lumi.

Security & data protection questionnaire

Lumi HR Ltd · company number 17063359 · completed 3 September 2026 · dpo@lumihr.co.uk

Read this first, because it changes which of the questions below matter. lumi benchmarks reward *policies*, not people. Our questionnaire has 317 questions and every one is multiple-choice, yes/no, or a number. **None is free text.** A member cannot submit employee records, names or salaries, because there is no field that accepts typing.

Every question we ask is published without an account at **lumihr.co.uk/register**. You can verify the paragraph above yourself rather than relying on it.

1 · COMPANY AND SERVICE

What does the service do?

A web platform on which UK organisations compare their reward policies — pension, leave, health cover, incentives, pay practice; everything except base salary — against a panel of other UK organisations.

Where is the company established?

England. Lumi HR Ltd, company number 17063359, registered office 6 Chestnut Close, Ampthill, MK45 2PU, United Kingdom.

Is the service multi-tenant?

Yes. Tenant isolation is enforced at the server on every request, not in the interface. A request carrying another organisation's identifier is refused rather than filtered.

Do you use sub-contractors or offshore development?

No. Development and operations are performed in the UK by the company.

2 · WHAT DATA WE HOLD

Do you process our employees' personal data?

No. No employee-level data is collected, and none can be entered. See the note at the top of this document.

Do you process any special category data?

No.

What personal data do you hold at all?

Only for the colleagues who use the platform: work email address, display name, a bcrypt password hash, session and invitation tokens, and a log of actions taken. Typically one to three people per member organisation.

Where is that held relative to the benchmark data?

In a separate database. The analytical store holds no names, no email addresses and no organisation names — those columns are empty by design.

Are you controller or processor?

Controller for the platform accounts described above. For contributed benchmark data no personal data is solicited; the Data Sharing Agreement provides that if personal data is inadvertently submitted, lumi acts as processor on the member's documented instructions and deletes it.

Can other members see our data?

No. Members see anonymised aggregates only. **No figure resting on fewer than five organisations is ever shown** — on screen, in an export, or in a board pack. The floor is enforced in the calculation engine, so it holds for exports and shared links too.

Is our data sold, or used to train AI models?

No, and this is contractual. Contributed data is not sold, rented or disclosed to any third party for that party's own purposes, and is not used to train externally available machine-learning models.

3 · HOSTING AND INFRASTRUCTURE

Where is data hosted?

Amazon Web Services, London region (eu-west-2), United Kingdom. Backups are held in the same region.

Is data encrypted?

In transit, yes — HTTPS/TLS, with HSTS. Backups are encrypted at rest with server-side encryption (AES-256). At rest on the server, the volume holding both databases is encrypted (AWS EBS gp3, encryption enabled), verified 3 September 2026.

What is exposed to the internet?

Ports 443 and 80 only, for the service itself and the certificate renewal redirect; port 80 answers with a permanent redirect to HTTPS and nothing else. Administrative SSH is reachable only from Amazon's EC2 Instance Connect range, so sessions are browser-based and brokered by AWS: there is no direct SSH from any internet address, including our own offices. The application listens only on the loopback interface, behind a reverse proxy.

Do you operate a host firewall as well as a network one?

Yes. Default-deny inbound, with three documented rules, each carrying a comment naming its business purpose.

4 · ACCESS CONTROL

Is multi-factor authentication enforced?

Yes, for **every** user of the platform — not optional, and not administrators only. The application refuses to start in production with MFA disabled. A user may choose to trust the browser they are on, which then skips the emailed code for up to 30 days: the trust token is single-use and rotates on every sign-in, is capped at eight browsers per account, is bound to the one account that earned it, and is destroyed on password change, sign-out everywhere, or admin revocation. Trusting a browser is the user's choice, never the default.

How are passwords stored and governed?

bcrypt, over a SHA-256 pre-hash so there is no maximum password length. Minimum eight characters, common passwords blocked by deny-list, no forced expiry, no complexity theatre — in line with NCSC guidance. Sign-in attempts are throttled to five per five minutes.

Are administrator accounts separate from everyday accounts?

Yes, on every layer: cloud console, server, and staff laptop. Everyday work is done from accounts with no administrative rights.

Is MFA enforced on your own cloud accounts?

Yes, on all six: AWS, Google Workspace, GitHub, Cloudflare, Anthropic and Postmark. The AWS root account holds MFA and no access keys; administration is done through a named account.

How is access removed when someone leaves?

Accounts are deactivated the same day, which immediately ends active sessions and refuses further sign-in while preserving the audit record.

Is there role-based access within our workspace?

Yes — administrator, contributor and viewer, enforced at the server.

5 · SUB-PROCESSORS AND TRANSFERS

SUB-PROCESSOR	PURPOSE	LOCATION	SAFEGUARD
Amazon Web Services	Hosting, encrypted backups	UK (London)	AWS DPA
Anthropic PBC	Narrative text in board packs, from aggregate figures only	United States	SCCs / UK Addendum; no training on inputs
Postmark (Wildbit LLC)	Sign-in codes, invitations, resets	United States	SCCs / UK Addendum

> That is the complete list, published at lumihr.co.uk/legal/subprocessors. Members who have accepted the Data Sharing Agreement are notified before it changes. Each user can switch AI features off for themselves at any time in Settings, and an Admin can switch it off for the whole organisation from the same place — no request to us, effective immediately, overriding every individual setting including new joiners and deleting AI text already generated. Benchmark function is unaffected.

6 · VULNERABILITY AND PATCH MANAGEMENT

How quickly are security patches applied?

Operating system security updates install automatically, daily, with an install log. High-risk and critical fixes are applied within fourteen days, and in practice within a day. Kernel livepatching is enabled, so kernel fixes apply without a reboot.

Is all software vendor-supported?

Yes. The server runs Ubuntu 24.04 LTS with Ubuntu Pro attached, bringing every installed package under vendor security maintenance. Application dependencies are pinned to supported releases.

How do you learn about vulnerabilities in dependencies?

Automated dependency scanning raises a pull request when a dependency has a published vulnerability; these are reviewed and merged inside the fourteen-day window and the change is recorded in a decision log.

Do you run a penetration test?

NOT YET. No independent penetration test has been commissioned. We would rather say so than imply otherwise. It is on the roadmap.

7 · BACKUP AND RECOVERY

What is backed up, and how often?

Both databases, nightly, to encrypted off-site object storage with versioning and a retention ceiling.

Have you tested a restore?

Yes, and this is evidenced rather than asserted. On 3 September 2026 both stores were pulled from the off-site copy, integrity-checked, schema-checked, and queried; the row counts matched the live system exactly on the same day. The drill is repeatable and is re-run after any change to the backup path.

What is your recovery objective?

Recovery point: 24 hours, being the nightly backup. Recovery time: a few hours, being the time to provision an instance and restore. The service is deliberately simple — a single application on one instance — which makes recovery fast and predictable.

8 · LOGGING, MONITORING AND INCIDENTS

What is logged?

Authentication events, administrative actions with the acting user, and sharing actions. Logs are held on the instance with restrictive permissions.

What happens if you suffer a breach?

We contain, assess, and notify affected members without undue delay, and the ICO within 72 hours where the threshold is met. Our contact for this is dpo@lumihr.co.uk.

Do you have a documented incident process?

LIGHTWEIGHT. The company is small enough that the process is short and the responsible person is named. We are not going to describe a 24/7 security operations centre we do not have.

9 · CERTIFICATIONS AND ASSURANCE

STANDARD	STATUS	DETAIL
Cyber Essentials	CERTIFIED	Certified 7 September 2026 by Periculo (certification body) under IASME (Cyber Essentials Partner). Certificate 000b5bc2-a54c-4f22-94ca-2d6188f58ddb, profile 3.3 (Danzell), scope: whole organisation. Recertification due 7 September 2027.
UK GDPR compliance	YES	Article 30 record, Legitimate Interests Assessment and data-minimisation attestation held
ISO 27001	NOT HELD	On the roadmap; not claimed
SOC 2	NOT HELD	On the roadmap; not claimed
Penetration test	NOT HELD	Not yet commissioned
Cyber insurance	HELD	Included cover for Cyber Essentials certificate holders: American International Group UK Limited, £25,000 in the aggregate including defence costs, 7 September 2026 to 7 September 2027, arranged through Sutcliffe & Co. under the IASME master policy.

> **On the gaps.** lumi is an early-stage company and says so. Our published principles commit us to not claiming certifications we do not hold, and this questionnaire is written to the same standard. If a control below your threshold is a blocker, tell us — we would rather know than win the review and disappoint you later.

10 · EXIT

Can we get our data out?

At any time, without asking us. Every benchmark, register and document downloads as CSV or PDF.

What happens if we leave?

On written request, contributed data is deleted from live systems within 30 days and excluded from later benchmark snapshots. Aggregates already distributed — which do not identify you — are not recalled. This is stated in the Data Sharing Agreement rather than left to be discovered.

What if lumi ceases trading?

Your export rights are unconditional and immediate, which is the practical protection. We hold no escrow arrangement.

Lumi HR Ltd · 6 Chestnut Close, Ampthill MK45 2PU · registered in England and Wales, company number 17063359 · dpo@lumihr.co.uk · lumihr.co.uk/security

Answers describe the service as operated on 3 September 2026 and were verified against the running systems on that date. This document is not legal advice. Supporting documents — Data Sharing Agreement, Privacy Notice, Sub-processor List, AI Insights Terms — are downloadable at lumihr.co.uk/security.