure the personal data against loss and unlawful processing, taking into account the state of the art, the costs, and the nature and risks of the processing. Annex C describes the main measures.

4.2. Processor may adjust the measures, as long as the level of security does not decrease.

Article 5. Sub-processors

5.1. The Customer gives Processor general authorisation to engage sub-processors. The sub-processors at the time of signing are listed in Annex B.

5.2. Processor informs the Customer at least thirty days in advance, by email, in the Account or on the Website, of a new sub-processor or a replacement. The Customer may raise a reasoned objection within that period. If the parties cannot find a solution, the Customer may terminate the Service concerned with effect from the date on which the sub-processor is engaged.

5.3. Processor imposes on sub-processors the same obligations as in this data processing agreement, and remains responsible towards the Customer for their compliance.

5.4. Parties with which the Customer itself has an agreement and whose integration it switches on in the Services, such as its payment service provider, channel manager, accounting package or cash register system, are not sub-processors of Processor. The Customer itself is responsible for the transfer of data to those parties.

Article 6. Transfer outside the European Economic Area

6.1. Processor processes personal data within the European Economic Area (EEA) as far as possible. Transfers outside it only take place if an adequate level of protection is ensured, such as by an adequacy decision (including the EU-US Data Privacy Framework) or the standard contractual clauses of the European Commission. Annex B lists the sub-processors outside the EEA.

Article 7. Rights of data subjects

7.1. The Services offer functions for handling requests from data subjects, such as access to, export and anonymisation of guest profiles. If the Customer cannot handle a request itself using these, Processor assists it within reasonable limits.

7.2. If Processor itself receives a request from a data subject, it forwards it to the Customer as soon as possible, and does not respond to it on the substance itself, unless the Customer asks it to.

Article 8. Personal data breaches

8.1. Processor notifies the Customer of a personal data breach concerning the Customer's personal data without undue delay and, where possible, within 48 hours of discovering it.

8.2. In doing so, Processor provides the information it has, and supplements it as soon as it knows more: the nature of the breach, the categories concerned and the approximate number of data subjects and records, the likely consequences and the measures taken or proposed.

8.3. The Customer decides whether to notify the breach to the supervisory authority and the data subjects. Processor assists it in doing so.

Article 9. Assistance and audits

9.1. Processor assists the Customer within reasonable limits with a data protection impact assessment (DPIA) and a prior consultation of the supervisory authority, to the extent that these concern the Services.

9.2. Processor provides the Customer with the information needed to demonstrate that the obligations under this data processing agreement are being met. The Customer may, at its own expense and no more than once a year, have an audit carried out by an independent expert who is bound by confidentiality, with at least fourteen days' notice, without unreasonably disrupting Processor's business operations. Processor may instead provide a recent audit report or certificate from an independent party.

9.3. Processor may charge at its usual rates for assistance under this article and Article 7 that requires more than a limited effort, unless the assistance is needed because of a failure on the part of Processor.

Article 10. End of processing

10.1. After the end of the Agreement, Processor makes the personal data available on request and then deletes it, as provided in Article 16 of the terms and conditions. Personal data subject to a statutory retention obligation is retained by Processor for as long as that obligation lasts, and during that time it does not use the data for anything else.

Article 11. Liability and term

11.1. Article 11 of the terms and conditions applies to the liability of Processor.

11.2. This data processing agreement applies for as long as Processor processes personal data for the Customer. Provisions that by their nature are intended to continue to apply after that remain in force.

11.3. If the parties have signed a separate data processing agreement, that agreement prevails over this annex.

Annex A. Description of the processing

Service	Data subjects	Personal data	Purpose
KEOR PMS and the apps KEOR PMS Staff, KEOR Guest and KEOR Display	Guests, contact persons of companies and organisers, employees of the Customer	Name, contact details, address, date of birth, nationality, identity document details and photo (if the Customer switches this on), stay and reservation details, preferences and notes, signatures, bills and payments (no full card numbers), requests and messages; of employees: name, email, role, login details, usage and changes in the logs, push tokens	Reservations, check-in and check-out, invoicing, housekeeping and maintenance, events and groups, communication with guests, reporting and statutory registrations
KEOR POS	Employees, customers and guests of the Customer	Of employees: name, language, rights, PIN (hashed), clock-in times and, with a registered cash register system, the national register number (rijksregisternummer) (encrypted); sales; customer database (name, company, contact details, VAT number, notes); data of hotel guests via KEOR PMS (name, room, stay, signature; photos only displayed, not stored)	Till, orders, payments, customer management, room charges and the statutory cash register registration
Hosting and email	Customers of the Customer, visitors to its website, senders and recipients of email	All data that the Customer stores on its website, in its databases and mailboxes, and log files	Storage and availability

Service	Data subjects	Personal data	Purpose
Wi-Fi networks and guest portals	Users of the Customer's network	Email address or telephone number when logging in, device ID (MAC address), IP address, session data and, with location services, the position of devices	Network access, management, security and (if the Customer switches this on) location services
Telephony	Employees of the Customer and the people they talk to	Telephone numbers, names, call data (who, when, how long), voicemail, call recordings (if the Customer switches these on), messages via connected channels	Telephony, call forwarding, reporting and (if the Customer switches this on) recordings
IT management, backup and remote support	Employees of the Customer and anyone whose data is in its systems	All data in the systems, mailboxes and backups that Processor manages, and log files of remote sessions	Management, maintenance, backup, restore and support
Development of websites and software	As above, to the extent that Processor has access to production data	Data in the Customer's systems	Development, testing and delivery

The processing lasts for as long as the Agreement runs, and thereafter for as long as necessary under Article 10.

Annex B. Sub-processors

Sub-processor	Place of processing	What	For which Services
Contabo GmbH	Germany	Hosting of Processor's servers and databases, with their backups	KEOR, hosting, remote support, and network and telephony servers that Processor hosts itself
Cloudflare, Inc.	Global network; company in the US (EU-US Data Privacy Framework and standard contractual clauses)	Security and routing of web traffic (proxy, DNS)	KEOR, websites

Sub-processor	Place of processing	What	For which Services
Google LLC (Firebase Cloud Messaging)	US (EU-US Data Privacy Framework and standard contractual clauses)	Delivering push notifications to the apps; short notification texts and device tokens	KEOR PMS Staff, KEOR Guest
Apple Inc. (Apple Push Notification service)	US (EU-US Data Privacy Framework and standard contractual clauses)	Delivering push notifications on iPhone and iPad	KEOR PMS Staff, KEOR Guest
Recommand	Belgium	Peppol access point for sending and receiving e-invoices	KEOR (only if the Customer invoices via Peppol)
Module2	Belgium	Signing of fiscal data by the fiscal data module (FDM)	KEOR POS (only with a registered cash register system)

The management of Wi-Fi networks (RUCKUS Virtual SmartZone), telephone systems (Yeastar P-Series) and remote support (ScreenConnect) runs on servers that Processor hosts itself, or at the Customer's premises. The suppliers of that software are therefore not sub-processors.

Not included in this list are parties with which the Customer itself has an agreement and whose integration it switches on (Article 5.4), such as Viva (payments), Channex or Cubilis (channel manager), Clearfacts (accounting), Lightspeed (cash register) and booking sites. Email from KEOR is sent via Processor's own mail server, or via the mail server that the Customer configures itself.

Annex C. Security measures

- All connections to the Services are encrypted (HTTPS with HSTS); web traffic is routed via Cloudflare.
- Sensitive fields are stored encrypted, such as guests' document numbers, secrets for two-factor authentication, login details for integrations, keys for guest links, and results of identity scans.
- Passwords are stored only as a hash (bcrypt). Login attempts are limited.
- Two-factor authentication (TOTP with recovery codes) is mandatory for administrators of the platform, and can be made mandatory per role by the Customer.
- Rights per role. Data of different customers is separated in the software.
- An audit log records changes, including the anonymisation of guests and the resetting of two-factor authentication.
- Full card numbers and security codes of payment cards are not stored.

- Photos of identity documents are retained in accordance with the period set by the Customer, ranging from not retained to the end of the stay, and are then deleted automatically.
- Databases are not directly accessible from the internet.
- Daily backups, with a copy off the server, within the EU. Backups and log files are retained for thirty days, unless the law prescribes a longer period.
- Remote support takes place via a server that Processor hosts itself, with log files of every session, which are retained for one year (365 days). Sessions are only recorded if this has been agreed with the Customer.
- Employees and engaged persons are bound by confidentiality.