

Data Protection Impact Assessment

Draft for completion by the member organisation · lumi sections pre-filled · version 1.0, 3 September 2026

How to use this. Sections in plain text are about lumi and are the same for every member — they are filled in and you can adopt them as they stand. Sections in a **shaded box** are yours: necessity, proportionality, your own risk appetite and sign-off. Nobody can complete those for you and we have not tried.

Whether you need this at all. lumi collects organisation-level reward policies, not employee data, and there is no field in which employee data could be entered. On that basis a full DPIA is often not required. Many organisations run one anyway because their supplier policy says so. This exists so that doing it costs an afternoon rather than a fortnight.

Structure follows the Information Commissioner's own DPIA template.

1 · IDENTIFY THE NEED FOR A DPIA

What is the project?

The organisation subscribes to lumi, a UK reward-benchmarking platform operated by Lumi HR Ltd (company number 17063359). One or more nominated employees answer a structured questionnaire about the organisation's reward policies. In return the organisation sees where its policies sit against an anonymised panel of other UK organisations.

Yours: why the organisation is adopting lumi, who sponsored it, and which of your screening criteria caused this assessment to be opened.

Nature — what data, and how is it collected?

Organisation-level reward policies and practices: pension contribution structures, leave entitlements, health and protection benefits, incentive design, pay practice and governance. Collected through a structured web questionnaire of 317 questions. Every question is multiple-choice, yes/no, or numeric — **none is free text**, so employee records, names and salaries cannot be entered. The complete question set is published without an account at lumihhr.co.uk/register.

Personal data involved

No employee personal data is collected. The only personal data processed concerns the nominated platform users:

CATEGORY	DATA SUBJECTS	PURPOSE
Work email address	Your nominated users	Authentication; delivery of the one-time sign-in code
Display name	Your nominated users	Attribution of actions within your workspace
Password (bcrypt hash)	Your nominated users	Authentication
Session / invitation tokens	Your nominated users	Session management; inviting colleagues
Activity log	Your nominated users	Audit of changes and sharing

No special category data. No criminal offence data. No children's data. Typically one to three data subjects per member organisation.

Scope and duration

Processing continues for the duration of membership. On written request, contributed data is deleted from live systems within 30 days and excluded from subsequent benchmark snapshots; aggregates already distributed, which do not identify the member, are not recalled. Account data is retained while the account exists.

Context — who is involved?

PARTY	ROLE	LOCATION	SAFEGUARD
Lumi HR Ltd	Controller for platform accounts. No personal data is solicited for the benchmark; where personal data is inadvertently submitted lumi acts as processor on documented instructions and deletes it	United Kingdom	Data Sharing Agreement
Amazon Web Services	Sub-processor — hosting and encrypted backups	United Kingdom (London)	AWS data processing agreement
Anthropic PBC	Sub-processor — generates narrative text in board packs from aggregate figures	United States	SCCs with UK Addendum; no training on inputs
Postmark (Wildbit LLC)	Sub-processor — sign-in codes, invitations, password resets	United States	SCCs with UK Addendum

Purposes

To let the member compare its reward policies against an anonymised panel of UK organisations, and to produce cited internal reporting from that comparison.

Yours: the benefit you expect — for the organisation, and for employees. A reward function that can evidence where it sits against the market usually makes better decisions about pay and benefits, but state it in your own terms.

3 · CONSULTATION

Yours: who you consulted — your DPO, works council or employee representatives, information security, and any processor. Record the date and the outcome. lumi is available to answer questions from your DPO directly at dpo@lumihhr.co.uk, and we will join a call with them if that is faster.

Lawful basis

For the organisation-level reward data: not personal data, so no lawful basis under UK GDPR is engaged. For platform account data, lumi relies on legitimate interests and performance of the contract with the member organisation.

Yours: your own lawful basis for nominating employees as platform users — ordinarily legitimate interests or performance of their employment contract — and how you inform them.

Data minimisation

Enforced structurally rather than by policy. The questionnaire has no free-text field, so the platform cannot receive more than it asks for. What is sent to the AI sub-processor is limited to aggregated and derived figures — percentiles, medians, counts of organisations, the text of a policy option. No individual salary and no employee record is transmitted, because neither is collected. A signed data-minimisation attestation evidencing this is available on request.

Preventing function creep

Contributed data is used only to compute anonymised aggregates, operate the member's own workspace, and maintain service quality. It 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. These are contractual terms, not statements of intent.

Individual rights

Platform users can export the personal data held about them at any time. The member can export all contributed data at any time without asking lumi. Deletion on request is covered in section 2. Rights enquiries: dpo@lumihr.co.uk.

Yours: confirm this satisfies your own rights-handling process.

5 · IDENTIFY AND ASSESS RISKS

The risks below are the ones that arise from the processing itself, with the controls lumi already applies. Likelihood, severity and overall risk are left for you, because they depend on your own appetite and context.

RISK	EXISTING CONTROL	LIKELIHOOD / SEVERITY / RISK
Another member identifies your organisation from an aggregate	No figure resting on fewer than five organisations is ever shown — on screen, in exports or in board packs. Enforced in the calculation engine, not the interface	Yours
Unauthorised access to your workspace	Multi-factor authentication enforced for every user (with an optional 30-day trusted browser, single-use rotating token); bcrypt password storage; sign-in throttling; tenant isolation enforced server-side	Yours
Personal data reaching the AI sub-processor	Only aggregate figures are sent; no employee data exists to send. Signed attestation held. Any user may switch AI off for themselves, and an Admin may switch it off for the whole organisation in Settings — immediate, self-service, and it deletes AI text already generated	Yours
International transfer to the United States	Two sub-processors only, both under SCCs with the UK Addendum. Benchmark data is hosted in the UK	Yours
Loss of data or availability	Nightly encrypted off-site backups, with a restore tested and evidenced rather than assumed. Member can export at any time	Yours
An employee is inadvertently identified in a submitted answer	Structurally prevented: no free-text field exists. If personal data is somehow submitted, lumi deletes it on notification and acts as processor to that limited extent	Yours
Supplier ceases trading	Export rights are unconditional and immediate, exercisable without lumi's involvement	Yours

6 • MEASURES TO REDUCE RISK

Yours: any additional measure you decide to apply — restricting who in your organisation holds an account, asking lumi to disable AI features before you begin, requiring a counter-signed Data Sharing Agreement, or scheduling a review date. Record the residual risk and whether it is accepted.

lumi is candid about what it holds and what it does not: Cyber Essentials certified (certificate 000b5bc2-a54c-4f22-94ca-2d6188f58ddb, 7 September 2026; recertification due 7 September 2027); ISO 27001 and SOC 2 are not held; no independent penetration test has been commissioned. These are stated so you can weigh them rather than discover them.

7 · SIGN OFF AND RECORD OUTCOMES

ITEM	NAME / DATE	NOTES
Measures approved by		
Residual risks approved by		
DPO advice provided		
DPO advice accepted / overruled		
Consultation responses reviewed by		
This DPIA will be kept under review by		

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

The lumi sections describe the service as operated on 3 September 2026 and were verified against the running systems on that date. This is a template offered in good faith to reduce duplicated effort; it is not legal advice, and completing it remains the member organisation's responsibility.