Aona

Worked customer-support DPIA

DPOs, security architects and customer-service owners

Read the complete guide on aona.ai

A DPIA is required where the proposed personal-data processing is likely to create a high risk under the applicable rules. Assess the specific task and data flow, not ChatGPT in the abstract. This worked example redesigns a raw-ticket proposal before any real customer data is used.

Fictional assessment of wording assistance for customer replies. This completed teaching record reaches a redesign decision rather than asserting the original raw-ticket use is approved.

Synthetic organisation, roles and assessment findings. Proposed safeguards have not been tested; no DPO or supervisory authority approval is claimed.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ **Trace every retained copy**

Include the ticket, AI conversation, attachments, generated drafts and exported evidence.

☐ **Test necessity**

Explain why a generic description or approved template would not meet the proposed real-data purpose.

☐ **Resolve the remaining risk**

Record actual evidence and responsibilities; assess prior consultation where the legal threshold is met.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: _____

Evidence to collect: _____

Owner and next review date: _____

Review matrix

Assessment element	Illustrative finding	Owner or follow-up
Purpose and scope	Improve reply wording; no automated customer decision or sending.	Support owner defines the permitted task.
Original data flow	Ticket text → employee device → ChatGPT workspace → draft back to ticket.	Security maps stored copies and recipients.

Assessment element	Illustrative finding	Owner or follow-up
Necessity and alternative	Generic wording examples can meet the initial purpose without raw tickets.	Support owner chooses the reduced-context design.
Lawfulness and transparency	Any later real-data use needs its Article 6 basis and relevant Article 9 analysis.	Privacy owner verifies grounds and information for customers.
Risk to individuals	Unnecessary identifiers, unexpected health details and misleading drafts could affect customers.	Privacy and support owners assess consequence and scope.
Proposed safeguards	No attachments/connectors in the example; generic inputs; human reply review.	Security verifies actual configuration; support tests the review procedure.
Residual uncertainty	Service terms, retention and effectiveness are not established for a real deployment.	Procurement and security obtain the missing evidence.
Illustrative decision	Do not start raw-ticket processing; begin with invented wording examples.	Reassess real-data scope and any Article 36 implications before a later change.

The proposed data path

- **Source:** Customer ticket system

Keep original records in their controlled source.

- **Input:** Reduced or invented wording context

Exclude identifiers for the teaching exercise.

- **Output:** Human-reviewed draft

No automated reply is enabled by this example.

Invented safe input

Rewrite this generic support message more clearly: “Please check the delivery instructions and contact our support team if they need updating.” Do not invent a customer, account number or personal circumstance.

Illustrative disposition

Original proposal: paste raw tickets.
Decision in this teaching example: redesign; use generic wording context only.
Live-data approval: none represented.
Control validation: not run.
Review trigger: any proposal to add identifiable tickets, attachments, connectors or automatic replies.

Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information; no professional approval or installed-product result is represented. It does not perform the controller's DPIA, establish a lawful basis or route privacy approvals automatically.

EU GDPR: Regulation (EU) 2016/679. Articles 5, 6, 9, 12, 17, 19, 28, 32, 35 and 36 establish the relevant processing, rights, processor and risk-assessment requirements.

ICO: Guidance on AI and data protection. UK guidance on risk assessment, accountability and the use of AI with personal information; distinct from the EU GDPR legal text.