

# AcmeHR SaaS - Sample AI & Security Response Packet

## Fictional sample disclaimer

This packet uses fictional AcmeHR SaaS and Northwind Bank demo data. Drafts should be reviewed and approved before sharing.

## Buyer request summary

Northwind Bank AI and Security Due Diligence request covering AI usage, subprocessors, vulnerability handling, human oversight, DPIA evidence, and model evaluation.

## Readiness metrics

| Metric                                 | Sample value |
|--|--------------|
| Answers drafted from existing evidence | 43           |
| Require owner review                   | 12           |
| Missing-proof items                    | 7            |
| Need CTO input                         | 3            |

## Selected approved answers

| Buyer question                                 | Draft answer  | Evidence                                    | Status       |
|--|---|---|--------------|
| Do you use AI to process candidate data?       | Yes. AcmeHR uses AI to summarize CVs and support recruiter review of candidate records. | Product specification; DPIA draft           | Needs review |
| Do you disclose AI chatbot usage to customers? | Yes. The support chatbot disclosure is approved for buyer sharing.                      | Chatbot Disclosure Copy                     | Approved     |
| Do you maintain a list of AI subprocessors?    | Yes. OpenAI and Intercom are tracked as AI subprocessors for relevant features.         | OpenAI Vendor Review; subprocessor register | Drafted      |

## Missing-proof items

Human oversight approval, public vulnerability disclosure URL, Legal approval for DPIA sharing, and control owner approval remain open.

## Evidence appendix

OpenAI Vendor Review; DPIA Draft for CV Summarization; Human Oversight Procedure; Vulnerability Disclosure Policy; Model Evaluation Notes.

## Review note

Owner-approved answers can be reused across future buyer requests, but stale evidence should trigger review before the next packet is sent.

Fictional sample. Complain supports readiness and evidence management. It does not provide legal advice. Your team remains responsible for review, approval, and final submission.