HOW MERIDIAN'S SECURITY ARCHITECTURE WORKS

SECURITY AND COMPLIANCE OVERVIEW

The mechanics behind matching your list against IMI's subscriber base without either side ever seeing the other's raw data.

CONTENTS

INTRODUCTION

Meridian tells you what share of a contact list is already an opted-in IMI subscriber, without either side ever exchanging a plaintext email address. This document explains: how your file reaches Meridian, how matching avoids exposing raw data, where data lives while that happens, and how it's removed afterwards. It complements, not replaces, your organisation's Data Processing Agreement (DPA).

~1.8M	EU-only	0	≤5 days
IMI subscriber records held as one-way hashes	Ireland & Frankfurt, enforced at an infrastructure level	Raw records retained once a match exercise completes	To a written deletion certificate

GETTING YOUR LIST TO MERIDIAN

Files move over HTTPS with TLS 1.2 or higher, whether you upload a CSV directly, or point Meridian at a file already sitting in your own cloud storage, via an AWS S3 presigned URL, a Dropbox share link, or any other direct-download HTTPS host. No long-lived storage credentials or transfer accounts are ever shared with IMI.

You can send raw emails or pre-computed SHA-256 hashes. Either way, the transfer is encrypted in transit. This is a workflow choice, not a security one.

- **Encrypted transport:** TLS 1.2+ on every request, file or URL alike.
- **No long-lived credentials:** links expire on their own, no account or key for either side to issue, store or rotate.
- **Your data, your choice:** upload a file directly, or point Meridian at wherever the file already lives - both are equally secure.

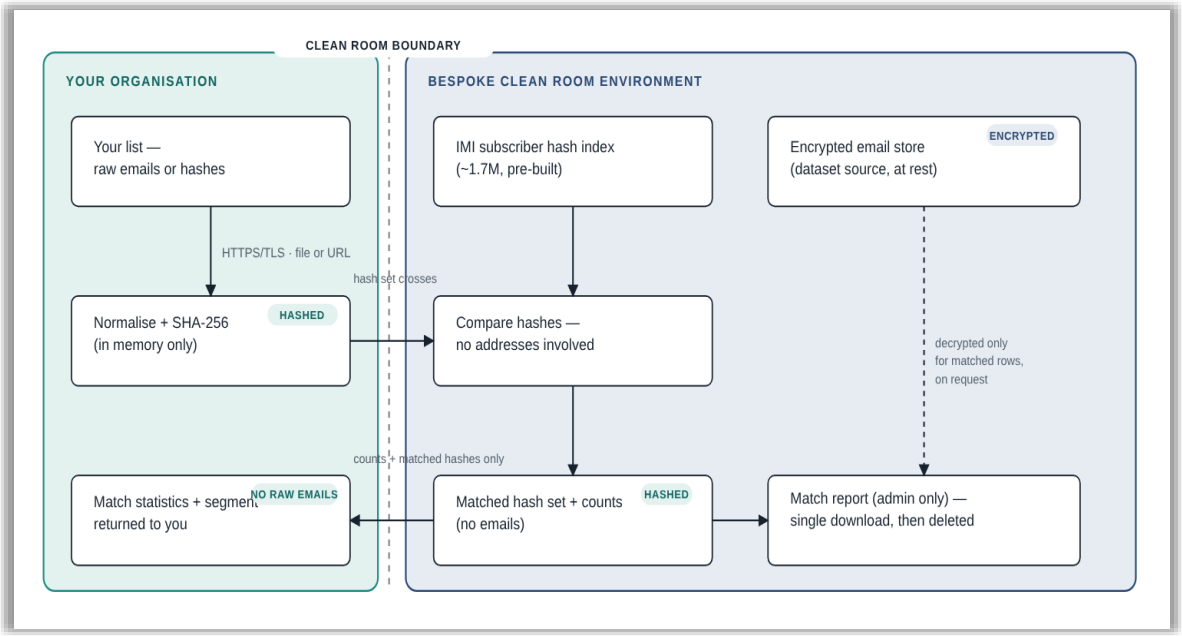
MATCHING WITHOUT EXPOSING EITHER LIST

Once a file arrives, Meridian normalises each address - trim, lower-case - and hashes it with **SHA-256: SHA256(LOWER(TRIM(email))).**

This happens row by row, in memory; the file Meridian keeps afterwards contains hashes only, never addresses. (A brief pass-through happens the instant any file reaches any web server - a basic mechanic of file uploads, not something Meridian stores.) The comparison itself runs separately, inside dedicated infrastructure we call the **Bespoke Clean Room Environment, independently audited to ISO 27001.**

SHA-256 is one-way: an email address cannot be recovered from its hash. Matching is a hash-to-hash comparison against IMI's pre-built subscriber index, and its output is match counts - never a list of email addresses.

Hashed data	One-way SHA-256 output. Cannot be reversed to a raw email address	**Encrypted at rest**	AES-encrypted; decrypted only transiently, only for confirmed matches

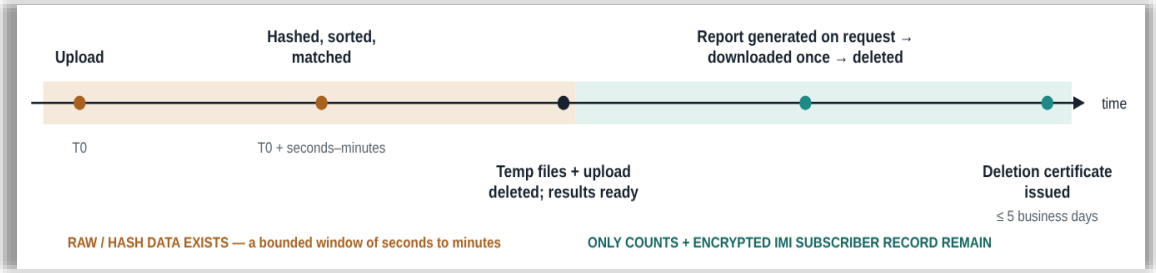


Only hashes cross the Clean Room boundary, in either direction. Your raw list never reaches IMI, IMI's list never reaches you, and only statistics leave the boundary.

HOW LONG YOUR DATA ACTUALLY EXISTS

Matching runs as a background process, separate from your upload request. Your uploaded file, and every temporary working file created along the way, are deleted the moment processing concludes or fails. The record Meridian keeps holds only match/total counts and a pointer to the matched-hashes file, never an email address.

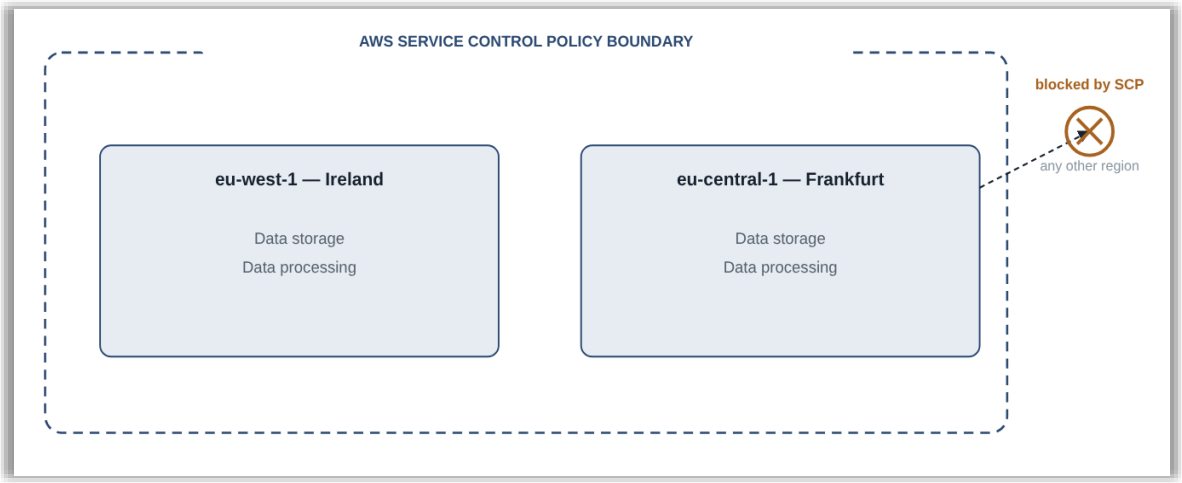
One exception: IMI's own subscriber emails are kept, but only encrypted - solely so a report can later show which contacts matched. That value is decrypted only for matched rows, never in bulk, and only ever surfaces in plaintext inside the report file itself. Downloadable once, then deleted, or purged automatically if never downloaded.



Anything resembling your raw list exists for seconds, not days. After that: statistics, an encrypted dataset record, or nothing at all.

WHERE PROCESSING PHYSICALLY HAPPENS

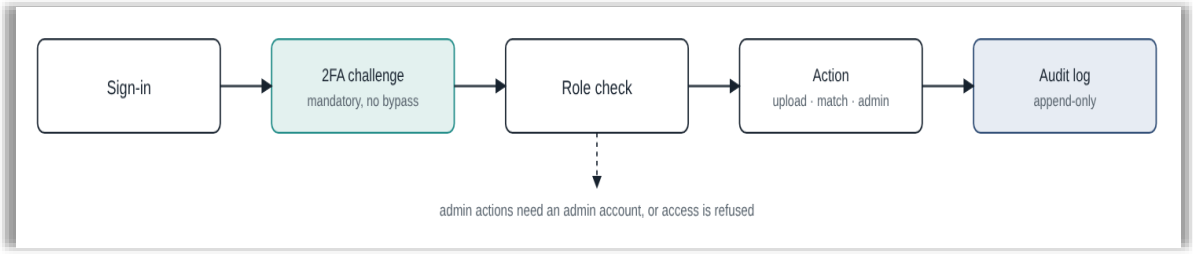
All storage and processing remains inside two **AWS regions: Ireland and Frankfurt**. This is enforced by AWS Service Control Policies at the account level, not just written policy. Resources simply cannot be created outside that boundary. The infrastructure is independently audited to ISO 27001.



Resource creation outside Ireland and Frankfurt is technically blocked at the account level, not just disallowed on paper.

OVERSIGHT - WHO CAN DO WHAT

Two-factor authentication is mandatory for every user, before any matching feature is reachable. Admin functions (managing datasets and exporting audit logs) sit behind a further check: an account without admin rights simply can't reach them. Every action of note including sign-ins, uploads, dataset changes, admin actions is **written to an append-only audit log, exportable on request.**



Access always passes through mandatory 2FA and a role check before an action executes. The action itself is what lands in the audit trail.

TECHNOLOGY AND COMPLIANCE FRAMEWORK

The controls above sit inside a contractual and regulatory framework. Some guarantees come from how the software is built; others come from agreement. the table below keeps the two distinct.

- Meridian's processing follows **UK GDPR, the Data Protection Act 2018, and PECR.**
- A Data Processing Agreement (DPA) is executed with every client before their first match exercise.
- A **named Data Protection Officer at IMI** oversees processing decisions.
- Every completed exercise ends with a written deletion certificate, issued within 5 working days, confirming no supplied data remains on any IMI system.

Safeguard	What it guarantees	Type
HTTPS/TLS ingestion + presigned URLs	Encrypted transport; no long-lived credentials shared	Technical
One-way SHA-256 hashing	Raw email is never the value compared or stored during matching	Technical
Clean Room match environment	Comparison is isolated; only counts leave the boundary	Technical
Temp-file & upload deletion on completion/failure	Nothing persists beyond the processing window	Technical
AWS Service Control Policies	Ireland/Frankfurt residency is enforced, not just declared	Technical
Mandatory 2FA + role-gated admin access	Only verified, authorised users can act on data	Technical
Append-only audit log	Every material action is recorded and exportable	Technical
ISO 27001-audited infrastructure	Independently verified security controls	Contractual
Data Processing Agreement	Legal basis, obligations and liability for each client's data	Contractual
Deletion certificate	Written, auditable confirmation of destruction	Contractual