

Data processing agreement

Last updated: 21 October 2026

This is the template of the data processing agreement between a store and Yimello LLC for the Maqadi app. It applies to every store that uses the app, and is published so you can read it before you install. A signed copy, adapted to your jurisdiction where needed, is available on request at **support@maqadi.dev**.

1. Parties and roles

This agreement is between the store that installs the Maqadi app (the **controller**) and Yimello LLC, Sharjah Media City (Shams), Al Messaned, Al Bataeh, Sharjah, United Arab Emirates, Trade License 2430802.01, operator of Maqadi (the **processor**). It forms part of the **Terms & Conditions** and applies whenever the processor processes personal data on the controller's behalf through the app.

2. Subject matter and duration

The processor runs subscriptions and repeat orders for the controller's store: it records subscriptions, creates repeat orders on schedule through the store's e-commerce platform, starts payments through the store's own checkout, sends reminders and payment links to subscribers, and provides a customer portal and a merchant dashboard. The agreement lasts as long as the app is installed, and the obligations on deletion and confidentiality continue after it ends.

3. Nature and purpose of the processing

Personal data is collected from the platform and from subscribers' own actions in the portal, stored in a database on a server in Jeddah, Saudi Arabia, and used only to run the controller's subscriptions as configured by the controller. It is not used for any other purpose, not sold and not used for advertising or to train AI models.

4. Types of personal data and data subjects

Data subjects are the controller's customers who subscribe, and the controller's staff who use the app. Personal data: subscribers' names, phone numbers, email addresses, a reference to their delivery address, subscribed products, frequencies, order history created by the app, subscription status, payment outcome (succeeded or failed, never card data) and a log of messages sent. For staff: what the platform provides about the signed-in store.

5. Obligations of the processor

- Process personal data only on the controller's documented instructions, which are the settings the controller chooses in the app, subscribers' own requests in the portal, and this agreement.
- Make sure everyone with access to the service is bound by confidentiality.
- Apply the technical and organisational measures in Annex 1, and keep them at least at that level.
- Help the controller meet its obligations on security, breach notification, data protection impact assessments and requests from data subjects, as far as the nature of the processing allows.
- Tell the controller if an instruction appears to break applicable data protection law.

6. Location of processing

The database and its backups are kept only in Saudi Arabia. Emails to subscribers pass through the email provider listed in Annex 2. Where each part of the service runs is described in the **data residency statement**. The processor will not move the storage of the controller's personal data outside Saudi Arabia without the controller's written consent.

7. Sub-processors

The controller authorises the sub-processors in Annex 2. The processor will announce a new sub-processor at least 30 days in advance; the controller may object on reasonable data protection grounds and, if no solution is found, remove the app, with a pro-rata refund of prepaid fees requested through the platform. The

processor imposes data protection obligations on each sub-processor equivalent to those in this agreement.

8. Personal data breaches

The processor will notify the controller without undue delay, and in any case within 48 hours of becoming aware of a breach affecting the controller's personal data. The notice will describe what happened, the data and people likely affected, the likely consequences and the measures taken. This allows the controller to meet the 72-hour notification period of the Saudi Personal Data Protection Law.

9. Requests from data subjects

Subscribers can view, change, pause and cancel their subscriptions in the customer portal. The controller can delete a subscriber's data from the dashboard at any time. For other requests, the processor will act on the controller's instructions within 14 days.

10. Deletion at the end of the service

When the app is removed, the processor stops automatic charges and deletes the controller's personal data from the live system at once, and from backups within 35 days, when the last backup containing it expires. Only the store's ID, installation and removal dates and monthly subscriber counts are kept as the billing record.

11. Audits

The processor will make available the information needed to show compliance with this agreement, including this template, the data residency statement and a description of the security measures, and will answer reasonable written questionnaires once a year. On-site audits are possible by separate agreement, at the controller's cost and with 30 days' notice.

12. Liability and precedence

Liability under this agreement is subject to the limits in the Terms & Conditions. If this agreement and the Terms & Conditions conflict on data protection, this

agreement prevails. The governing law is that stated in the Terms & Conditions, unless a signed copy states otherwise.

Annex 1: technical and organisational measures

- **Encryption in transit:** the app, the customer portal and the website are served only over HTTPS.
- **Encryption of secrets:** the access keys the platform gives the app are stored encrypted with a key kept only on the server.
- **No card data:** card details are entered only in the platform's checkout; the app stores only subscription references.
- **Separation of stores:** every request of the app page is tied to one store after the platform confirms the signed-in store; one store cannot read another store's data. Portal links give access only to one subscriber's subscriptions and can be replaced.
- **Verified events:** events from the platform are accepted only with a valid signature.
- **Minimal logs:** logs record only the method, the path without parameters, the status and the duration; no personal data.
- **Access control:** the server accepts administrative access only with SSH keys; repeated failed attempts are blocked.
- **Backups:** the database is backed up daily within the Jeddah region, encrypted before upload with a key not kept on the server, protected from deletion for 14 days and removed after 35 days.
- **Maintenance:** operating system security updates are applied automatically.
- **Availability:** the service is checked on the server and restarted automatically if it stops responding, and is also monitored from outside.

Annex 2: sub-processors

Sub-processor	Purpose	Location
Oracle Cloud Infrastructure	Server hosting, database, encrypted backups	Saudi Arabia (Jeddah)
Rackhost Zrt.	Emails to subscribers (reminders, payment links, portal links) and email correspondence: email address and message text	Hungary (European Union)

The e-commerce platform (Salla or Zid) and the store's payment provider are not sub-processors: the controller uses them under its own agreements with them, and Maqadi only exchanges data with them on the controller's behalf.