Privacy & Data Protection Configuration Export — Core Banking (Temenos T24)

privacy and data protection configuration export — the documented data protection settings and record keeping · settings read from the system of record · synthetic assessor-grade test document

Export ID	SOU-EXP-0100
System	Core Banking (Temenos T24)
Exported by	Mei-Lin Tan (IT Operations Manager)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A privacy and data protection configuration export — the documented data protection settings and record keeping for Core Banking (Temenos T24): the current settings as held by the system, section by section, with the compliance status against the applicable baseline. It reports state; it does not describe intent. Settings shown as non-compliant carry a remediation ticket.

2. Data leakage prevention (DLP)

Setting	Value	Status
DLP on endpoints	Endpoint DLP agent on all managed devices: sensitive-data patterns (personal information, cardholder data) blocked from removable media and unapproved cloud storage	Compliant
DLP on email and web	Email DLP rules quarantine outbound messages carrying unapproved sensitive data; web gateway DLP inspects uploads	Compliant
DLP on network	Network DLP sensors on internet egress; incidents routed to the security operations queue	Compliant
Detected and prevented disclosures (30 days)	27 blocked, 6 released after review	Compliant

3. Privacy notices and public-facing services

Setting	Value	Status
Privacy policy on external-facing websites	Published in plain language, organised for navigation; version-controlled documentation with record keeping of each revision	Compliant
Privacy policy on mobile applications and digital services	Presented at first use and linked from settings; plain language; documented procedures for updates	Compliant
Information for the public to make an informed decision	What is collected, why, who it is shared with, how to access and correct it, how to complain	Compliant

4. Personal information in records and transmissions

Setting	Value	Status
Personally identifiable information in audit records	Limited to the elements identified in the privacy risk assessment (user id, timestamp, action); no names or account numbers in logs	Compliant

Setting	Value	Status
Security and privacy attributes on transmission	Classification and privacy labels associated with information exchanged between systems and components; labels validated on receipt	Compliant
Differential privacy for reported results	Non-deterministic noise added to published aggregate statistics before release; per-query privacy budget enforced	Compliant
Records management	Records of processing and the personal-information holdings register maintained as controlled documentation; retention period applied	Compliant

5. Control framework mapping

Framework	Indicative mapped controls
NDB Scheme	Assessment, Notification
APRA CPS 234	Information security capability, Control testing, Incident notification
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23

Exported from the management console; integrity hash recorded in the evidence register. Reviewed by the control owner and second-line risk.