POLICY

Subscriber Privacy and Data Handling Policy

Version	Owner	Approved by	Date adopted
1.0	Khaleel Ahmad, Chief Technology Officer	Khaleel Ahmad, Chief Technology Officer	9th Sept 2026

> **What measure 22 requires**
>
> Operators of public telecommunications networks and broadcasting facilities shall ensure the privacy rights of their subscribers are protected, in accordance with all applicable legislation in effect, and address privacy concerns promptly and transparently.

1. Purpose and scope

This policy sets out how Green Dot Limited handles information about its subscribers: what is held, why, who may see it, how long it is kept, and what a subscriber is entitled to ask for.

It applies to every member of staff, to contractors working on Green Dot systems, and to OCM personnel with access to Green Dot systems. It applies to subscriber information in every form — in CRM.COM, in email, on paper, in a photograph on a phone, and in network logs.

It sits above the Customer Identity Information Retention and Deletion Procedure, which deals in detail with one particular category: proof-of-identity documents.

2. The legal position

Trinidad and Tobago's Data Protection Act 2011 is partially proclaimed. The general private-sector obligations have not been brought into force. Green Dot nonetheless treats the Act's principles as the standard it works to, for three reasons: the Authority's framework requires privacy rights to be protected in accordance with applicable legislation and does not wait for full proclamation; the remaining parts may be proclaimed at any time; and the principles are ordinary good practice.

The Telecommunications Act and Green Dot's concession also impose confidentiality obligations regarding communications carried over the network. Nothing in this policy authorises Green Dot to inspect the content of a subscriber's communications.

Green Dot is not on the Financial Intelligence Unit's list of supervised entities. It has no statutory customer due-diligence obligation. Identity documents are collected because Green Dot has a legitimate business need for them, not because law requires it — and that distinction governs how long they may be kept.

3. Principles

1. Collect only what is needed. If a piece of information is not required to provide, bill or support the service, or to meet a legal obligation, Green Dot does not ask for it.

2. Use it only for the purpose it was collected for. Subscriber information is not used for anything the subscriber would not expect.
3. Keep it accurate. Where a subscriber tells Green Dot their details have changed, the record is corrected.
4. Keep it no longer than needed. Every category of information has a retention period and information is deleted at the end of it.
5. Keep it secure. Access is limited to those who need it for their work, and systems holding it are protected accordingly.
6. Be open about it. A subscriber who asks what Green Dot holds about them, and why, gets a straight answer.

4. What Green Dot holds

Category	Examples	Why it is held
Identity and contact	Name, address, telephone, email	To identify the subscriber and communicate with them
Proof of identity	Photograph or number of a national ID, driver's permit or passport	To confirm the person contracting is who they say they are; to support debt recovery; to respond to a court order or police request
Account and billing	Account number, plan, payment history, balance	To bill for and administer the service
Service and technical	Installation address, equipment serial numbers, IP allocation, service configuration	To provide and maintain the service
Support	Tickets, correspondence, call notes	To resolve faults and answer queries
Network logs	Connection records, authentication events, system logs	To operate the network, diagnose faults and investigate security incidents

Green Dot does not monitor, record or retain the content of subscribers' communications, and does not build profiles of subscriber browsing for its own purposes or for sale.

5. Who may see it

Who	Extent of access
Green Dot staff	Only what their role requires. Sales and support see account and contact records; engineering sees technical and network records; billing sees payment records.
OCM personnel	Only where the group provides a system or service that requires it, under the intra-group access agreement, and on the same terms as Green Dot staff.
Contractors	Only what a specific piece of work requires, under a written access agreement containing confidentiality and return-or-destroy obligations.

Who	Extent of access
Suppliers of systems	Only as necessary to provide and support the system, under the terms of the supply contract.
Law enforcement and courts	Only on a lawful request — a court order, a warrant, or a request the Chief Technology Officer is satisfied Green Dot is obliged to answer. Every such disclosure is recorded.
Anyone else	Not without the subscriber's consent.

Access is by named individual account. Shared logins are not used for systems holding subscriber information.

6. How long it is kept

Category	Retention	From
Identity and contact	Duration of the account plus 2 years	Account closure
Proof-of-identity documents	See the Retention and Deletion Procedure	—
Account and billing	7 years	End of the financial year in which the transaction fell
Service and technical	Duration of the account plus 1 year	Account closure
Support records	3 years	Closure of the ticket
Network logs	As configured on each system; currently 30 days on the central log platform	Generation
Incident records	6 years	Closure of the incident

Where a dispute, a legal claim or a regulatory matter is live, the information relevant to it is held until that matter is concluded, whatever the ordinary period says.

7. Subscriber requests

A subscriber may ask what Green Dot holds about them, ask for a correction, or raise a concern about how their information has been handled. Green Dot answers.

Request	Timeframe	How it is handled
What do you hold about me?	30 days	Verify identity, compile the record, provide it in writing
Correct this detail	10 working days	Verify identity, correct the record, confirm in writing
Delete my identity document	30 days	Assess against the Retention and Deletion Procedure; act or explain why not
Complaint about handling	Acknowledge in 5 working days; substantive answer in 30 days	Chief Technology Officer investigates and responds in writing

Handling a request

1. Verify that the person asking is the subscriber. Do not send subscriber information to an unverified requester.
2. Pass the request to the Chief Technology Officer, who owns every privacy request. Support staff do not answer them directly.
3. Log the request — who, what, when received, when answered, what was provided.
4. Answer in writing, within the timeframe.
5. Where a request is refused, say so plainly and give the reason.

Requests that reveal a possible breach — a subscriber reporting that someone accessed their account, or that they received another customer's information — are incidents. Open an incident record and follow the Incident Response Procedure.

8. When something goes wrong

A breach of subscriber privacy is a cybersecurity incident. It is handled under the Incident Response Procedure and, where it meets the threshold, notified to the Authority within 24 hours under measure 17.

- Any incident touching subscriber personal information is treated as severity S1 until established otherwise.
- Affected subscribers are told what happened, what information was involved, what Green Dot is doing, and what they should do — promptly, and without waiting for the investigation to conclude.
- Where the facts are still uncertain, subscribers are told that too. Silence while establishing the position is worse than an incomplete but honest account.

9. Publishing this

Green Dot's Customer Terms and Conditions at clause 11.1 promise subscribers a Customer Privacy Policy. A subscriber-facing version of this policy, written for customers rather than for staff and the Authority, is published on the Green Dot website and referenced from the Terms and Conditions.

Publication is what makes the transparency limb of measure 22 real. A privacy policy held internally satisfies the first half of the measure and not the second.

10. Responsibilities

Role	Responsibility
Chief Technology Officer	Owns this policy. Handles every subscriber privacy request and complaint. Approves every disclosure to a third party. Decides on breach notification to subscribers.
Head of Engineering	Ensures systems holding subscriber information are secured and access is limited. Ensures retention periods are technically enforced where they can be.
Network Administrator	Applies access controls. Reports any suspected exposure immediately.
All staff and contractors	Handle subscriber information only for their work. Do not copy it to personal devices or accounts. Report anything that looks like exposure at once.

11. Review

Reviewed annually under the Annual Review Protocol, and sooner if the Data Protection Act is further proclaimed, if the Authority issues guidance, or following any privacy incident.