SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

Data Protection Impact Assessment

Meridian Home Retail (sample)

Loyalty app with personalised offers, in-store location tracking by Bluetooth beacons, and sharing of customer segments with brand partners.

ASSESSED	25 September 2026
METHOD	GDPR Article 35(7), with WP248 screening and Article 36 prior consultation
IN SCOPE	10 scope items, 11 risks
APPETITE	Medium and below (level 9 or less) accepted without treatment
PROFILE	Retail and e-commerce · 250 to 999 people
PREPARED BY	Governance Docs

Confidential. Prepared for Meridian Home Retail (sample). Contains details of a planned processing operation, the risks it poses to individuals and the measures that address them; share on a need-to-know basis.
Based on a self-assessment using information supplied by the organization. Not independently verified by Governance Docs; see "Basis of this report and limitation of liability".

CONTENTS

Where the organization's risks stand

PROCESS SCORE

90 / 100

Level 2 · Developing

The risks are identified, but gaps in rating or treatment would not survive an audit.

Held at Developing while 1 critical finding is open; the score alone would place it higher.

Initial | **Developing** | Defined | Managed

The score measures how complete and defensible the assessment is, not how risky the organization is.

RISKS	ABOVE APPETITE	CRITICAL	ABOVE AFTER TREATMENT	FINDINGS
11	5	0	1	6

WHAT THIS ASSESSMENT TELLS YOU

- DPIA required: The processing meets 5 of the nine WP248 criteria. In most cases two or more mean a DPIA is required.
- High risk remains after the planned measures (R-05). Unless further measures bring it down, the supervisory authority must be consulted before processing starts.
- 5 of 10 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-01, monitoring intrudes on people's private lives, at level 16 (High), owned by Head of Loyalty.
- 1 risk above the line has no treatment decision yet (R-05). Until it has one, the treatment plan is incomplete.

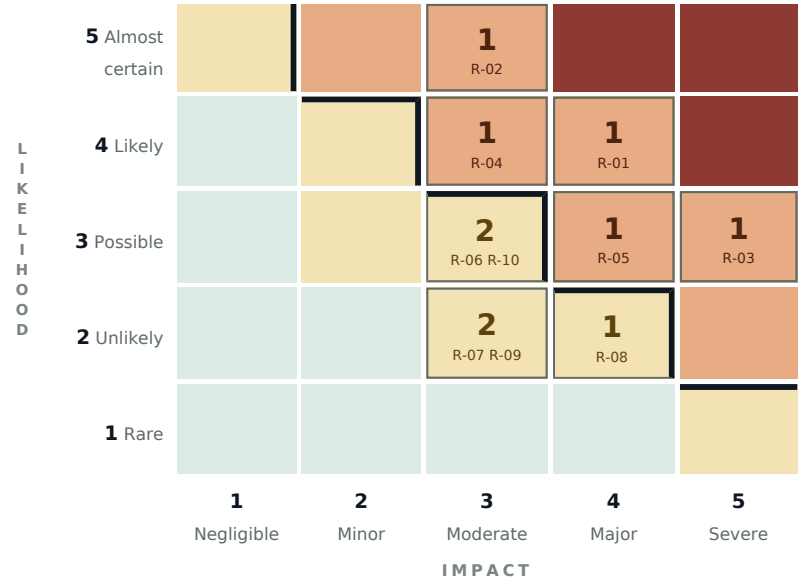
DO THESE FIRST

	SEVERITY	ACTION	RISKS	OWNER	DOCUMENT THAT CLOSES IT
1	CRITICAL	**Above the appetite line with no treatment decision** Choose modify, avoid, share or retain for each one, with the risk owner.	R-05	Procurement Manager	Risk treatment plan
2	MAJOR	**Not yet rated for likelihood and impact** Rate each one against the likelihood and impact scales in your criteria.	R-11	Data Protection Officer	Risk assessment and treatment methodology

Heat maps: today and after treatment

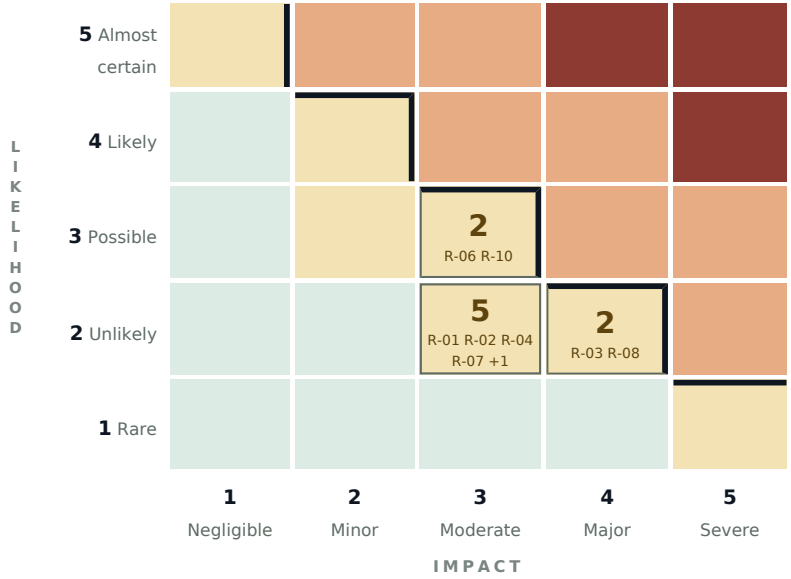
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

Current risk levels



10 of 11 risks rated.

Target levels after treatment



9 risks plotted; 0 removed by avoidance; risks above the line with no decision are not plotted.

Low 1–4 · Medium 5–9 · High 10–16 · Critical 17–25 · Appetite line

RISKS BY LEVEL

Analysis and priorities

IN ONE SENTENCE

A DPIA is required and mostly complete; decide how to treat the US transfer risk before the location features launch.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our DPIA for the loyalty app confirms a DPIA is required and that the planned measures bring four of the five high risks to members within our appetite. One decision is outstanding: how we protect member data hosted in the United States. Until that risk is treated, the location features should not launch without consulting the supervisory authority.

WHERE YOU STAND

The screening found 5 of the nine WP248 criteria met, so a DPIA is required. You have recorded 11 risks to members across 10 scope items, and 10 are rated. Your process score is 90 out of 100, but the level is held at Developing because one risk above your appetite line, the transfer of member data to the United States, has no treatment decision.

WHAT IT MEANS FOR THE ORGANIZATION

5 risks sit above your appetite line, all of them High, and the highest is the in-store tracking of members' movements, which most members would not expect. Planned measures bring 4 of them within appetite. Until the transfer risk is treated, high risk remains, and the supervisory authority would have to be consulted before processing starts.

WHERE TO FOCUS FIRST

Decide how to treat the transfer risk first, starting with a transfer risk assessment for the US hosting. Then set a retention period for purchase history, which the necessity test answered no, rate the risk to under-18 members, name an owner for the supplier reuse risk and record why the DPO's advice was only partly followed.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Decide how to treat the US transfer risk** R-05 Data transferred abroad without a valid safeguard · Above the appetite line with no treatment decision	It is the only High risk with no decision, so high risk remains and prior consultation would be needed before launch.	Ask the Procurement Manager to complete a transfer risk assessment for the US hosting.	Risk treatment plan	30 DAYS
2	**Set a retention period for purchase history** Necessity or proportionality not shown	Keeping every purchase since 2018 fails the necessity test and widens the harm in any breach.	Agree the three-year period the DPO advised and plan the deletion of older records.	DPIA template	60 DAYS
3	**Rate the risk to under-18 members** R-11 Children's data processed without extra protection · Not yet rated for likelihood and impact	Members can join at 16, and an unrated risk cannot be compared with your appetite.	Rate likelihood and impact for under-18 members, with a sentence of rationale.	Risk assessment and treatment methodology	30 DAYS
4	**Record why the DPO's advice was partly followed** DPO advice not followed, with no reason recorded	Departing from the DPO's advice is your decision, but the reason should be on record.	Add the reason to the sign-off and confirm which parts of the advice were adopted.	DPIA sign-off record	30 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Record a treatment decision for the US transfer risk.
- Rate the risk to under-18 members.
- Name an owner for the supplier reuse risk.

DAYS 31 TO 60

- Adopt the three-year retention period for purchase history.
- Make in-store location opt-in and off by default.
- Record the owner's acceptance for the data combining risk.

DAYS 61 TO 90

- Delete purchase records older than three years.
- Review the DPIA before the location features launch.

Why a DPIA: the screening

DPIA required

The processing meets 5 of the nine WP248 criteria. In most cases two or more mean a DPIA is required.

Screening note: Five WP248 criteria met: profiling, in-store tracking, location data, 1.2 million members and matching with partner data. A DPIA is required before the location features launch.

Article 35(3) and the authority's list: any one makes a DPIA mandatory	Met
Systematic and extensive evaluation of people, including profiling, used for decisions with legal or similarly significant effects	No
Large-scale processing of special category data or criminal offence data	No
Systematic monitoring of a publicly accessible area on a large scale	No
The processing is on your supervisory authority's list of processing that needs a DPIA	No

WP248 criteria: two or more usually mean a DPIA is required	Met
Evaluation or scoring, including profiling and predicting	**Yes**
Automated decision-making with legal or similarly significant effect	No
Systematic monitoring	**Yes**
Sensitive data or data of a highly personal nature	**Yes**
Data processed on a large scale	**Yes**
Matching or combining datasets	**Yes**
Data about vulnerable people	No
Innovative use or new technology	No
The processing prevents people from exercising a right or using a service or contract	No

Description of the processing

Article 35(7)(a): a systematic description of the processing operations and their purposes. The personal data, people, systems and recipients involved are listed with the risk register.

Purposes of the processing	Reward loyalty members, send offers matched to their interests, measure how store layouts perform, and give brand partners anonymous insight into customer segments.
Nature: how the data is collected, used, stored and deleted	Members join in the app. Purchases are linked to the member ID at the till and online. Beacons in 42 stores detect the app and record which departments a member visits. A customer data platform builds segments and offer rules. Offers are sent by push notification and email.
Scope: how much data, about how many people, where	About 1.2 million members in two countries. Contact details, purchase history since 2018, in-store location visits, inferred interests. Purchase data is processed daily; location data during store visits.
Context: your relationship with the people and what they would expect	Members expect points and offers, but most do not expect their movements in store to be tracked. Members can be 16 or over. Beacon tracking is new for the business and has drawn public attention elsewhere.
Lawful basis (Article 6)	Contract for the loyalty scheme; consent for personalised marketing and for in-store location tracking; legitimate interests for aggregate store analytics.
Condition for special category or criminal data (Articles 9 and 10)	None
Retention period	Account data while membership is active plus 12 months. No period set yet for purchase history.
Recipients and processors	Customer data platform provider (processor); email and push notification service (processor); brand partners receive aggregate segment reports only.
Transfers outside the country or region	Customer data platform hosted in the United States, under Standard Contractual Clauses.

Necessity and proportionality

Article 35(7)(b): whether the processing is necessary for its purpose and proportionate to it, with the measures that show compliance with the core principles. Every "partly" or "no" says what is missing.

Question	Answer	Explanation or evidence
The purpose is specific, explicit and legitimate, and the processing actually achieves it	Yes	–
There is no less intrusive way to achieve the same purpose	Partly	Store analytics could use anonymous footfall counters; only personalised in-store offers need member-level location.
Only the personal data needed for the purpose is collected and used	Partly	Beacons record every department visited; offers need only the store and the department of the offer.
The lawful basis is appropriate and documented for each purpose	Yes	–
Data is kept no longer than needed, and deleted or anonymised at the end	No	Purchase history has been kept since 2018 with no retention period.
Data is kept accurate and up to date, and errors can be corrected	Yes	–
People are told about the processing in a clear privacy notice	Yes	Privacy notice updated and shown in the app before location permission is asked.
People can exercise their rights, including access, objection and human review	Partly	Opt-out of location works in the app but does not yet reach the customer data platform.
Processors act under a contract meeting Article 28	Yes	–
Transfers abroad have a valid safeguard, or there are none	Yes	–

The risks to the rights and freedoms of the people concerned (Article 35(7)(c)) follow in the risk register, and the measures envisaged to address them (Article 35(7)(d)) in the measures plan.

What was in scope

The personal data, people concerned, processing step, system or technology, processor or recipient and location or transfer the assessment covered, with their owners.

Type	Scope item	Owner	Risks
Personal data	**Purchase history**	Head of Loyalty	1
Personal data	**In-store location visits**	Head of Loyalty	1
Personal data	**Inferred interests and segments**	Head of Data	1
People concerned	**Loyalty members**	Head of Loyalty	3
Processing step	**Profiling and segmentation**	Head of Data	2
Processing step	**Sharing with brand partners**	Head of Partnerships	1
System or technology	**Loyalty app**	Product Owner	2
System or technology	**In-store Bluetooth beacons**	Head of Stores	1
Processor or recipient	**Customer data platform provider**	Procurement Manager	4
Location or transfer	**United States hosting region**	IT Manager	1

Risk register

Every risk, highest level first. Level = likelihood x impact, rated with the controls already in place. The rationale is the organization's own reason for the rating. The full scenario for each risk (threat, weakness and consequence) is in the workbook.

#	Ref	Risk scenario	Scope items	Harm to people	Owner	Existing controls	L	I	Level	Rationale
1	R-01	**Monitoring intrudes on people's private lives** Weakness: Monitoring broader or more constant than the purpose needs, and poorly explained	In-store location visits, In-store Bluetooth beacons, Loyalty members	Loss of control, Physical or emotional harm, Surveillance	Head of Loyalty	Location permission asked in the app	4	4	16 · High	Beacons log every department a member visits, on every visit, whether or not an offer applies.
2	R-03	**Personal data exposed in a cyber attack** Weakness: Security measures not matched to the sensitivity of the data	Loyalty app, Customer data platform provider	Confidentiality lost, Financial loss, Physical or emotional harm	IT Manager	Platform provider certified to ISO 27001	3	5	15 · High	The platform holds contact details, purchase and location history for 1.2 million people.
3	R-02	**Personal data kept longer than needed** Weakness: No retention schedule and no deletion routine	Purchase history	Confidentiality lost, Loss of control	Head of Loyalty		5	3	15 · High	Eight years of purchase history is held for every member, including lapsed members.
4	R-05	**Data transferred abroad without a valid safeguard** Weakness: No transfer mechanism and no assessment of the destination	United States hosting region, Customer data platform provider	Confidentiality lost, Loss of control, Rights obstructed	Procurement Manager	Standard Contractual Clauses signed	3	4	12 · High	No transfer risk assessment has been done for the US hosting.
5	R-04	**Datasets combined in ways people would not expect** Weakness: The combined effect on people was never assessed	Inferred interests and segments, Profiling and segmentation	Loss of control, Discrimination, Surveillance	Head of Data	Partners receive segment reports only	4	3	12 · High	Segments combine purchase, location and partner campaign data in ways members were not told about.

6	R-06	**Objections and opt-outs not honoured** Weakness: The opt-out does not reach every system and supplier	Loyalty app, Profiling and segmentation	Loss of control, Rights obstructed	Head of Loyalty	Opt-out in the app settings	3	3	9 · Medium	Opt-outs reach the app within a day but the platform only weekly.
7	R-10	**A supplier uses the data for its own purposes** Weakness: Supplier terms not reviewed before the data is shared	Customer data platform provider	Confidentiality lost, Loss of control	None	Processor contract	3	3	9 · Medium	The platform's terms allow it to use data to improve its own services.
8	R-08	**Staff access data they do not need** Weakness: Broad access rights, with no access reviews or logging	Customer data platform provider, Loyalty members	Confidentiality lost, Physical or emotional harm	IT Manager	Role-based access in the platform	2	4	8 · Medium	Twenty-six staff can view member-level data; access is reviewed yearly.
9	R-07	**Data shared with third parties people would not expect** Weakness: No sharing agreement and no transparency about recipients	Sharing with brand partners	Loss of control, Surveillance	Head of Partnerships	Partners receive aggregate reports; no member-level data	2	3	6 · Medium	Segments below 50 members are suppressed before reports are sent.
10	R-09	**Access requests not answered in time** Weakness: No procedure or owner, and data spread across systems nobody has mapped	Loyalty members	Rights obstructed	Data Protection Officer	Access request procedure	2	3	6 · Medium	All 38 requests last year were answered within the month.
11	R-11	**Children's data processed without extra protection** Weakness: No age check, parental consent or information a child can understand	None linked	Loss of control, Physical or emotional harm	Data Protection Officer		–	–	Not rated	

What will be done, by whom and by when

Every risk with a treatment decision, earliest due date first. The data protection measures listed are the ones the treatment relies on; they carry into the dpia measures plan. Acceptance is the risk owner's approval of the plan and of the risk that remains.

Ref	Risk	Decision	Planned actions	Data protection measures	Owner and due date	Current to target	Accepted
R-03	**Personal data exposed in a cyber attack** IT Manager	**Modify**	Encrypt the member database, require multi-factor authentication for all admin access and review access logs weekly.	DP.3 Encryption in transit and at rest (Art 32) DP.4 Access control and least privilege (Art 32) DP.17 Logging and monitoring of access (Art 32)	IT Manager 30 Nov 2026	15 · High → 8 · Medium	Chief Executive 22 Sep 2026
R-01	**Monitoring intrudes on people's private lives** Head of Loyalty	**Modify**	Make in-store location opt-in and off by default, record only the department linked to an offer, and delete visit logs after 30 days.	DP.1 Data minimisation (Art 5(1)(c)) DP.20 Privacy by design and by default (Art 25) DP.6 Privacy notice and transparency (Art 12 to 14)	Product Owner 31 Dec 2026	16 · High → 6 · Medium	Chief Executive 22 Sep 2026
R-02	**Personal data kept longer than needed** Head of Loyalty	**Modify**	Adopt a three-year retention period for purchase history and delete older records.	DP.5 Retention schedule and deletion (Art 5(1)(e))	IT Manager 31 Jan 2027	15 · High → 6 · Medium	Chief Executive 22 Sep 2026
R-04	**Datasets combined in ways people would not expect** Head of Data	**Modify**	Use partner data only for aggregate reporting and tell members which data builds their segments.	DP.23 Purpose limitation controls (Art 5(1)(b)) DP.6 Privacy notice and transparency (Art 12 to 14)	Head of Data 31 Jan 2027	12 · High → 6 · Medium	**Not recorded**

ABOVE THE LINE WITH NO DECISION YET

Ref	Risk	Owner	Level
R-05	**Data transferred abroad without a valid safeguard**	Procurement Manager	12 · High

5 risks are within appetite (Medium and below) and need no treatment; 1 are not yet rated.

Where the assessment falls short

Each finding is a gap between the assessment as recorded and what GDPR Article 35 ask for, with the risks it applies to and the document that closes it.

Severity	Finding	Applies to	What it means	To fix	Document that closes it
CRITICAL	**Above the appetite line with no treatment decision**	R-05	These risks are rated above Medium, the highest level you accept without treatment, but nobody has decided what to do about them. GDPR expects a treatment option to be chosen for every risk that fails the acceptance criteria.	Choose modify, avoid, share or retain for each one, with the risk owner.	Risk treatment plan
MAJOR	**Not yet rated for likelihood and impact**	R-11	Without both ratings a risk has no level, so it cannot be compared with the appetite line or placed in priority order.	Rate each one against the likelihood and impact scales in your criteria.	Risk assessment and treatment methodology
MAJOR	**Risk with no owner**	R-10	Each risk to individuals needs an owner who can put the measures in place. Without one, the DPIA records a risk nobody will reduce.	Name an owner, by role, for each risk.	Risk assessment and treatment methodology
MAJOR	**Necessity or proportionality not shown**	Data is kept no longer than needed, and deleted or anonymised at the end	Article 35(7)(b) requires the DPIA to show the processing is necessary and proportionate to its purpose. A "no" here is a compliance gap in itself, whatever the risk ratings say.	Change the design until each answer is yes, or record the measures that close the gap.	DPIA template
MINOR	**Residual risk not yet accepted by the owner**	R-04	The controller should approve the measures and accept the risk that remains. If high risk remains, Article 36 requires consulting the supervisory authority before processing starts.	Record the owner's acceptance once they have approved the plan.	Risk treatment plan
MINOR	**DPO advice not followed, with no reason recorded**	Sign-off	Departing from the DPO's advice is the controller's decision to make, but the reason should be on record.	Record why the advice was not followed in full.	DPIA sign-off record

PROCESS SCORE IN DETAIL

Criteria defined Every likelihood and impact level has a definition, and the appetite line is set.	100%	11 of 11	weight 10
Scope covered Every scope item has at least one risk linked to it.	100%	10 of 10	weight 10
Risk owners named Every risk has an owner accountable for it.	91%	10 of 11	weight 15
Risks rated Every risk has a likelihood and an impact, so it has a level.	91%	10 of 11	weight 15
Ratings explained Existing controls and a rationale are recorded for each risk.	86%	19 of 22	weight 10
Treatment decided Every risk above the appetite line has a treatment option chosen.	80%	4 of 5	weight 15
Targets within appetite Treatments bring each risk to a target at or below the line.	100%	4 of 4	weight 10
Treatments scheduled Each treatment has an owner and a due date.	100%	4 of 4	weight 5
Residual risk accepted Risk owners have accepted what remains after treatment, by name and date.	75%	3 of 4	weight 10
DPIA record complete Screening, description, necessity and proportionality, DPO advice, outcome and review date are all recorded.	86%	19 of 22	weight 25

Findings by severity

1 · Initial (0+)

A start on a register, not yet an assessment that decisions can rest on.

2 · Developing (40+)

The risks are identified, but gaps in rating or treatment would not survive an audit.

3 · Defined (60+)

A complete, repeatable assessment with a treatment plan behind it.

4 · Managed (80+)

Owned, justified and accepted: ready for management review and audit.

The decision on the processing

RESIDUAL RISK AND PRIOR CONSULTATION (ARTICLE 36)

High risk remains after the planned measures (R-05). Unless further measures bring it down, the supervisory authority must be consulted before processing starts.

DATA PROTECTION OFFICER'S ADVICE (ARTICLE 35(2))

Who advised	A DPO is designated and gave advice
Advice	Data Protection Officer: make location tracking opt-in and off by default, set a three-year retention period for purchase history, and keep under-18s out of profiling.
Followed	**Partly**
Why not in full	**Not recorded**

VIEWS OF THE PEOPLE CONCERNED (ARTICLE 35(9))

Views	Sought, and summarised below
Summary or reason	Survey of 1,400 members: 61% welcome personalised offers; 22% are uncomfortable with in-store tracking.

OUTCOME AND APPROVAL

Outcome	**Proceed once the planned measures are in place**
Approved by	Chief Executive
Approved on	22 Sep 2026
Review by (Article 35(11))	30 Sep 2027

Review the DPIA whenever the processing changes in a way that could change the risk: new data, a new purpose, new technology, a new supplier or a new group of people. If high risk remains that the measures cannot reduce, do not start the processing until the supervisory authority has been consulted and has responded.

A · APPENDIX

Criteria used and basis of this report

Article 35(7)(c) asks for an assessment of the risks to the rights and freedoms of the people concerned, so likelihood and severity are rated for them, not for the organization. This is the record of the criteria every rating in this report was made against.

LIKELIHOOD SCALE

Value	Label	Definition
1	**Rare**	Not expected in the next 5 years; no known case here or in the sector
2	**Unlikely**	Could happen once in 2 to 5 years; has happened in the sector
3	**Possible**	Could happen about once a year
4	**Likely**	Expected several times a year
5	**Almost certain**	Expected monthly or more often, or already happening

IMPACT SCALE

Value	Label	Definition
1	**Negligible**	Negligible: people are not affected, or only trivially
2	**Minor**	Minimal: minor inconvenience people overcome without difficulty
3	**Moderate**	Significant: real inconvenience, distress or cost people can overcome with some difficulty
4	**Major**	Serious: significant consequences such as discrimination, fraud, financial loss or damage to reputation
5	**Severe**	Severe: serious, lasting or irreversible harm, such as to health, livelihood or safety

RISK LEVELS AND ACCEPTANCE

Band	Levels	Treatment
Low	1–4	Accepted without treatment
Medium	5–9	Accepted without treatment
High	10–16	Needs a treatment decision
Critical	17–25	Needs a treatment decision

Level = likelihood x impact. A risk above the appetite line may still be retained, but only with the risk owner's recorded acceptance.

Process score. Ten dimensions: nine for the register, each the share of risks (or of risks above the line) that meet it, and one for the completeness of the DPIA record. Each is multiplied by its weight and the total is scaled to 100. A dimension with nothing in scope counts in full. Any critical finding holds the level at Developing, whatever the score.

Your workbook. The Excel workbook that comes with this report is the register as a working file. Change a likelihood or impact on the Risk register sheet and every level, the heat maps on the Dashboard and the process score recalculate. It also holds the treatment plan and a list of the data protection measures your treatments rely on.

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The risks, ratings, risk levels, treatment decisions, findings, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

Data protection impact assessment for Meridian Home Retail (sample), generated 25 September 2026 by Governance Docs. This is a structured self-assessment based on the organization's own criteria and ratings. It is not a certification, an audit opinion or a substitute for an independent risk assessment.