AI data-leak checklist

Fill in one card for your company. Fill in what you know; every blank line gets an owner and a date. Any blank line means: that route stays open.

QUESTION	ANSWER	OWNER / BY WHEN
Which personal AI subscriptions do people use for work? (count them)		
Which personal accounts have training switched off? (how many checked, when)		
Which work has moved to a workspace that stays out of training by default?		
What has already been pasted into a public chatbot? (P&L, client data, source code)		
Is that material listed and counted as outside our control?		
Which paid software has AI features switched on? (summarize, draft reply)		
Sub-processor disclosure pulled for each: which outside model provider sits behind each feature?		
Which internal chat tools are built on a public model?		
Which routes have a filter in front of the model? (browser, in code)		
Which sensitive categories does the filter detect? (secrets, keys, regulated data, names)		
Secrets and keys: block and ask why? (yes / no)	☐ Yes ☐ No	
Values where the format matters: swap in synthetic values? (yes / no)	☐ Yes ☐ No	
Customer names in tickets: strip the name? (yes / no)	☐ Yes ☐ No	
Where is the business justification recorded when a prompt is blocked?		
Decision and date	**☐ READY ☐ NOT READY ☐ RE-CHECK ON _____ Date _____ Signed _____**	

AI data-leak checklist

Example (fictional): online pet-food retailer, 140 staff

QUESTION	ANSWER	OWNER / BY WHEN
Which personal AI subscriptions do people use for work? (count them)	About 30 personal chatbot accounts across 140 staff; sales and finance heaviest users	n/a
Which personal accounts have training switched off? (how many checked, when)	All 30 checked on 12 Nov; training off on 30 of 30	n/a
Which work has moved to a workspace that stays out of training by default?	Business workspace bought for finance, 10 seats, live 20 Nov	n/a
What has already been pasted into a public chatbot? (P&L, client data, source code)	Margin summaries for the past two years, two supplier contracts, one pricing script	n/a
Is that material listed and counted as outside our control?	Listed in the risk register on 5 Nov; pricing script owner is rewriting it	n/a
Which paid software has AI features switched on? (summarize, draft reply)	Team wiki summarize button, support desk draft-reply, CRM email rewrite	n/a
Sub-processor disclosure pulled for each: which outside model provider sits behind each feature?	Wiki and CRM: named (same large provider). Support desk: **Blank: not ready**	Support desk admin, by 1 Dec
Which internal chat tools are built on a public model?	One internal "ask the handbook" chat tool, built on a public model's API	n/a
Which routes have a filter in front of the model? (browser, in code)	Browser filter on all 140 managed laptops; handbook tool filtered in code	n/a
Which sensitive categories does the filter detect? (secrets, keys, regulated data, names)	Secrets, keys, customer names, order numbers	n/a
Secrets and keys: block and ask why? (yes / no)	☒ Yes: blocks and asks for a business reason	n/a
Values where the format matters: swap in synthetic values? (yes / no)	☒ Yes: addresses, order totals and dates swapped, same format	n/a
Customer names in tickets: strip the name? (yes / no)	☐ Yes ☒ No: names still go to the draft-reply provider → **Fails the bar**	Support desk lead, by 8 Dec
Where is the business justification recorded when a prompt is blocked?	Logged to a weekly report the CIO reads	n/a
Decision and date	**☐ READY ☒ NOT READY ☐ RE-CHECK ON 8 Dec · Date 14 Nov · "Customer names still leaving with tickets, and one disclosure unread."**	CIO