MEKET

The amulet that keeps who you are

PRIVACY POLICY

Information on personal data processing in the MEKET service

OWNER	Carmen María Pineda Castro
TAX ID	46701588L
ADDRESS	Avda. Lluís Companys, 3, local 1, 08640 Olesa de Montserrat (Barcelona)
EMAIL	info@meketid.com
BRAND	MEKET
DOCUMENT	Privacy Policy
VERSION	v05
DATE	24 April 2026
NEXT REVIEW	After empirical calibration of the automated moderation system or when reaching 10,000 active users

1. IDENTITY OF THE DATA CONTROLLER

For the purposes of Regulation (EU) 2016/679 (GDPR) and Spanish Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights (LOPDGPD), the controller of the personal data collected through the MEKET service is:

CONTROLLER	Carmen María Pineda Castro
TAX ID	46701588L
ADDRESS	Avda. Lluís Companys, 3, local 1, 08640 Olesa de Montserrat (Barcelona)
EMAIL	info@meketid.com
WEBSITE	https://meketid.com
BRAND	MEKET

1.1. Assignment of the service to a corporate entity

The user expressly consents that the ownership of the service may be transferred to a corporate entity established by the current owner for the operation of MEKET, provided that such assignment does not entail a substantive modification of the processing purposes or service conditions. The assignment will be communicated with reasonable notice through the usual contact channels and will be valid without need for new express acceptance, without prejudice to the user's right to terminate the contract if the new conditions are not accepted.

2. WHAT MEKET IS

MEKET is a digital service delivered through a Progressive Web App (PWA) that allows the user to create and manage an emergency profile, add relevant information for urgency situations, register emergency contacts (ICE — In Case of Emergency), and generate a controlled public access via QR code and/or NFC to display minimum emergency information.

This Privacy Policy governs the processing of personal data of both registered users and the ICE contacts they add to their profile.

3. WHAT PERSONAL DATA WE PROCESS

MEKET processes the following categories of personal data:

a) Identification and profile data

- name
- full date of birth (private data kept in the user private area)
- profile photograph, only if the user chooses to upload it voluntarily

b) Contact data

- email address
- telephone number, where requested or added to the service

c) Health data voluntarily provided (special category — Art. 9 GDPR)

- blood type
- allergies
- relevant medication
- special or critical conditions
- other health data that the user decides to expressly add to the emergency profile

d) ICE contact data

- name
- telephone
- relationship to the user

e) Technical and usage data

- authentication data
- technical logs of access, security and service usage
- data required for traceability, abuse prevention, incident diagnosis and operational continuity

f) Data derived from automated image analysis

When the user uploads a photograph to the service, it is subject to a prior automated analysis for content moderation purposes (see section 5). Transient technical indicators may result from such analysis (generic visual attributes such as the presence of a face, facial occlusions, approximate estimated age ranges, content moderation classification). These indicators are not stored in association with the user beyond the binary decision of acceptance or rejection of the image and the generic reason for that decision.

MEKET does not generally request national ID, identification or medical documentation as part of the ordinary service.

4. HOW WE OBTAIN DATA

Personal data is obtained:

- directly from the user through the PWA;
- through the corporate email, when the user contacts MEKET;
- in the case of ICE contacts, through data provided by the user.

5. WHAT WE USE DATA FOR (PURPOSES)

MEKET processes personal data for the following purposes:

- to manage registration and the user account;
- to enable access to the private area and management of the emergency profile;
- to enable entry, editing and updating of health data voluntarily provided;
- to enable the optional profile photograph functionality;
- to generate and manage the controlled public access through QR code and/or NFC;
- to display the minimum public emergency profile when a third party scans the QR code or uses NFC;

- to manage the ICE contacts associated with the profile;
- to send transactional service emails (sign-up confirmation, password recovery, operational notifications, moderation alerts);
- to provide user support;
- to guarantee service security, technical traceability, abuse prevention, incident detection, recovery and operational continuity;
- to manage payments and billing for subscription plans, where applicable;
- to send commercial or informational communications about MEKET, news, improvements, related products or services, where a valid legal basis exists;
- to automatically moderate images uploaded by the user in order to prevent publication of inappropriate content, protect minors, and ensure the usefulness of the emergency service;
- to detect and report to competent authorities images that show indicia of constituting child sexual abuse material, in compliance with applicable legal obligations.

6. WHAT DATA IS DISPLAYED IN THE PUBLIC EMERGENCY PROFILE

When the user activates the service and generates public emergency access, MEKET may display to third parties scanning the QR or using NFC the following minimum public profile data:

- name;
- age calculated as an integer number of years from the date of birth (the full date of birth is not shown publicly);
- blood type, where the user has provided it;
- allergies, where the user has provided them;
- relevant medication, where the user has provided it;
- special or critical conditions, where the user has provided them;
- ICE contacts;
- profile photograph, only if the user has uploaded it, it has passed automated moderation, and the user has expressly authorised its visibility in the public emergency profile.

The purpose of this display is to facilitate assistance in an emergency situation. MEKET strictly applies the data minimisation principle (Art. 5.1.c GDPR) and does not display more public information than is necessary for that purpose.

> *The full date of birth is stored exclusively in the user private area and is used internally only to calculate the age shown publicly. It is never exposed to third parties through the QR code or NFC.*

7. LEGAL BASIS FOR PROCESSING

The applicable legal bases are as follows:

a) Performance of the contract — Art. 6.1.b GDPR

Creation and management of the account, access to the private area, service operation, generation and regeneration of the QR/NFC, operational support, transactional

communications necessary to provide the service, and management of charges for contracted subscription plans.

b) Consent — Art. 6.1.a GDPR

For processing requiring specific user authorisation, including optional functionalities such as the addition and public visibility of the profile photograph.

c) Explicit consent for health data — Art. 9.2.a GDPR

The processing of health data voluntarily entered by the user into the emergency profile, as well as its minimum disclosure to third parties through QR or NFC, is based on the explicit consent of the user under Article 9.2.a GDPR, in conjunction with Article 9 of the Spanish LOPDGPD.

> *The ordinary processing of health data in MEKET is not generally based on vital interests (Art. 9.2.c GDPR), but on the explicit consent of the user as the main legal basis of the service.*

d) Legitimate interest — Art. 6.1.f GDPR

Security measures, abuse prevention, technical traceability, incident diagnosis, backup, restoration, operational continuity and automated moderation of user-uploaded content to prevent inappropriate content and protect minors. The balance between the controller's legitimate interest, the protection of the best interest of the minor, and the rights of data subjects is documented in the corresponding Data Protection Impact Assessment (DPIA).

e) Compliance with a legal obligation — Art. 6.1.c GDPR

The detection and reporting to competent authorities of images with indicia of constituting child sexual abuse material is based on compliance with applicable legal obligations, including those arising from Article 450 of the Spanish Criminal Code, Article 17 bis of Law 34/2002 on Information Society Services and Electronic Commerce, and Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children.

f) Automated individual decision necessary for contractual or legal reasons — Art. 22.2.b GDPR

When the automated moderation system detects with high confidence that an uploaded image may constitute child sexual abuse material, the user's account will be automatically suspended as a precautionary measure. This individual automated decision is necessary for compliance with legal obligations and for the protection of the best interests of the minor, under the exception provided in Article 22.2.b GDPR.

g) Consent for commercial communications — Art. 21 Spanish LSSI-CE

Commercial communications by electronic means will be sent on the basis of the user prior and informed consent, unless another valid legal basis applies.

8. HOW CONSENT IS COLLECTED

Where processing requires consent, MEKET collects it through clear affirmative actions within the PWA or the relevant forms. Consent boxes will not be pre-ticked.

In particular, MEKET requests separately and independently:

- explicit consent for the processing of health data;
- acceptance of the addition of the profile photograph;

- authorisation for the photograph to form part of the public emergency profile;
- consent for receiving commercial communications;
- declaration of having informed the ICE contacts;
- declaration of parental authority or legal guardianship where the profile belongs to a minor.

MEKET keeps technical evidence of the consent given including, at least: account identification, date and time, version of the accepted text, channel or screen on which it was given, and current consent status (active, withdrawn, or modified). Withdrawals and modifications are likewise recorded.

9. MINORS

MEKET may be used to create profiles of minors when the management of the profile, the provision of data and, where applicable, the consent are handled by their parents or legal guardians.

Where processing is based on consent and the user is below the minimum age required by the law of the country of habitual residence to validly consent in information society services (Article 8 GDPR), such consent must be given by the holders of parental authority or guardianship.

The applicable minimum age varies between 13 and 16 years across the Member States of the European Union. The minimum age in each country is set out in Annex A of this Policy.

Any person who registers or manages a minor profile declares that they act with sufficient capacity and legitimacy to do so.

10. ICE CONTACTS (IN CASE OF EMERGENCY)

The user may add one or more ICE contacts (reference persons for emergency situations) to the emergency profile.

When adding an ICE contact, the user declares that they have previously informed that person that their data will be provided to MEKET for use as an emergency contact.

MEKET may use such data for display within the public emergency profile and, where applicable, for communications related to the purpose of the service. Pursuant to Article 14 GDPR, MEKET will provide the ICE contact with the relevant information on the processing of their data within one month from obtaining them and, in any case, before the first communication with that contact if that communication takes place earlier.

11. RECIPIENTS OF THE DATA

Personal data may be communicated to or accessed by:

- third parties who scan the QR code or use NFC, exclusively with respect to the minimum public emergency profile;
- emergency services, responders, or people who assist the user in an emergency situation;

- providers rendering services necessary for the operation of MEKET, acting as processors or technology providers under the corresponding data processing agreements (Art. 28 GDPR);
- competent authorities, when legally required, in particular in the event of detection of indicia of child sexual abuse material.

11.1. Current and planned providers

As of the date of this Policy, the technology providers of MEKET are:

- Supabase — database, authentication, and storage when enabled;
- Vercel — hosting, deployment, and edge distribution network;
- Brevo — delivery of transactional emails, marketing campaigns, wait-list email capture, and automated moderation system alerts, through differentiated sender identities;
- DonDominio — domain, DNS and corporate email management;
- Amazon Web Services (AWS) — automated image moderation services (Amazon Rekognition) and technically isolated storage of material under review or reported, where applicable;
- Stripe — payment gateway for subscription plans, to be incorporated when paid plans are activated;
- Shopify — e-commerce platform for MEKET physical products, to be incorporated when the store is activated.

MEKET does not currently envisage the transfer of personal data to clubs, federations, or event organisers by reason of the mere use or promotion of the service. This relationship will be updated if new providers are added or the scope of the processing is extended.

12. INTERNATIONAL DATA TRANSFERS

Some of the technology providers of MEKET are headquartered in or have their infrastructure partly or totally located outside the European Economic Area (EEA), notably in the United States of America. Specifically, as of the date of this Policy, international data transfers to the United States may occur in connection with the services provided by Supabase, Vercel, Brevo, Amazon Web Services (AWS), Stripe and — when activated — Shopify.

The guarantees applicable to these transfers are the following:

- Commission Implementing Decision (EU) 2023/1795, of 10 July 2023, declaring the adequacy of the level of protection offered by the EU-US Data Privacy Framework, for certified providers;
- Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914, of 4 June 2021, where applicable;
- Additional technical and organisational complementary measures foreseen contractually with each provider.

The user may request a copy of the safeguards applicable to international data transfers by writing to info@meketid.com.

13. RETENTION PERIODS

Personal data will be kept for the following periods:

- account and profile data: while the account is active or for as long as necessary to provide the service;
- ICE contacts: while they remain actively associated with the user profile;
- technical and security logs: 30 days;
- backups: according to the internal backup and recovery policy;
- billing and payment data: for the periods legally required under tax and commercial law (generally six years under Article 30 of the Spanish Commercial Code and four years under the Spanish General Tax Act);
- consents and their evidence: while the account is active and during the statutory limitation periods of any related actions;
- images under review by the moderation system: up to 10 calendar days for material pending human verification;
- images isolated in the event of reporting to authorities: 90 days from the report, extendable until the authority formally communicates the closure of the case;
- technical hashes of rejected images incorporated into the blocklist: kept indefinitely without linkage to any user, as they do not constitute personal data on their own.

When the user requests the deletion of the account, the account, the private access, and the associated public QR will be deactivated without undue delay. A 15-day security period will apply before definitive deletion, after which data will be erased, without prejudice to the retention periods applicable to backups, logs, or data that must be blocked due to legal obligation or justified technical necessity.

14. COMMERCIAL COMMUNICATIONS

MEKET may send commercial or informational communications by electronic means when the user has provided prior and informed consent, pursuant to Article 21 of Law 34/2002 on Information Society Services and Electronic Commerce (LSSI-CE).

The user may withdraw this consent at any time through the unsubscribe link in each email, through the application when the functionality is available, or by writing to info@meketid.com.

15. RIGHTS OF DATA SUBJECTS

The data subject may exercise the following rights recognised by the GDPR and the LOPDGPD:

- right of access (Art. 15 GDPR);
- right to rectification (Art. 16 GDPR);
- right to erasure or "right to be forgotten" (Art. 17 GDPR);
- right to restriction of processing (Art. 18 GDPR);
- right to data portability (Art. 20 GDPR), with respect to data provided by the user and processed by automated means on the basis of consent or contract performance;
- right to object (Art. 21 GDPR);
- right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal (Art. 7.3 GDPR);
- right not to be subject to automated individual decisions and, in particular, to obtain human intervention, express their point of view and contest the decision (Art. 22 GDPR).

Rights may be exercised:

- by email, writing to info@meketid.com;
- through the application, when the relevant functionality is available.

MEKET will respond to rights requests within a maximum period of one month from their receipt, extendable by two additional months in the case of particularly complex or numerous requests, in accordance with Article 12.3 GDPR.

The data subject may also lodge a complaint with the Spanish Data Protection Agency (www.aepd.es) or with the competent supervisory authority in their country of residence, and exercise judicial actions to defend their rights pursuant to Article 79 GDPR.

16. AUTOMATED IMAGE MODERATION AND TRANSPARENCY ON THE USE OF ARTIFICIAL INTELLIGENCE

MEKET uses automated image analysis systems based on artificial intelligence (in particular Amazon Rekognition) to moderate photographs uploaded by users before their incorporation into the profile. This information is provided in compliance with Article 50 of Regulation (EU) 2024/1689 on transparency of artificial intelligence systems.

16.1. Purposes of the analysis

The automated analysis pursues three clearly delimited purposes:

- preventing the publication of images with explicit sexual content;
- protecting minors, detecting possible minors on profiles where they should not appear (e.g. pet or object profiles) and detecting indicia of child sexual abuse material;
- ensuring the usefulness of the emergency service by verifying that person profile photographs allow reasonable identification of the holder (visible face, without significant obstructions such as helmets or glasses covering much of the face).

16.2. Three-level system

The result of the automated analysis is classified into three decision levels:

Level 1 — Automated acceptance or rejection with high clarity. When the system clearly determines that the image does not meet technical requirements (e.g. no visible face, face covered), the user receives an automated notification to retake the photo. The user may request human review by replying to that notification.

Level 2 — Doubtful image, human review. When the image is neither clearly acceptable nor clearly rejectable, it is referred to human review. MEKET has a maximum period of 10 calendar days to complete verification. During that period, the user's public emergency profile remains operational, displaying a neutral mark or the previously approved photograph where available. If the user does not respond to additional requests for information, the photograph is rejected and a new one must be uploaded.

Level 3 — Clear indicia of child sexual abuse material. When the system detects clear indicia of child sexual abuse material, the image and its technical metadata are isolated in an encrypted environment, the user's account is precautionarily suspended, and a report is made to the competent authorities (Guardia Civil and, where appropriate, INCIBE or other analogous authorities) in compliance with applicable legal obligations. Pursuant to Article 14.5.b GDPR, the user will not receive specific information on this processing when such communication would seriously obstruct the achievement of the objectives of the investigation.

16.3. Operational threshold and calibration

The Level 3 activation threshold is initially set at a confidence score equal to or above 95% on the indicators of explicit content and apparent minor age. This score corresponds to an output of the automated moderation model and does not constitute a calibrated probability. The threshold is considered a provisional parameter and is reviewed periodically by comparison with the outcomes of human review at Level 2, in accordance with the procedure documented in the Data Protection Impact Assessment.

16.4. Right to human intervention

Any automated decision to reject an image at Level 1 may be reviewed by a human upon request of the user. The request is made by replying to the automated notification, or by writing to moderation@meketid.com. MEKET will respond within a maximum period of 72 business hours.

16.5. Technical image blocklist

Images rejected by the moderation system may be added to an internal technical blocklist through a non-invertible perceptual digital hash, in order to prevent their re-incorporation by any account. This list does not link the hashes to any user nor constitutes a per-user incident record, therefore it does not imply additional personal data processing.

16.6. Absence of biometric identification

MEKET does not use the moderation system to biometrically identify the user or to confirm their identity by facial comparison. The automated analysis is limited to the generic categorisation of visual attributes for content moderation purposes and does not constitute processing of biometric data for the purpose of uniquely identifying a person within the meaning of Article 9.1 GDPR.

17. SECURITY OF PROCESSING

MEKET applies appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR) and to protect personal data against unauthorised access, alteration, loss, or improper disclosure.

Among other measures, the service incorporates:

- authentication and access management controls;
- strict separation of data by user;
- minimisation of the data exposed in the public emergency profile;
- control of public access through a non-visible token;
- public routes configured without cache;
- technical access logs with token_hash and ip_hash and limited retention;
- manual backup and restore verification;
- revocation mechanisms by token, by user, and by email;
- global kill switch for immediate public blocking of the service;
- post-incident diagnosis procedures and secret rotation;
- encrypted and isolated storage, with immutable access logging, for material under human review or reported to authorities.

18. COOKIES AND ANALYTICS

MEKET uses cookies and similar technologies in accordance with the applicable regulations (Art. 22.2 LSSI-CE) and the Cookies Guidelines of the Spanish Data Protection Agency.

Detailed information on cookies used, their purpose, duration, and third parties involved can be found in the Cookie Policy of MEKET, accessible separately from the website itself and from the footer of all service pages. Consent for non-strictly necessary cookies is collected through the cookie banner displayed when first accessing the site.

19. DATA PROTECTION OFFICER (DPO)

As of the date of this Policy, MEKET has assessed the need to designate a Data Protection Officer under Article 37 GDPR. Considering the current volume of data subjects, geographic scope, and nature of the service, a DPO has not been designated.

This decision will be reviewed when the service exceeds 10,000 active users or when the nature, scope, or volume of processing is substantially modified. In that case, a DPO will be designated and contact details will be communicated through this Policy and to the Spanish Data Protection Agency.

20. CHANGES TO THIS POLICY

MEKET may update this Privacy Policy to adapt it to legal, technical, operational, or product changes. When changes are significant, users will be notified by reasonable means through the website, the application, or email.

The current version of this Policy, together with the last update date, will always be accessible from the service. Previous versions will be kept internally for compliance-demonstration purposes.

21. CONTACT

For any query on privacy or data protection, the user may write to:

info@meketid.com

ANNEX A — MINIMUM DIGITAL CONSENT AGES IN THE EUROPEAN UNION

Article 8.1 of Regulation (EU) 2016/679 (GDPR) provides that Member States may set a minimum age between 13 and 16 years for a minor to validly give consent in relation to information society services. Below that age, consent must be given by the holders of parental authority or guardianship.

The following table reflects the minimum age in force in the EU Member States as of the date of this document. This information is updated with every review of MEKET legal framework.

MEMBER STATE	MINIMUM AGE (Art. 8 GDPR)
Germany	**16 years**
Austria	**14 years**
Belgium	**13 years**
Bulgaria	**14 years**
Czechia	**15 years**
Cyprus	**14 years**
Croatia	**16 years**
Denmark	**13 years**
Slovakia	**16 years**
Slovenia	**15 years**
Spain	**14 years**
Estonia	**13 years**
Finland	**13 years**
France	**15 years**
Greece	**15 years**
Hungary	**16 years**
Ireland	**16 years**
Italy	**14 years**
Latvia	**13 years**
Lithuania	**14 years**
Luxembourg	**16 years**
Malta	**13 years**
Netherlands	**16 years**
Poland	**16 years**
Portugal	**13 years**
Romania	**16 years**
Sweden	**13 years**

> *Note: outside the EU (United Kingdom, Norway, Iceland, Liechtenstein, Switzerland, and the rest of the world) the minimum age in force in the user country of residence will apply or, failing that, the age established by the law applicable to the contract.*