



ILLUSTRATIVE EXAMPLE. FICTIONAL ORGANISATION.

GDPR and AI Operations Review

Action Plan

XYZ Recruitment Ltd, 14 staff, London. Prepared by BridgeLayer Advisory.

Version 1.0, July 2026.

Real plans are built from your operations, so no two are alike. The shape is always this: findings in plain English, why each one matters, a priority, a named owner and a target date. Nothing below describes a real business.

1. BUSINESS PROFILE

A 14-person recruitment agency placing permanent candidates with UK employers. Holds candidate CVs, client contacts and employee records across a cloud applicant tracking system, shared drives and email. Runs its own email marketing to a list built over six years. Consultants use AI tools informally to speed up shortlisting and drafting.

2. OVERALL RISK POSITION

Moderate operational risk

XYZ Recruitment Ltd is a well-run agency with careful people in it. The findings below are typical of a business that has grown faster than the documents written for it. Three would become difficult quickly under scrutiny from a candidate, a client procurement team or the regulator. None require a large project to address.

3. KEY FINDINGS

FINDING	WHY IT MATTERS	PRIORITY	OWNER	TARGET
Marketing list is not categorised by recipient type	Different direct-marketing rules apply to corporate subscribers and to individual subscribers such as sole traders and unincorporated partnerships. Without categorisation the team cannot demonstrate which approach applies to which contacts, or evidence it if asked.	High	Marketing lead	Week 2
Candidate CVs pasted into consumer AI tools	Personal data leaves controlled systems with no record of where it went, what the tool retains, or whether the candidate would expect it.	High	Directors	Week 1
Privacy notice describes an earlier version of the business	The notice omits tools and activities now in daily use, so it no longer describes what actually happens to candidate data.	High	Operations lead	Week 3



FINDING	WHY IT MATTERS	PRIORITY	OWNER	TARGET
No named owner for the 72-hour breach decision	A decision with a statutory deadline needs an owner appointed before the day it is needed.	Medium	Directors	Week 2
Processing record incomplete for higher-risk activity	Documentation expectations scale with the nature of the processing. Candidate screening sits at the end where records matter most.	Medium	Operations lead	Week 3
Subject access requests handled ad hoc	Requests are answered by whoever sees them first, with no log and no record that the deadline was met.	Medium	Operations lead	Week 4
Vendor terms not reviewed for processor obligations	Client procurement reviews routinely ask for this, and the answer is currently an assumption rather than a document.	Medium	Operations lead	Week 4
ICO data protection fee position not documented	The registration position has never been assessed or recorded, so nobody can confirm it if a client asks.	Medium	Directors	Week 2
Candidate data retained without a stated period	Old records accumulate in shared drives, increasing what would be exposed by any single incident.	Low	Operations lead	Month 2
No AI-risk screening before adopting a new tool	New tools arrive through individual consultants rather than a decision, so nobody assesses them before candidate data reaches them.	Low	Directors	Month 2
Staff have had no data-protection refresher	Processes only work if the people running them know they exist.	Low	Operations lead	Month 3

All findings shown, ordered by priority.

4. THIRTY-DAY ACTION SEQUENCE

WEEK 1	Circulate the one-page workplace AI rules. Approved tools, what may be entered, what never may, and who to ask when it is not obvious.
WEEK 2	Categorise the marketing list by recipient type and source, document the position for each group, and suppress or remove contacts that cannot lawfully be used.
WEEK 2	Name the owner for breach decisions and put the escalation route on one page. Document the ICO fee position.
WEEK 3	Run a single working session to build the processing record, focused on regular and higher-risk activity rather than every conceivable field.
WEEK 3	Update the privacy notice so it describes the business as it operates today.
WEEK 4	Walk one subject access request and one breach scenario through as a dry run, and fix whatever the dry run exposes.



5. ONE-PAGE WORKPLACE AI POLICY (PREVIEW)

Approved tools: the named tools on the approved list, accessed through business accounts only.

Never enter: candidate CVs, contact details, salary information, client commercial terms, or anything you would not send to a stranger.

Always: check output before it reaches a candidate or client. The tool drafts; a person is accountable.

When unsure: ask the named owner before pasting. Asking is never the wrong call.

6. WHERE SPECIALIST LEGAL ADVICE IS RECOMMENDED

Two items sit at the boundary of legal interpretation rather than operational implementation: the retention position for candidate records tied to an existing client contract, and one clause in a client's data-processing agreement. We have organised the facts for both and recommend that XYZ Recruitment Ltd obtains advice from an appropriately qualified solicitor. We are happy to prepare the brief.

XYZ Recruitment Ltd is a fictional organisation created solely to demonstrate the format of a BridgeLayer action plan. It is not a client, has never been a client, and any resemblance to a real business is coincidental. Findings, owners, dates and the legal-boundary examples above are illustrative. Real plans are built from your operations after a review and remain operational documents. They are not legal advice and not a compliance determination.

BridgeLayer Advisory is a compliance and operations consultancy. It is not a law firm, is not regulated by the Solicitors Regulation Authority and does not provide reserved legal services. bridgelayeradvisory.com

This is a sample. Your plan would be built from your business.

A BridgeLayer Privacy, GDPR and AI Operations Review looks at your privacy notices, processing records, subject access request readiness, breach response, direct marketing, suppliers and workplace AI tools as one operating picture. You receive a prioritised action plan with a named owner and a target date against every finding, the agreed policy and process documents, a thirty day implementation sequence, and a sixty minute walkthrough with one of our founders.

contact@bridgelayeradvisory.com bridgelayeradvisory.com