Privacy Policy

How Marvel Technology processes personal data across the Doorstone website, app and dashboard.

Version 1.1 · Last updated 29 October 2026 · Effective 5 November 2026

1. About this Policy

This Privacy Policy explains how personal data is processed through the Doorstone website, mobile application, web dashboard and related support services (together, the **Services**), in accordance with the Personal Data Protection Law promulgated by Law No. (30) of 2018 of the Kingdom of Bahrain (the **PDPL**) and the orders issued under it.

Doorstone is operated by Marvel Technology Services and Information System W.L.L., Commercial Registration No. 51902-2 (**Marvel**, **Doorstone**, **we**, **us** or **our**), with an office at Arcapita, Office 2, Building 551, Road 4612, Block 346, Bahrain Bay, Manama, Kingdom of Bahrain.

Doorstone is used by owners associations, developers, property managers and other organisations responsible for a property or community (each a **Community Customer**). The Community Customer that invited you to Doorstone is identified in the application or your invitation.

This Policy applies to residents, owners, tenants, family members, household staff, visitors, delivery drivers, authorised community representatives, website visitors, prospects and other users, and to drivers and occupants of vehicles at community gates where the Doorstone Gatehouse module is used. It should be read with the Doorstone Terms and Conditions and any privacy information supplied by your Community Customer.

2. Who controls your personal data?

The answer depends on the purpose for which the data is used.

2.1 Community data

Your Community Customer normally decides why and how the following data is used: your unit or community relationship; identity verification required for that relationship; service and maintenance requests; community documents and notices; invoices, dues and payments; violations; visitors, vehicles, gate events, number-plate readings and gate camera images (Section 3.10); and, where the community uses these features, owners-association meetings, attendance, proxies and voting records.

For that data, the Community Customer is the data controller and Marvel processes the data on its documented instructions as a data processor under a written data processing agreement. The Community Customer is responsible for its legal authority, privacy information, user permissions and retention instructions. Marvel assists it in protecting the data, in meeting its obligations to the Personal Data Protection Authority and in responding to your rights.

2.2 Doorstone operational data

Marvel is the data controller when it decides how data is used for:

- creating and administering your Doorstone account;
- authentication, fraud prevention, logs and platform security;
- responding directly to support requests and feedback;
- website enquiries and demo requests;
- cookie choices, service analytics and product improvement;
- optional Doorstone marketing; and
- Marvel's legal, audit and business administration.

If you are unsure who controls a particular record, contact us. We will answer the request or direct it to the appropriate Community Customer without unnecessary delay.

3. Personal data we process

Depending on the Services enabled for your community and how you use them, we process the following categories.

3.1 Account and contact data

- name, email address, primary and secondary mobile numbers and country code, postal address;
- username, password hash, password-reset and one-time-password records and account status;
- preferred language, notification settings and communication choices;
- an optional profile photograph, which you choose from your device gallery or take with your device camera. It is used only to display your profile, is never used for identity verification or facial recognition, and is served through a public link that can be seen by anyone who has that link; and
- customer, community, building, unit and user role.

3.2 Identity and eligibility data

- CPR or other identity number, identity-document type and expiry date;
- front and back images of a CPR card or passport where identity verification is required;
- name, nationality and date of birth extracted from or checked against the document (text recognition is performed on your device);
- ownership, tenancy, occupancy, family, household or other relationship to a unit; and
- verification result, reviewer, date and audit record.

Identity verification uses your identity document only. We do not collect a photograph of you for verification and do not process facial or other biometric data.

We treat identity documents as high-risk and restrict access to authorised personnel. A Community Customer can view your identity documents only while you have granted it access, and you can withdraw that grant at any time in the app. Identity documents are kept while the sharing consent is in place and you remain a member of the community, and are deleted within 30 days after you withdraw the consent or the membership ends, unless the Community Customer gives a documented lawful retention instruction or the document is needed for a legal claim.

3.3 Community and property data

- property, estate, community, unit, ownership, tenancy and occupancy records;
- authorised family members, household staff (with their household role, for example driver, domestic worker or gardener), representatives and role permissions;
- service or maintenance requests, descriptions, status, appointments and communications;
- photographs, video, audio, documents and other request attachments;
- community news, notices, alerts, events, offers, surveys and acknowledgements;
- visitors, deliveries, access requests, vehicle or permit information where enabled (see Section 3.10); and
- complaints, incidents, warnings and violation records.

3.4 Owners-association and governance data

Where your community uses these features:

- membership, unit entitlement and meeting eligibility;
- meeting notices, attendance, proxies, nominations and participation;
- ballots, votes, voting status, results and audit events; and
- minutes, resolutions and association documents.

Where a ballot is configured as secret, access must be limited so that an individual choice is not disclosed except where technically necessary and legally authorised. The Community Customer determines the applicable voting and record rules.

3.5 Invoice and payment data

- invoices, dues, credits, balances, rates applied and payment status;
- amount, currency, date, transaction reference, gateway used and receipt information;
- for card and Apple Pay payments through EazyPay, only the order and transaction references, status, amount, currency, authorisation code, receipt number, card brand, whether Apple Pay was used and the last

four digits of the card number;
- for BENEFIT debit card and BenefitPay payments, only the gateway's payment ID, transaction ID, reference number, result and authorisation code (no card data);
- proof-of-payment images you upload for offline payments; and
- reconciliation, refund, dispute and support records.

When you pay, you are sent to the payment provider's own page and enter your details there: the EazyPay hosted payment page of Eazy Financial Services B.S.C. (c), licensed by the Central Bank of Bahrain, for debit and credit cards and Apple Pay; or the BENEFIT payment gateway of The BENEFIT Company B.S.C. (c) for BENEFIT debit cards and BenefitPay. EazyPay is a Bahraini company; its payment page is served from data-centre servers in Australia (see Section 8). Apple Pay is also subject to Apple's own terms. Your full card number, CVV, expiry date and cardholder name are never stored by Doorstone. The provider processes payment information under its own privacy terms.

3.6 Device, usage and technical data

- IP address, device and application identifiers, push-notification identifiers, browser, operating system and app version;
- login, authentication, consent, change and security audit events;
- pages, screens, functions and timestamps associated with your use;
- diagnostic, performance and crash information, linked to your user identifier; and
- approximate location inferred from an IP address, where used for security.

3.7 App permissions

The app may request access to camera or photo storage to scan an identity document or attach evidence, notifications to send alerts, and other device functions required for a feature you choose. The operating system lets you grant or withdraw permissions. Refusing an optional permission affects only the feature that needs it.

Face ID and device biometrics: when you enable biometric login, your device operating system performs the biometric match. Doorstone receives an authentication result and does not receive or store your face image, fingerprint or biometric template.

3.8 Website enquiry, cookie and marketing data

- company, mobile number and enquiry content;
- cookie consent and preference records;
- website analytics and interaction data where permitted; and
- subscription, campaign and opt-out records.

3.9 Sensitive data

A request, attachment, violation, visitor record or other user-submitted content may incidentally contain health, religious, criminal-record or other sensitive personal data, and an identity document image may show a facial image or place of origin. Do not submit sensitive information unless it is necessary and you or the Community Customer has lawful authority to do so. We apply enhanced access and security controls where we are instructed to process such data.

3.10 Gate access, visitors and number-plate recognition (Gatehouse)

Some communities choose to enable the Doorstone Gatehouse module. Doorstone does not install cameras: it connects to the automatic number-plate recognition (ANPR) cameras and recorder that the community already operates at its vehicle gates. Communities that do not enable the module are not connected. Where it is enabled:

- **Vehicles:** plate number, plate country and category, vehicle type, make, model and colour, the unit and resident it is registered to, approval status, date of last use at a gate and dormant status.
- **Gate events:** the plate as read by the camera and the reading confidence, gate and lane, direction, date and time, the decision and its reason, the operator who acted, the unit, pass or vehicle matched, guard notes, and whether the vehicle is inside the community.

- **Gate camera images:** one still image per gate event, which may incidentally show the driver, occupants, pedestrians and other vehicles. No facial recognition or other biometric identification is performed; plates are matched as text only.
- **Visitors, contractors, deliveries and household staff:** name, mobile number and country code; where the inviting resident records them or the community requires them, email address, nationality and an identity reference (CPR or passport number); vehicle plate and description; visit type, purpose, party size, notes, validity and recurrence; pass code and link; how the pass was shared; arrival and departure times; the host unit and inviting resident; delivery company names and fleet plates.
- **Intercom records:** a resident's approval or refusal of a caller at the gate, with the caller's name, mobile number, plate, purpose and party size as entered by the guard, and a link to the gate image.

Communities that enable the module must display a sign at each ANPR lane telling drivers that plates and images are processed for access control. Gate images are deleted automatically 30 days after capture and plate numbers on gate events are masked after 365 days, unless the community sets a shorter period. Images can be viewed only by authorised staff of that community and by Marvel support staff, and every export is logged. The continuous video recorded on a community's own CCTV recorder is not sent to Doorstone; the community is responsible for it. This processing is carried out under the prior authorization of the Personal Data Protection Authority and a Data Protection Impact Assessment.

To request gate images or events relating to you, write to info@marvel-technology.com or to your community with proof of identity and the approximate date, gate and plate. We answer on the community's behalf within 15 working days.

4. How we receive personal data

We receive data:

- from you when you register, verify your identity, use a feature, make a payment or contact us;
- from your Community Customer, owner, landlord, authorised representative or property records used to invite or validate you;
- from a resident who registers you as a household member, household staff or visitor;
- from the community's gate cameras, where the Gatehouse module is enabled;
- from your device and use of the Services;
- from payment, messaging, identity-verification and support providers; and
- from competent authorities or public records where authorised by law.

When a Community Customer or resident supplies your data, the Community Customer is responsible for giving you the privacy information required by law. We also make this Policy available at registration and in the Services.

5. Why we use personal data and our legal basis

Where we rely on legitimate interests, we assess the necessity, expected benefit, impact on you and safeguards. You may object as described in Section 11.

Purpose	Main data	Legal basis	Controller
Create, secure and administer your account	Account and contact data, technical data	Performance of the service you requested; legitimate interests (security)	Marvel
Verify your relationship to a unit and community	Identity and eligibility data	Performance of the community relationship; consent for sharing identity documents with the community	Community Customer
Community services: requests, maintenance, violations, permits, bookings, events, notices	Community and property data	Performance of the community relationship; legitimate interests of the community	Community Customer
Invoices, dues and payment collection	Invoice and payment data	Performance of a contract; legal obligation (accounting records)	Community Customer

Purpose	Main data	Legal basis	Controller
Gate access control, visitor passes, entry and exit records, incident investigation	Gatehouse data (Section 3.10)	Legitimate interests of the community and residents in security and controlled access, under PDPA prior authorization	Community Customer
Notifications, announcements and service messages (in-app, push, email, WhatsApp where enabled)	Contact data, push identifiers, message content	Performance of the service; legitimate interests	Community Customer / Marvel
Activity and audit logs, fraud prevention and platform security	Technical and audit data	Legitimate interests; legal obligation	Marvel
App analytics, performance monitoring and product improvement	Usage and diagnostic data	Legitimate interests; consent for non-essential website cookies	Marvel
Optional Doorstone marketing	Contact and preference data	Consent	Marvel
Legal, audit and regulatory compliance; legal claims	Any relevant data	Legal obligation; legitimate interests	Marvel / Community Customer

6. Is providing data mandatory?

Fields are identified as required or optional at collection.

- Without required contact and account data, we cannot create or secure your account.
- Without evidence needed to validate your relationship to a unit, the Community Customer may be unable to approve community access.
- Without transaction information, a payment cannot be completed or reconciled.
- Optional profile fields, app permissions, marketing and non-essential cookies can be refused without losing unrelated core functions.

7. When we disclose personal data

We disclose only what is necessary to:

- **Your Community Customer and authorised users.** Authorised association board members, property/community managers, staff, gate operators, contractors or service providers may access information needed for their role. The Community Customer controls these roles for community data.
- **Service providers.** The providers listed below, which are contractually restricted and assessed for privacy and security.
- **A person you authorise.** For example, a family member, representative or service provider you choose, subject to role controls.
- **Authorities and legal advisers.** We may disclose data where required by a valid law, court or regulatory request; to establish, exercise or defend legal rights; or to protect people and the Services.
- **A corporate transaction.** Data may be disclosed under confidentiality in a merger, financing, restructuring or sale, with notice and protection as required by law.

Provider	Service	Data	Location
Amazon Web Services	Hosting, database, file storage and backups	All platform data, including gate images	India (Mumbai)
Eazy Financial Services B.S.C. (c) (EazyPay), licensed by the CBB	Card and Apple Pay payments on its hosted payment page	Order reference, amount, description; card details you enter on its page	Bahrain (payment page servers in Australia)
The BENEFIT Company B.S.C. (c)	Debit card and BenefitPay payments	Payment data	Bahrain

Provider	Service	Data	Location
OneSignal, Inc.	Push notifications and email	Push identifiers, email, mobile number, name, message content (which may include a visitor name or plate)	USA / Netherlands
Google LLC	Outbound email, Firebase Analytics and Performance Monitoring, web fonts	Email address and content, usage and diagnostic data, IP address	USA / EU
Meta Platforms (WhatsApp Business)	Visitor pass links and status messages, where the community enables it	Mobile number, first name, pass link, message content	USA / Ireland

We do not sell personal data. We do not disclose identifiable community data to third parties for their independent advertising. A community offer or external service remains subject to the provider's own terms and privacy notice when you choose to engage with it.

8. International transfers

Doorstone is hosted on Amazon Web Services in Mumbai, India, and some of the providers in Section 7 process data in Australia, the United States of America, the Netherlands, Ireland and other European Union member states. All of these destinations are listed in the annex to Order No. (42) of 2022 as providing adequate protection for the transfer of personal data from the Kingdom of Bahrain. Transfers are protected by encryption in transit (HTTPS/TLS) and by each provider's data processing agreement or terms, and card payments are handled by EazyPay and BENEFIT under PCI DSS.

We host Doorstone in Mumbai because the AWS Middle East (Bahrain) region is currently unavailable as a result of the regional conflict. We plan to move hosting, data storage and backups to the AWS Bahrain region once services there are restored and stable, and will update this Policy when we do.

Before adding a new destination, the responsible controller assesses the destination, vendor and legal mechanism, and transfers only to destinations recognised by the Bahrain PDPA or under an applicable authorisation, statutory exception and the safeguards required by Bahrain law. Contact us for information about the safeguards relevant to your data. We may withhold details that would compromise security or another person's rights.

9. Retention and deletion

We keep personal data only for a documented purpose and period. Where Marvel acts as processor, the Community Customer sets the period in its instructions, subject to law. The following defaults apply unless the Community Customer instructs a different lawful period, or a longer period is required for law, fraud prevention, dispute resolution or a legal hold.

Data	Default retention
Account and profile data	While the account is active; erased 24 months after the account is closed
Identity documents	While the sharing consent and membership continue; deleted within 30 days after consent is withdrawn or membership ends
Gate camera images	30 days from capture (a community may set 1 to 365 days)
Plate numbers on gate events	Masked after 365 days (a community may set 30 to 3,650 days)
Visitor records	Erased on the resident's request, otherwise 12 months after the last visit
Service requests, violations and event permits	24 months after closure
Invoices and payment records	10 years, as required for accounting records
Activity and audit logs	24 months
Read in-app notifications	Archived after 7 days
Website enquiries and marketing records	Until you opt out, or 24 months after the last contact

Data	Default retention
Backups	Overwritten on a rolling cycle of no more than 35 days

When you delete your account in the app, it is closed immediately: sign-in is blocked, every session is ended and your device push identifiers are removed from the notification provider. Your record is kept in a closed state with the community records that refer to it until the period above ends, so that the association's records remain complete. You can ask for earlier erasure of data that is no longer necessary.

Deletion from an active system does not always remove a record immediately from a protected backup. Backup data is not restored to ordinary use and is overwritten according to the cycle above. We securely delete or irreversibly anonymise data when its period ends.

10. Cookies and third-party content

We use strictly necessary storage to operate security, login and privacy choices. Analytics, advertising and third-party media/map cookies are disabled until you make an affirmative choice where consent is required.

Our preference panel provides Accept All, Reject All and category-level controls. You can withdraw or change consent at any time using Cookie Settings in the website footer. Refusing non-essential cookies does not prevent access to ordinary website content; a specific embedded video, map or audio player may remain unavailable until you choose to load it.

Third-party content may include services such as YouTube, Vimeo, Google Maps, Spotify or SoundCloud. When enabled, the relevant provider may receive your IP address, device data and its own cookie information under its privacy terms.

11. Your rights

Subject to Bahrain law and applicable exceptions, you may:

- ask whether your personal data is processed and obtain access to it, including gate images relating to you;
- ask for inaccurate, incomplete or outdated data to be corrected;
- ask for unlawful data to be blocked or erased;
- object to processing that causes substantial material or moral harm;
- object at any time to direct marketing;
- withdraw consent, without affecting earlier lawful processing;
- ask for human reconsideration of a decision made solely by automated processing (Section 12); and
- complain to Bahrain's Personal Data Protection Authority.

Access requests are normally answered free of charge within 15 working days. Valid correction, blocking, erasure and direct-marketing objections are normally handled within 10 working days. We may request proportionate proof of identity and authority. We may refuse or limit a request only where law permits and will explain the reason.

For community data, we may send the request to the relevant Community Customer and assist it. To submit a request, email info@marvel-technology.com with the subject "Privacy Request" or use the in-app support channel.

You may complain to the Bahrain Personal Data Protection Authority (www.pdp.gov.bh, info@pdp.gov.bh). We would appreciate the opportunity to address the issue first, but this does not limit your right to contact the PDPA.

12. Automated decisions

Doorstone does not use your personal data for profiling or to make a solely automated decision that has a legal or similarly significant effect on you, except the gate decisions below, which a community enables. Rules may flag an account or transaction for security review, but an authorised person must review any material restriction.

Gate access. At a gate where the Gatehouse module is enabled, a plate matched to a vehicle registered to a unit, to a valid visitor pass or to a registered delivery fleet opens the barrier automatically, and exits open

automatically. Where a community enables it, a plate differing from a registered plate by up to two characters also opens automatically. Any other vehicle is referred to a guard, who decides whether to admit it. Entry is never refused by automated means alone.

Dormant vehicles. A registered vehicle not seen at any gate for 90 days is moved to a dormant status after a warning at 76 days. You can reactivate it in the app; until then the vehicle is referred to the guard rather than refused.

You can ask for any of these outcomes to be reviewed by a person by contacting your community or info@marvel-technology.com. If our use of automated decisions changes, we will provide the required information and rights before the processing begins.

13. Security

We use risk-based technical and organisational safeguards designed to protect confidentiality, integrity and availability, in line with Article (8) of the PDPL and Order No. (43) of 2022. These include access based on job role and community, authentication controls, encryption in transit and at rest, private storage released only through time-limited links, audit logging, protected backups, secure development and change controls, vendor review, vulnerability management, staff confidentiality and incident response.

No internet service is completely secure. Keep your credentials confidential, enable device security and promptly report suspected unauthorised access or misuse to info@marvel-technology.com.

We document every personal-data breach, its effects and the remedial action taken. The responsible controller notifies the Personal Data Protection Authority within 72 hours of becoming aware of a breach, unless the breach is unlikely to affect your rights, and, if a breach is likely to create a high risk to you, informs you as required by Bahrain law and explains its nature, likely effects and protective steps.

14. Children and dependent family members

An individual must be at least 18 and have legal capacity to create and accept a Doorstone account unless a legally authorised guardian or representative acts for them. The Services are not directed to children for independent account creation.

A Community Customer or authorised adult may add limited information about a minor or dependent family member where necessary for a lawful community purpose. The person adding it must have authority and should provide only the minimum information. Contact us if you believe a minor's data was added without authority.

15. Changes to this Policy

We may update this Policy to reflect changes in law, Services or processing. We will post the new version with its effective date and give reasonable advance notice of material changes. Where law requires consent, we will request it before the new processing begins. Earlier versions will be available on request.

16. Governing law and courts

This Policy and any non-contractual dispute connected with it are governed by the laws of the Kingdom of Bahrain, without limiting mandatory rights you have under applicable law.

The competent courts of the Kingdom of Bahrain have jurisdiction, subject to any mandatory consumer forum or dispute right that cannot lawfully be excluded.

17. Contact us

Marvel Technology Services and Information System W.L.L. (Doorstone)
Commercial Registration No. 51902-2
Arcapita, Office 2, Building 551, Road 4612, Block 346
Bahrain Bay, Manama
Kingdom of Bahrain

Privacy requests and suspected breaches: info@marvel-technology.com
General support: hello@doorstone.co

Questions about this policy? Contact us at hello@doorstone.co.