SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

# Transfer Impact Assessment

## Meridian Retail Group (sample)

Employee HR and payroll data sent to a US HR platform, with the platform's support team in India able to view records.

| | |
|---|---|
| ASSESSED | 25 September 2026 |
| METHOD | GDPR and UK GDPR Chapter V, following the EDPB six steps and the UK transfer risk assessment |
| IN SCOPE | 11 scope items, 12 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 |

CONTENTS



Confidential. Prepared for Meridian Retail Group (sample). Contains details of an international transfer of personal data, the risks it poses to individuals and the supplementary 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".

# Where the organization's risks stand

PROCESS SCORE

**96** / 100

**Level 4 · Managed**

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

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 |
|---|---|---|---|---|
| 12 | 3 | 0 | 0 | 4 |

## WHAT THIS ASSESSMENT TELLS YOU

- TIA required: This is a restricted transfer under both regimes. Assess it once, against both tests: essential equivalence for the EU SCCs (Clause 14), and "not materially lower" for the UK IDTA or Addendum.
- No High or Critical risk remains once the supplementary measures are in place, so the transfer tool can be relied on for this transfer.
- 3 of 11 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-01, data accessed in clear from a country with problematic laws, at level 12 (High), owned by Data Protection Officer.
- Planned treatment brings the number of risks above the line from 3 to 0.

## DO THESE FIRST

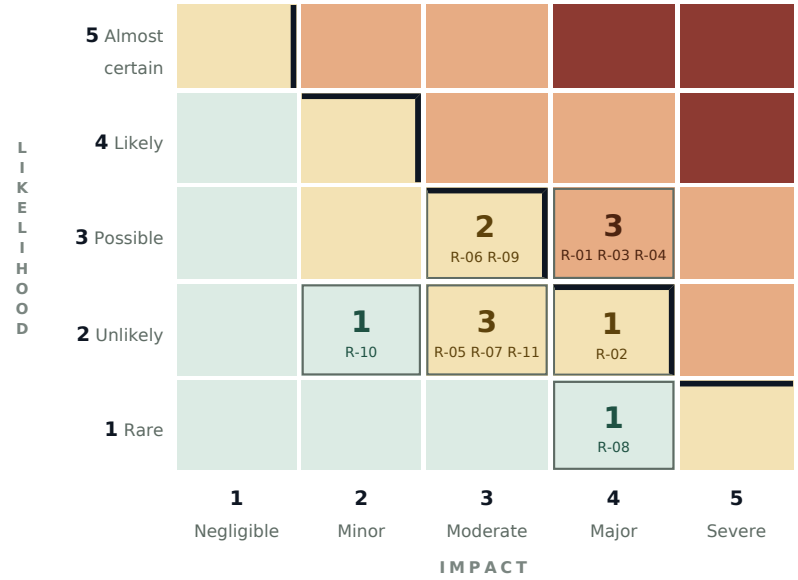
| | SEVERITY | ACTION | RISKS | OWNER | DOCUMENT THAT CLOSES IT |
|---|---|---|---|---|---|
| 1 | MAJOR | **Not yet rated for likelihood and impact**<br>Rate each one against the likelihood and impact scales in your criteria. | R-12 | Legal Counsel | Risk assessment and treatment methodology |

| | | | | | |
|---|---|---|---|---|---|
| 2 | MAJOR | **Risk with no owner**<br>Name an owner, by role, for each risk. | R-11 | To assign | Risk assessment and treatment methodology |
| 3 | MAJOR | **Scope item with no risks identified**<br>Link an existing risk to it, add a new one, or take it out of scope. | Employee records and performance reviews | To assign | Transfer register and TIA |

# Heat maps: today and after treatment

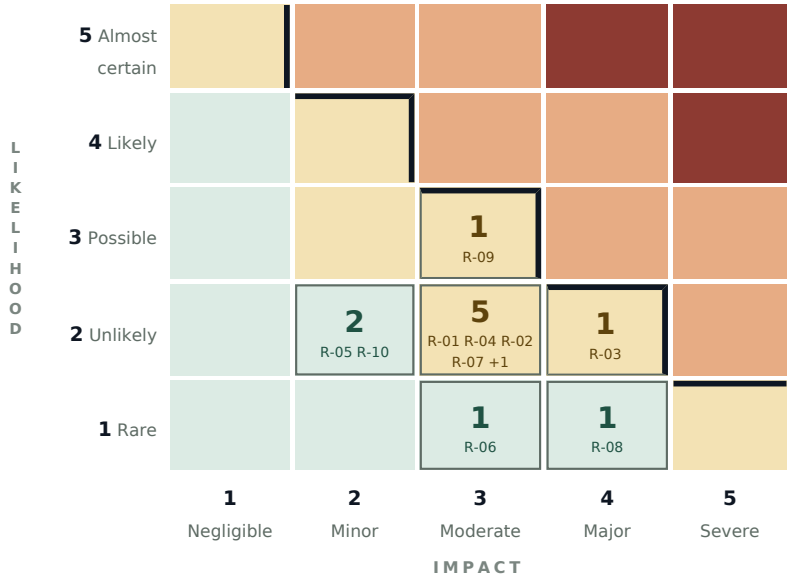
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

**Current risk levels**




11 of 12 risks rated.

**Target levels after treatment**




11 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

| 2 Low | 6 Medium | 3 High | 1 Not rated |
|---|---|---|---|

# Analysis and priorities

IN ONE SENTENCE

**A TIA is required and the planned supplementary measures make the transfer tool effective; deliver them on time and close four gaps in the record.**

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 transfer impact assessment for the HR platform confirms that employee data sent to the United States, with support access from India, needs supplementary measures before it can rely on the SCCs and the UK Addendum. The measures we have planned bring every high risk within our appetite. The most important ones are masked, logged support access and signing the UK Addendum, both due this quarter.

| | |
|---|---|
| WHERE YOU STAND | The screening shows a restricted transfer under both the EU GDPR and the UK GDPR, relying on the EU SCCs and the UK Addendum, so a TIA is required. You have recorded 12 transfer risks across 11 scope items, and 11 are rated. Your process score is 96 out of 100, at the Managed level. |
| WHAT IT MEANS FOR THE ORGANIZATION | 3 risks sit above your appetite line, all of them High, and the highest is support staff in India viewing employee records in clear. Planned supplementary measures bring all three within appetite, so the transfer tool can be relied on once they are in place. Two of your destination answers were no: redress in India, and the US provider falling within the laws that allow access. |
| WHERE TO FOCUS FIRST | Make sure the two destination problems are each answered by a supplementary measure in the register, then rate the risk of secrecy orders, name an owner for the supplier reuse risk and add a risk for employee records and performance reviews. Customer-held keys are the measure most worth tracking, because until they arrive encryption does not stop compelled access. |

## PRIORITIES

| | PRIORITY | WHY IT MATTERS | FIRST STEP | START FROM | WITHIN |
|---|---|---|---|---|---|
| 1 | **Match each destination problem to a supplementary measure**<br>Problems found in the destination's laws or practice | The redress gap in India and the US provider's exposure to access laws are the reasons the SCCs need supplementing at all. | Check that R-01, R-02 and R-05 name the measures that answer these two problems, and note it in the destination answers. | Transfer impact assessment | 30 DAYS |
| 2 | **Rate the risk of secrecy orders**<br>R-12 The importer is barred from telling you about access requests · Not yet rated for likelihood and impact | An unrated risk cannot be compared with your appetite, and secrecy orders are possible under the laws you identified. | Rate likelihood and impact, using the provider's transparency report as the source. | Risk assessment and treatment methodology | 30 DAYS |
| 3 | **Name an owner for the supplier reuse risk**<br>R-11 The importer uses the data for its own purposes · Risk with no owner | The provider's terms allow benchmarking use of your data, and nobody is accountable for closing it. | Assign the risk to the Procurement Manager and review the reuse clause at renewal. | Risk assessment and treatment methodology | 30 DAYS |
| 4 | **Track the move to customer-held keys**<br>R-03 Encryption keys held by the importer or in the destination | It is the only measure that stops compelled access to data at rest, and it depends on the provider's roadmap. | Ask the provider for a committed date and put it in the re-evaluation plan. | Supplementary measures plan | 90 DAYS |

## 30 / 60 / 90-DAY ROADMAP

### FIRST 30 DAYS

- Sign the UK Addendum and complete Annex I.
- Rate the secrecy order risk and name an owner for the supplier reuse risk.
- Link each destination problem to its supplementary measures.

### DAYS 31 TO 60

- Switch support access from India to just in time, logged and masked.
- Add notification and challenge commitments to the contract.
- Replace free-text sickness reasons with coded absence types.

### DAYS 61 TO 90

- Get a committed date for customer-held keys.
- Add a risk for employee records and performance reviews, and plan the re-evaluation.

# Is a TIA needed: the screening

**Transfer rules:** Both

## TIA required

This is a restricted transfer under both regimes. Assess it once, against both tests: essential equivalence for the EU SCCs (Clause 14), and "not materially lower" for the UK IDTA or Addendum.

**Screening note:** Restricted transfer under both the EU GDPR (stores in Ireland and the Netherlands) and the UK GDPR (UK head office). The HR platform provider is not certified to the Data Privacy Framework for HR data, and its support centre in India has no adequacy decision, so the transfer relies on the EU SCCs and the UK Addendum.

| Restricted transfer test: all three must be met | Answer |
|---|---|
| The EU GDPR or the UK GDPR applies to the processing | **Yes** |
| The data is sent to, or can be accessed from, a country outside the EEA or the UK | **Yes** |
| The recipient is a separate organization | **Yes** |

| How the transfer is covered | Answer |
|---|---|
| An adequacy decision or adequacy regulations cover the destination or the recipient | No |
| You rely on an Article 49 exception instead of a safeguard | No |

# The transfer

EDPB steps 1 and 2: know the transfer and the tool it relies on. The personal data, people, importers, systems and locations involved are listed with the risk register.

| | |
|---|---|
| **Exporter and importer, and their roles** | Exporter: Meridian Retail Group, controller for its 6,800 employees in the UK, Ireland and the Netherlands. Importer: the HR platform provider in the United States, processor (EU SCCs module 2). Its support subsidiary in India is a sub-processor (module 3 flow-down). |
| **Purpose of the transfer** | Run HR administration and payroll preparation: employee records, absence, performance reviews and monthly payroll files. |
| **Personal data and people concerned** | About 6,800 current employees and 9,000 former employees. Identity and contact details, job and pay history, bank details, absence records including sickness absence (health data), performance reviews. No criminal records data. |
| **Format of the data at the importer** | Encrypted in transit and at rest; the provider manages the encryption keys. Support staff see records in clear when they open a ticket. |
| **How the data is transferred and accessed** | Nightly upload from the payroll system; HR staff use the platform in the browser. The Indian support team can open any employee record while working on a ticket; around 40 tickets a month. |
| **Destination countries and storage locations** | United States (primary hosting and backups), India (remote support access only). |
| **Onward transfers** | Email notification service in the United States; cloud hosting provider in the United States. Both are listed as sub-processors with flow-down terms. |
| **Transfer tool relied on** | EU SCCs module 2 with the provider, module 3 flow-down to the Indian subsidiary; UK Addendum to the EU SCCs for UK employees. |
| **Duration and retention at the importer** | For the life of the contract (three years, renewable). Records of former employees kept six years, then deleted. |

# Laws and practice in the destination

EDPB step 3: whether anything in the law or practice of the destination may stop the transfer tool from being effective. For the UK, whether the protection is not materially lower than under UK law. Every "partly" or "no" says what is missing.

| Question | Answer | Explanation or evidence |
|---|---|---|
| **Any law that lets public authorities access the data is clear, precise and publicly available** | Partly | US: the main surveillance laws are public. India: access powers under the IT Act rules are broad and their use is not published. Source: importer questionnaire and published legal reviews. |
| **That access is limited to what is necessary and proportionate, with no bulk or indiscriminate access to data like this** | Partly | US: Executive Order 14086 adds necessity and proportionality limits for signals intelligence. India: no equivalent limits found for access to data held by service providers. |
| **Access by public authorities is subject to independent oversight, such as a court or an independent body** | Partly | US: FISA Court and the Privacy and Civil Liberties Oversight Board. India: no independent oversight of access orders found. |
| **People whose data is transferred have effective redress against unlawful access** | No | India: no redress route found for EU or UK residents whose data is accessed. |
| **The importer and this data fall outside what those laws target, or the laws are not applied to data like this in practice** | No | The US provider is an electronic communications service provider within FISA Section 702. |
| **The importer has received no access requests for data like this, or reports them transparently** | Yes | The provider's transparency report shows no requests for customer HR data in the last three years. |
| **The importer can comply with the transfer tool, and will tell you if it no longer can** | Yes | Provider questionnaire answered in full; commits to notify and to challenge requests. |
| **Onward transfers keep the same level of protection, or there are none** | Yes | Sub-processors listed; the same terms flow down. |
| **The destination has data protection law, an independent regulator and respects the rule of law** | Partly | India's Digital Personal Data Protection Act is in force but its rules are still being phased in. |
| **The sources used are relevant, objective, reliable, verifiable and recorded** | Yes | Importer questionnaire, the provider's transparency report, published analyses of US and Indian law. |

The risks to the people whose data is transferred follow in the risk register, and the supplementary measures that address them (EDPB step 4) in the measures plan.

# What was in scope

The personal data transferred, people concerned, importer or sub-processor, destination or data location, service or system and transfer flow the assessment covered, with their owners.

| Type | Scope item | Owner | Risks |
|---|---|---|---|
| Personal data transferred | **Payroll and bank details** | Head of Payroll | 1 |
| Personal data transferred | **Sickness absence records** | HR Director | 1 |
| Personal data transferred | **Employee records and performance reviews** | HR Director | **0** |
| People concerned | **Employees and former employees** | HR Director | 2 |
| Importer or sub-processor | **US HR platform provider** | Procurement Manager | 5 |
| Importer or sub-processor | **Support subsidiary in India** | Procurement Manager | 1 |
| Destination or data location | **United States** | Data Protection Officer | 2 |
| Destination or data location | **India (support access)** | Data Protection Officer | 2 |
| Service or system | **HR and payroll platform** | IT Manager | 1 |
| Transfer flow | **Remote support access** | IT Manager | 1 |
| Transfer flow | **Nightly payroll upload** | Head of Payroll | 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 | **Data accessed in clear from a country with problematic laws**<br>Weakness: Remote access needs the data in clear, so encryption cannot protect it (EDPB use case 7) | Remote support access, Support subsidiary in India, Payroll and bank details | Access by authorities, Confidentiality lost, Loss of control | Data Protection Officer | Support staff bound by confidentiality terms | 3 | 4 | 12 · High | About 40 support staff can open any record, including bank and sickness fields, and views are not logged. |
| 2 | R-03 | **Encryption keys held by the importer or in the destination**<br>Weakness: Keys are within reach of the importer and so of the destination's authorities | HR and payroll platform, US HR platform provider | Access by authorities, Confidentiality lost | Information Security Manager | Provider-managed encryption at rest | 3 | 4 | 12 · High | The provider holds the keys, so encryption does not stop compelled access to data at rest. |
| 3 | R-04 | **Special category or criminal data transferred**<br>Weakness: The most sensitive data travels with the same safeguards as any other | Sickness absence records | Access by authorities, Confidentiality lost, Harm to people | HR Director | Absence reasons entered as free text | 3 | 4 | 12 · High | Sickness reasons are typed into a free-text field and go to the US with every record. |
| 4 | R-06 | **The wrong or an incomplete transfer tool is used**<br>Weakness: Annexes left blank, and no legal review against the actual data flow | US HR platform provider | Loss of control, Rights and redress | Legal Counsel | EU SCCs module 2 signed in 2024 | 3 | 3 | 9 · Medium | The UK Addendum was never signed, so UK employee data has no valid safeguard. |
| 5 | R-09 | **The destination's law or adequacy status changes**<br>Weakness: Nobody monitors developments, and there is no fallback transfer tool | United States, India (support access) | Access by authorities, Loss of control | Data Protection Officer | | 3 | 3 | 9 · Medium | No one monitors changes in US or Indian law, and there is no fallback if the provider cannot comply. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | R-02 | **The importer is compelled to hand the data to public authorities**<br>Weakness: Destination law allows access beyond what is necessary and proportionate, and the importer holds the data in clear | US HR platform provider, United States | Access by authorities, Confidentiality lost, Rights and redress | Data Protection Officer | EU SCCs signed; provider commits to challenge requests | 2 | 4 | 8 · Medium | The provider falls within FISA Section 702, but its transparency report shows no requests for customer HR data in three years. |
| 7 | R-05 | **People have no effective redress against unlawful access**<br>Weakness: Redress in the destination is limited to its own nationals, or the body deciding is not independent | India (support access), Employees and former employees | Rights and redress | Data Protection Officer | | 2 | 3 | 6 · Medium | No redress route found in India; the US Data Protection Review Court applies to EU and UK individuals. |
| 8 | R-07 | **Sub-processors in other countries receive the data**<br>Weakness: No list of sub-processors and no flow-down of the same protections | US HR platform provider | Access by authorities, Loss of control, Onward disclosure | Procurement Manager | Sub-processor list published by the provider | 2 | 3 | 6 · Medium | Changes are announced by email with 30 days to object; nobody at Meridian reads the notices. |
| 9 | R-11 | **The importer uses the data for its own purposes**<br>Weakness: Terms not reviewed; no purpose restriction in the contract | US HR platform provider | Loss of control, Onward disclosure | **None** | Processor contract | 2 | 3 | 6 · Medium | The provider's terms allow aggregated use of customer data for benchmarking. |
| 10 | R-08 | **Data intercepted in bulk while in transit**<br>Weakness: Data sent unencrypted, or with encryption that could be broken or bypassed | Nightly payroll upload | Access by authorities, Confidentiality lost | IT Manager | TLS 1.2 or higher on all connections | 1 | 4 | 4 · Low | All uploads and browser sessions are encrypted with current TLS. |
| 11 | R-10 | **People cannot exercise their rights over data held abroad**<br>Weakness: No process for the importer to find, return or delete the data on request | Employees and former employees | Rights and redress | HR Director | Rights requests handled by HR | 2 | 2 | 4 · Low | All data can be exported from the platform by HR; last year's 14 requests were answered in time. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 12 | R-12 | **The importer is barred from telling you about access requests**<br>Weakness: Local law allows secrecy orders; no transparency reporting or warrant canary | None linked | Access by authorities, Rights and redress | Legal Counsel | – | – | Not rated |

# What will be done, by whom and by when

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

| Ref | Risk | Decision | Planned actions | Supplementary measures | Owner and due date | Current to target | Accepted |
|---|---|---|---|---|---|---|---|
| R-06 | **The wrong or an incomplete transfer tool is used**<br>Legal Counsel | **Modify** | Sign the UK Addendum and complete Annex I with the actual data categories. | SM.9 Contractual: transfer tool correctly executed (right SCC module, annexes complete, IDTA or UK Addendum) | Legal Counsel<br>31 Oct 2026 | 9 · Medium → 3 · Low | Chief People Officer<br>22 Sep 2026 |
| R-02 | **The importer is compelled to hand the data to public authorities**<br>Data Protection Officer | **Modify** | Add the notification and challenge commitments to the contract, and review the transparency report twice a year. | SM.10 Contractual: duty to notify you of access requests, where the law allows<br>SM.11 Contractual: commitment to challenge unlawful requests and disclose the minimum<br>SM.12 Contractual: transparency reporting and a warrant canary | Legal Counsel<br>30 Nov 2026 | 8 · Medium →<br>6 · Medium | Chief People Officer<br>22 Sep 2026 |
| R-05 | **People have no effective redress against unlawful access**<br>Data Protection Officer | **Modify** | Contractual commitment that the provider will support Meridian and employees in any challenge, and route all rights requests through Meridian. | SM.11 Contractual: commitment to challenge unlawful requests and disclose the minimum<br>SM.20 Organisational: rights requests routed to and answered by the exporter | Legal Counsel<br>30 Nov 2026 | 6 · Medium → 4 · Low | **Not recorded** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| R-01 | **Data accessed in clear from a country with problematic laws**<br>Data Protection Officer | **Modify** | Just-in-time support access approved by Meridian per ticket, logged, with bank and health fields masked. | SM.7 Technical: remote access limited to named roles, just in time and logged<br>SM.3 Technical: pseudonymisation, with the key kept by the exporter (EDPB use case 2) | IT Manager<br>15 Dec 2026 | 12 · High → 6 · Medium | Chief People Officer<br>22 Sep 2026 |
| R-04 | **Special category or criminal data transferred**<br>HR Director | **Modify** | Replace free-text sickness reasons with a coded absence type; keep medical details in the UK occupational health system. | SM.5 Technical: data minimisation before transfer<br>SM.3 Technical: pseudonymisation, with the key kept by the exporter (EDPB use case 2) | HR Director<br>31 Jan 2027 | 12 · High → 6 · Medium | Chief People Officer<br>22 Sep 2026 |
| R-03 | **Encryption keys held by the importer or in the destination**<br>Information Security Manager | **Modify** | Move to customer-held keys when the provider releases them; until then, rely on the other measures and re-evaluate. | SM.1 Technical: encryption at rest, keys held only by the exporter (EDPB use case 1) | Information Security Manager<br>30 Jun 2027 | 12 · High → 8 · Medium | Chief People Officer<br>22 Sep 2026 |

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 Chapter V 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 |
|---|---|---|---|---|---|
| MAJOR | **Not yet rated for likelihood and impact** | R-12 | 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-11 | Each transfer risk needs an owner who can put the supplementary measures in place. Without one, the TIA records a risk nobody will reduce. | Name an owner, by role, for each risk. | Risk assessment and treatment methodology |
| MAJOR | **Scope item with no risks identified** | Employee records and performance reviews | Something you put in scope has no risk attached to it. Either it faces no credible risk, which is rare, or the identification step missed it. | Link an existing risk to it, add a new one, or take it out of scope. | Transfer register and TIA |
| MAJOR | **Problems found in the destination's laws or practice** | People whose data is transferred have effective redress against unlawful access; The importer and this data fall outside what those laws target, or the laws are not applied to data like this in practice | Each "no" is a reason the transfer tool may not be effective on its own. The EDPB says you must then adopt supplementary measures that close the gap, or not transfer. Contractual and organisational measures alone rarely stop access by public authorities to data held in clear. | Make sure each problem is matched by a risk in the register with supplementary measures that address it. | Transfer impact assessment |

## PROCESS SCORE IN DETAIL

| | | | |
|---|---|---|---|
| **Criteria defined**<br>Every likelihood and impact level has a definition, and the appetite line is set. | 100% | 11 of 11 | weight 10 |
| **Scope covered**<br>Every scope item has at least one risk linked to it. | 91% | 10 of 11 | weight 10 |
| **Risk owners named**<br>Every risk has an owner accountable for it. | 92% | 11 of 12 | weight 15 |
| **Risks rated**<br>Every risk has a likelihood and an impact, so it has a level. | 92% | 11 of 12 | weight 15 |
| **Ratings explained**<br>Existing controls and a rationale are recorded for each risk. | 83% | 20 of 24 | weight 10 |
| **Treatment decided**<br>Every risk above the appetite line has a treatment option chosen. | 100% | 3 of 3 | weight 15 |
| **Targets within appetite**<br>Treatments bring each risk to a target at or below the line. | 100% | 3 of 3 | weight 10 |
| **Treatments scheduled**<br>Each treatment has an owner and a due date. | 100% | 3 of 3 | weight 5 |
| **Residual risk accepted**<br>Risk owners have accepted what remains after treatment, by name and date. | 100% | 3 of 3 | weight 10 |
| **TIA record complete**<br>Screening, the transfer, the destination's laws and practice, the importer's input, DPO advice, outcome and re-evaluation date are all recorded. | 100% | 23 of 23 | weight 25 |

**Findings by severity**


Critical Major Minor

**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 transfer

RESIDUAL RISK: IS THE TRANSFER TOOL EFFECTIVE?

No High or Critical risk remains once the supplementary measures are in place, so the transfer tool can be relied on for this transfer.

## DATA PROTECTION OFFICER'S ADVICE

| | |
|---|---|
| **Who advised** | A DPO is designated and gave advice |
| **Advice** | Data Protection Officer: support access from India must become just in time and logged, with bank and health fields masked; move to keys held by Meridian when the provider offers them. |
| **Followed** | **Partly** |
| **Why not in full** | Customer-held keys are on the provider's roadmap for next year; the other measures are adopted now. |

## THE IMPORTER'S INPUT (SCC CLAUSE 14(C))

| | |
|---|---|
| **Importer input** | The importer answered a questionnaire or gave commitments, summarised below |
| **Summary or reason** | The provider answered the 32-question due diligence questionnaire, sent its transparency report and confirmed it will notify Meridian of any access request where the law allows. |

## OUTCOME AND APPROVAL

| | |
|---|---|
| **Outcome** | **Proceed once the supplementary measures are in place** |
| **Approved by** | Chief People Officer |
| **Approved on** | 22 Sep 2026 |
| **Re-evaluate by (EDPB step 6)** | 30 Sep 2027 |

Re-evaluate the TIA whenever the transfer changes (new data, a new sub-processor, a new country) and whenever the destination's law or an adequacy decision changes. If no supplementary measure makes the transfer tool effective, the transfer must not start, or must be suspended.

A · APPENDIX

# Criteria used and basis of this report

A transfer impact assessment asks whether the people whose data is transferred keep the protection they would have at home, 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 TIA 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 supplementary 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.

Transfer impact assessment for Meridian Retail Group (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.