MERIDIAN RETAIL GROUP

Breach / Incident Register

GDPR Article 33(5)

Generated 2026-06-30

CONFIDENTIAL — This document contains sensitive information about data protection practices. Distribution should be limited to authorized personnel and supervisory authorities upon request.

Summary

4	0	1	1
TOTAL INCIDENTS	CRITICAL	HIGH	PENDING DPA NOTIFICATIONS

By Status

Status	Count
INVESTIGATING	1
CONTAINED	1
CLOSED	2

All Incidents

ID	Title	Type	Severity	Status	Discovered	Affected Records
INC-2026	Unauthorized Database Query — Customer DB	UNAUTHORIZED ACCESS	HIGH	INVESTIGATING	2026-02-12	15000
INC-2026	Vendor Data Processing Violation — Klaviyo	VENDOR INCIDENT	MEDIUM	CONTAINED	2026-01-08	850000
INC-2025	Lost Employee Laptop — Amsterdam Office	DATA LOSS	LOW	CLOSED	2025-11-28	45
INC-2025	Phishing Attack Targeting Finance Team	PHISHING	MEDIUM	CLOSED	2025-09-15	0

1. Unauthorized Database Query — Customer DB

HIGH INVESTIGATING

Incident ID	INC-2026-0002
Type	UNAUTHORIZED ACCESS
Discovered	2026-02-12 11:20
Discovered By	Database Administrator
Discovery Method	Routine audit log review flagged unusual query pattern
Affected Records	15000
Affected Subjects	Customers
Data Categories	IDENTIFIERS
Contained At	—
Resolved At	—
DPA Notification Required	Yes
Notification Deadline	2026-02-15 11:20

Description

Audit logs revealed an unauthorized SELECT query against the customer database from a developer staging environment. The query returned ~15,000 customer email addresses. Investigation ongoing to determine if data was exfiltrated.

DPA Notifications

Jurisdiction	Status	Date
General Data Protection Regulation (GDPR)	DRAFTED	—

Timeline

Timestamp	Event	By
2026-02-12 11:20	Suspicious Query Detected — DBA identified unusual SELECT * query on customer_emails table from staging environment IP.	Alex Petrov
2026-02-12 12:00	Incident Escalated to Privacy Team — Query returned 15,000 records. Escalated to DPO for breach assessment.	James Mitchell
2026-02-12 13:30	Developer Account Suspended — Staging environment access revoked. Developer's corporate account temporarily suspended p ending investigation.	James Mitchell
2026-02-13 05:00	Forensic Analysis Started — IT Security reviewing network logs, endpoint activity, and cloud storage for signs of data exfiltration.	James Mitchell

2. Vendor Data Processing Violation — Klaviyo

MEDIUM CONTAINED

Incident ID	INC-2026-0001
Type	VENDOR INCIDENT
Discovered	2026-01-08 06:00
Discovered By	Privacy Officer (Maria Torres)
Discovery Method	Annual vendor review identified scope creep in data processing

Affected Records	850000
Affected Subjects	Customers, Newsletter subscribers
Data Categories	IDENTIFIERS, BEHAVIORAL
Contained At	2026-01-15 04:00
Resolved At	—
DPA Notification Required	No
Notification Deadline	—

Description

Discovered that Klaviyo was processing customer data for their own product improvement purposes beyond the scope authorized in our DPA. Identified during annual vendor review when Klaviyo disclosed updated terms.

Containment Actions

1. Formally objected to Klaviyo's additional processing
2. Disabled analytics sharing features in Klaviyo settings
3. Requested written confirmation of data deletion for unauthorized purposes

Timeline

Timestamp	Event	By
2026-01-08 06:00	Violation Discovered — During annual vendor review, discovered Klaviyo's updated terms include processing customer data for p roduct improvement — beyond DPA scope.	Maria Torres
2026-01-10 09:00	Formal Objection Sent — Sent formal letter to Klaviyo objecting to unauthorized processing and requesting immediate cessation.	Maria Torres
2026-01-15 04:00	Klaviyo Confirms Compliance — Klaviyo confirmed they have disabled analytics processing for our data and will delete any derived datasets within 30 days.	Maria Torres

3. Lost Employee Laptop — Amsterdam Office

LOW CLOSED

Incident ID	INC-2025-0015
Type	DATA LOSS
Discovered	2025-11-28 13:00
Discovered By	HR Manager (self-reported)
Discovery Method	Employee reported lost device to IT helpdesk
Affected Records	45
Affected Subjects	Employees
Data Categories	EMPLOYMENT, FINANCIAL
Contained At	2025-11-28 14:00
Resolved At	2025-12-02 05:00
DPA Notification Required	No
Notification Deadline	—

Description

HR manager's laptop lost during train commute between Amsterdam and Rotterdam. Laptop contained local copies of e mployee performance reviews and compensation data. Device was encrypted with BitLocker and had remote wipe capability.

Containment Actions

Remote wipe initiated via Intune MDM. Corporate account credentials reset. VPN certificate revoked.

Root Cause

Employee left laptop bag on train. No policy violation — device was encrypted and protected.

Lessons Learned

1. Remind employees of secure transport policies
2. Consider reducing local data storage — migrate to cloud-only workflows
3. Track policy was already in place and effective

DPA Notifications

Jurisdiction	Status	Date
General Data Protection Regulation (GDPR)	NOT REQUIRED	—

Timeline

Timestamp	Event	By
2025-11-28 13:00	Lost Device Reported — HR manager reported losing laptop bag on NS Intercity train.	James Mitchell
2025-11-28 14:00	Remote Wipe Initiated — IT triggered remote wipe via Microsoft Intune. Device pinged and wipe command acknowledged.	James Mitchell
2025-11-29 03:30	Remote Wipe Confirmed — Intune dashboard shows wipe completed successfully. BitLocker recovery key rotated.	James Mitchell
2025-12-02 05:00	Incident Closed — No data breach determined. Encryption + successful remote wipe means negligible risk to data subjects. No DPA notification required.	Maria Torres

4. Phishing Attack Targeting Finance Team

MEDIUM CLOSED

Incident ID	INC-2025-0012
Type	PHISHING
Discovered	2025-09-15 05:30
Discovered By	IT Security Team
Discovery Method	Employee reported suspicious email to IT helpdesk
Affected Records	0
Affected Subjects	Employees
Contained At	2025-09-15 06:15
Resolved At	2025-09-20 10:00
DPA Notification Required	No
Notification Deadline	—

Description

Sophisticated spear-phishing emails sent to 5 finance team members impersonating the CEO, requesting urgent wire transfers. Two employees clicked the link but did not enter credentials. No data breach occurred.

Containment Actions

Blocked sender domain, quarantined all related emails, forced password reset for affected accounts, revoked active sessions.

Root Cause

Attacker used publicly available LinkedIn data to craft targeted phishing emails. Email security gateway did not flag the domain (newly registered).

Lessons Learned

1. Implement DMARC enforcement on all company domains
2. Deploy email link scanning/sandboxing
3. Conduct quarterly phishing simulations
4. Add finance-specific wire transfer verification procedures

Timeline

Timestamp	Event	By
2025-09-15 05:30	Incident Reported — Finance team member reported suspicious email requesting urgent wire transfer to IT helpdesk.	James Mitchell
2025-09-15 05:45	Investigation Started — IT Security identified 5 similar emails targeting finance team. Analysis of email headers and links initiated.	James Mitchell

2025-09-15 06:15	Incident Contained — Sender domain blocked, malicious emails quarantined across all mailboxes. Affected accounts password-reset.	James Mitchell
2025-09-20 10:00	Incident Closed — No data breach confirmed. Remediation complete. Phishing training scheduled for all staff.	James Mitchell