DOCUMENT 1 OF 3 · 16 PAGES

Retail AI-DPIA

AI-specific Data Protection Impact Assessment for retail personalisation — GDPR Article 35 / CPRA / sector-specific, with necessity & proportionality, risk-to-rights assessment, mitigations and named DPO sign-off.

Audience · Data Protection Officer, Privacy / Legal, model owner, business owner, security, DPA / regulator interface
Companion documents · Retail Recommender Model Card · Retail Personalisation Risk Register
Use as · Audit-grade artefact requiring named human sign-off
Version · v1.0 · 2026-05

§ 1

Scope, lawful basis & trigger

A formal DPIA is required under GDPR Article 35 where processing is likely to result in a high risk to the rights and freedoms of natural persons. Retail AI personalisation typically meets the threshold — large-scale processing of behavioural data, profiling, automated decision-making influence — and is on the EDPB list of operations always requiring a DPIA.

Field	Detail
Initiative	[Retail personalisation surface — e.g. homepage, PDP, email, app, in-store clienteling]
Controller	[Legal entity name + role]
Joint controllers / processors	[List with contractual basis]
DPIA trigger	Art. 35(3)(a) systematic & extensive profiling · Art. 35(3)(b) large-scale processing · EDPB list
Lawful basis	Art. 6(1)(a) consent · 6(1)(b) contract · 6(1)(f) legitimate interest (with LIA) — selected per purpose
Special category data?	No (default) · if Yes, additional Art. 9 basis required
Children?	No (default for adult retail) · if Yes, Art. 8 conditions apply
DPIA author / DPO	[Named]

> **Boundary.** This DPIA covers personalisation processing. Separate DPIAs exist for account management, payments, fraud, and other workflows that may share data.

§ 2

Description of the processing

Nature of the processing

- Collection of behavioural events (page views, search, item interactions, cart, purchase, returns, app events, email opens / clicks, store visits where applicable)
- Aggregation into identity-resolved profiles (anonymous / authenticated)
- Feature derivation (recency, frequency, monetary, affinities, embeddings)
- Inference / scoring against personalisation models (retrieval + ranking)
- Serving personalised content (product recommendations, search ranking, email content, push notifications, on-site placements)
- Retention for model training and offline evaluation

Scope

Dimension	Value
Data subjects	Customers (registered) · visitors (anonymous) · loyalty members
Volume	[Customers / visitors per period]
Geographic scope	[Jurisdictions covered]
Period	Ongoing
Channels	Web · app · email · store · push

Context

Retail personalisation operates in a competitive environment where individuals expect tailored experiences. Concerns include over-personalisation (filter bubbles), price discrimination, exposure of sensitive inferences (e.g. health, financial situation) and intrusion into in-store presence. This DPIA addresses each.

§ 3

Data inventory · categories & sources

Category	Examples	Source	Pseudonymised?	Retention
Identifiers	anonymous_id (cookie / device), user_id, email hash	Web SDK · CDP	anonymous_id ✓ · user_id pseudonymous	24 mo inactivity
Account data	Name, email, billing address, marketing preferences	Account system	—	Per account-management policy
Behavioural events	Page views, item views, cart, purchase, search, click, app events	Web/app SDK	—	13 mo hot · 24 mo warm
Transaction data	Orders, returns, refunds (for personalisation)	Order system	—	Per tax law (long); analytical copy 24 mo
Channel context	Device class, OS, IP-derived region, locale, referrer	Web/app SDK	IP hashed	13 mo
Marketing engagement	Email opens / clicks, push opens, notification dismissals	CRM	—	24 mo
Inferred attributes	Category affinities, price tier, lifecycle stage	Derived	—	While active + 24 mo
Consent state	Per-purpose flags + timestamps	CMP	—	Indefinite (legal record)
Store / clienteling (if applicable)	POS, appointment, in-store dwell (with explicit consent)	Store systems	—	13 mo

Out of scope. Special-category data (Art. 9) and biometric data are not used for personalisation. Inferred attributes that would amount to special-category inferences (health, religion, sexual orientation) are blocked by feature-acceptance policy.

§ 4

Purposes & lawful basis per purpose

Purpose	Lawful basis	Necessary data	Notes
On-site product recommendations (anonymous visitors)	Legitimate interest (with LIA)	Session events, item catalog, anonymous_id	Easy opt-out path; cookie consent governs ad / analytics cookies
Personalised email content (registered marketing opt-in)	Consent (Art. 6(1)(a))	Engagement history, affinities, transaction history	Granular per-purpose consent; one-click unsubscribe
Personalised push notifications	Consent	Engagement, recency	OS-level + app-level opt-in
Loyalty programme personalisation	Contract (Art. 6(1)(b))	Account, loyalty transactions	Necessary for programme benefits
Cart abandonment / lifecycle messages	Legitimate interest or consent (per jurisdiction)	Cart state, contact	PECR / ePrivacy alignment; opt-out path
Re-marketing to existing customers	Legitimate interest or consent (per jurisdiction)	Identifiers, suppression lists	Honour GPC / Do Not Track signals
Store clienteling (assisted)	Consent	Identifiable in-store presence	Visible signage + opt-in
Model training & evaluation	Same as the operational purpose	Aggregated / pseudonymised feature stores	Internal use only; not shared

Legitimate-interest assessments (LIAs) are filed alongside this DPIA and revisited annually. Consent records (Art. 7) are stored in the consent ledger with timestamp and proof-of-action.

§ 5

Necessity & proportionality assessment

The processing must be necessary for the stated purposes (no less-intrusive way to achieve the same outcome) and proportionate (the impact on data subjects is balanced against the legitimate benefit).

Test	Assessment
Could the purpose be achieved with less data?	Yes — non-personalised baseline (popular / editorial) is implemented as fallback and as the holdout. Personalisation is the marginal layer.
Could it be done at the cohort level rather than individual?	For some surfaces yes (segment-level email content); evaluated per surface.
Is the data the minimum necessary?	Feature acceptance policy excludes data not justified by a model performance gain or business need; reviewed quarterly.
Are retention periods the minimum?	13 / 24 month tiers documented in § 3; reviewed annually.
Does the personalisation align with reasonable expectations?	Transparency notice describes processing; surfaces visible to the customer; in-store opt-in.
Are vulnerabilities considered?	No targeting based on vulnerability inferences; promotional messaging guardrails for credit-card / debt-related products.

§ 6

Risk assessment · rights & freedoms

Risk	Likelihood	Severity	Mitigation	Residual
Unlawful processing without valid lawful basis	Low	High	LIA on file · consent ledger live · per-purpose enforcement at serve-time	Low
Consent withdrawal not honoured promptly	Medium	High	Withdrawal SLA 24 h with CI test; cascade to feature store	Low
Profiling leads to unjustified differential treatment (price, offer)	Medium	High	Fairness guardrails; no protected-class proxies; pricing policy bans personalised price for same SKU/ configuration outside documented exceptions	Medium
Inference of special-category attributes	Low	High	Feature acceptance policy; quarterly proxy review	Low
Manipulation / dark patterns	Low	Medium	UX governance; honest defaults; opt-out parity; ad-content standards	Low
Filter bubble / serendipity collapse	Medium	Medium	Diversity post-processor; category caps	Low
Re-identification of pseudonymised data	Low	High	Combination-control via access matrix; key segregation; risk re-test on data set release	Low
PII leakage into model / output	Low	High	Pseudonymisation before training; output filters; red-team	Low
Cross-border transfer concerns	Per use	High	SCCs / TIA / DPF; vendor data-residency commitments	Low
Sub-processor failure	Medium	High	DPA + audit rights + inventory + change-notice	Low
Inadequate transparency to data subjects	Medium	Medium	Layered privacy notice; in-product disclosures; FAQ	Low
Data-subject rights not actioned in time	Medium	Medium	DSR workflow with 30-day SLA; access to model-derived data extended	Low

§ 7

Mitigations · controls map

Mitigation	Implementation	Owner
Granular consent (per purpose)	CMP with named purposes (analytics · personalisation · advertising · email · push)	Privacy + Eng
Consent enforcement at serve-time	Personalisation request rejected if consent not present for the purpose; fallback to non-personalised	Engineering
Consent withdrawal propagation	Event fans out to feature store TTL, online cache invalidation, audit log within 24 h	Engineering + DPO
Pseudonymisation	PII redacted before event ingest; identifiers hashed; access matrix segregates raw and pseudo stores	Data eng + Security
Feature acceptance policy	Quarterly review of features for proxy / special-category risk	Model risk + DPO
Fairness guardrails	Exposure-parity and outcome-parity monitors on protected proxies; auto-pause on red breach	Model owner
Transparency notice	Layered notice + in-product disclosures + FAQ describing personalisation	Privacy
DSR workflow	Request → triage → AI-derived data extracted → response ≤ 30 d (with extension protocol)	Privacy + Eng
DPA & sub-processor inventory	All processors under DPA; inventory with renewal schedule	Privacy + Procurement
International transfer	SCCs · TIA · regional residency where contractable	Legal + Eng
Encryption	TLS 1.3 in transit · AES-256 at rest · KMS-managed keys · rotation policy	Security
Logging & audit	OWASP-aligned logging; immutable retention; SIEM forwarding	Security
Access controls	RBAC matrix · quarterly access review · least privilege	Security + DPO
Breach response	72 h GDPR notification capability; runbook tested; comms templates pre-drafted	Security + Privacy

§ 8

Data-subject rights handling

Right	Source	How handled	SLA
Right to be informed	Art. 13–14 GDPR · CPRA notice-at-collection	Layered privacy notice; in-product disclosures	At collection
Right of access	Art. 15 · CPRA	Account export + AI-derived data extract	30 days (+30 d extension)
Right to rectification	Art. 16	Account self-service + verified requests	30 days
Right to erasure	Art. 17 · CPRA	Cascading deletion: account · events · features · backups (best-effort)	30 days
Right to restrict	Art. 18	Suppression flag enforced at serve-time	Without undue delay
Right to portability	Art. 20	Machine-readable export of provided data	30 days
Right to object	Art. 21	Especially absolute for direct marketing; immediate stop	Immediate for marketing
Rights re automated decisions	Art. 22	Personalisation is not solely automated decision-making with legal or similarly significant effect; documented	—
Right to opt out of sale / share	CCPA / CPRA · GPC	Global Privacy Control honoured; "Do Not Sell or Share My Personal Information" link	Immediate
Right to correct (CA)	CPRA	Same as rectification + AI-derived corrections re-propagated	45 days (CA)
Right to limit SPI use (CA)	CPRA	SPI not used for personalisation by default; documented	—

§ 9

International transfers & sub-processors

Transfer inventory

Recipient	Role	Region	Transfer mechanism	TIA on file
[Cloud platform A]	Compute / storage	EU · US	SCCs · supplementary measures	
[Foundation-model API B]	Inference	US	SCCs · DPF where applicable	
[Email service C]	Delivery	EU	—	—
[Analytics D]	Telemetry (pseudonymised)	EU · US	SCCs · IP truncation	
[Ad partner E]	Suppression / measurement	US	SCCs · DPF	

Sub-processor change-notification

- Each processor is contractually required to notify of sub-processor changes with advance notice
- Right to object preserved (with proportionate remedies)
- Inventory reviewed quarterly; material changes reviewed before approval

§ 10

Profiling, automated decisions & transparency

Article 22 boundary

Personalisation produces decisions about content surfacing, not legal or similarly significant decisions about the data subject. Eligibility, pricing of credit, employment and equivalent decisions are out of scope; if any are introduced, this DPIA must be revised.

Transparency artefacts

- Layered privacy notice with section on personalisation
- In-product disclosure on personalisation surfaces ("Recommended for you" labels, "Why am I seeing this?" affordance where present)
- FAQ with worked examples and opt-out paths
- Cookie consent banner per applicable jurisdiction (GDPR / ePrivacy / CPRA / others)

Behavioural advertising boundary

This DPIA focuses on first-party personalisation. Behavioural advertising to third parties is governed by separate ad-tech DPIA, including GPC handling and audience-share controls.

§ 11

Consultation requirements

Stakeholder	When	Outcome
DPO	Throughout DPIA development	Sign-off (mandatory)
Data subjects (sample)	Where practical; e.g. user research	Documented insights
Representatives	If applicable	
Works council / employee reps	If processing employee data	N/A for customer personalisation
Supervisory authority (DPA)	If residual high risk remains	Prior consultation per Art. 36
Security	For Art. 32 controls	Signed posture
Legal	For lawful basis, transfers	Signed posture

Prior consultation (Art. 36). If residual risk is High and cannot be reduced further, the controller must consult the supervisory authority before processing begins. Document the determination here.

§ 12

Annual review & re-DPIA triggers

- New purpose added to personalisation
- New category of data or new source
- New processor or sub-processor with material role
- New international transfer mechanism
- Material change to retention or pseudonymisation
- Significant incident or near-miss
- Regulator clarification or new law (e.g. EU AI Act high-risk overlap, new state laws)
- Annual review cadence

Change log

Date	Trigger	Section updated	Approver
	Initial	All	
	Annual review	All	

§ 13

Decision & residual-risk acceptance

Risk domain	Residual	Acceptance authority
Confidentiality (unauthorised access / disclosure)		DPO
Integrity (data & model)		Security
Profiling / differential treatment		DPO + business
Cross-border transfer		Legal
Vendor / sub-processor		Procurement + DPO

Decision

[ ] Proceed [ ] Proceed with conditions (specified) [ ] Do not proceed [ ] Consult supervisory authority (Art. 36)

Conditions (if any). List concrete actions, owners and due dates; tracked in the personalisation risk register (companion doc).

§ 14

Evidence index

Evidence #	Description	Section	Location
DPIA-01	Lawful-basis matrix (per purpose)	§ 4	Privacy repo
DPIA-02	Legitimate-interest assessment(s)	§ 4	Privacy repo
DPIA-03	Consent ledger spec & withdrawal SLA	§ 7	Privacy repo
DPIA-04	Feature acceptance policy + quarterly review record	§ 7	Model risk
DPIA-05	DSR workflow	§ 8	Privacy
DPIA-06	Transfer impact assessments (TIA) per recipient	§ 9	Legal
DPIA-07	DPA / SCC inventory	§ 9	Legal + Procurement
DPIA-08	Privacy notice (current version)	§ 10	Privacy
DPIA-09	Breach-response runbook	§ 7	Security + Privacy
DPIA-10	Access control matrix	§ 7	Security

§ 15

Stakeholder map & companion documents

Role	Responsibility
Controller (legal entity)	Accountability for the processing
DPO	Oversight, advice, sign-off
Business owner	Purpose, benefit articulation
Engineering / data	Implementation of controls
Security	Art. 32 measures
Legal	Lawful basis, transfers, contracts
Procurement	Sub-processor management
Comms	Transparency, breach comms

Companion documents in this pack

- Retail Recommender Model Card (Doc 2 of 3) — model-side controls and validation
- Retail Personalisation Risk Register (Doc 3 of 3) — operational risk view across the personalisation programme

§ 16

Sign-off & attestation

Sign-off block

Role	Name	Date	Signature
Data Protection Officer (DPO)			
Legal			
Security			
Model owner			
Business owner			
Controller representative			

This DPIA is filed in the privacy register and re-affirmed annually or on any trigger in § 12. Where residual risk remains high, the controller consults the supervisory authority per Art. 36 before processing begins.