USE CASE BRIEF / 02

Useful AI.
Without uncontrolled data sharing.

An everyday scenario

A fictional employee copies a customer spreadsheet into a personal AI chat to prepare a sales summary. It includes names, email addresses and internal notes. The employer has not approved the account, assessed the supplier or defined a permitted data boundary.

What creates the risk?

The issue is the handling of the information: what is sent, why, who receives it, which account and settings apply, and what safeguards exist. Simply using ChatGPT or another AI tool does not automatically breach the GDPR or trigger a fine.

What could be exposed?

Personal data may be disclosed outside approved controls. Confidential prices, trade secrets or customer commitments may also be exposed, even when they are not personal data. Wrong or incomplete outputs can create a separate operational risk.

A controlled alternative

Use an approved workspace or private agent with a defined purpose. Minimise the input, restrict access and external tools, verify the applicable supplier terms, and have a person review the output. A private deployment still needs governance and testing.

Illustrative use case, not a report of an actual customer incident or enforcement action. General information, not legal advice. Ask your DPO or qualified adviser to assess a specific case. Sources checked 18 September 2026.

EXPOSURE / STATUTORY CEILINGS

What fines could apply?

Up to EUR 10 million or 2%

For the infringements listed in GDPR Article 83(4), the maximum is EUR 10 million or, for an undertaking, 2% of the preceding financial year's total worldwide annual turnover, whichever is higher. Relevant examples can include security and certain controller/processor obligations. [1]

Up to EUR 20 million or 4%

For Article 83(5)-(6) infringements, the maximum is EUR 20 million or, for an undertaking, 4% of the preceding financial year's total worldwide annual turnover, whichever is higher. Examples include basic processing principles, data-subject rights and unlawful international transfers. [1]

These are maximums, not a price per mistake

A fine is not automatic. Authorities assess the circumstances, including seriousness, duration, negligence, mitigation and cooperation. Do not add the two ceilings together as a routine estimate for one incident. An employee's use of a named AI product alone does not determine liability. [1]

The wider business impact

An incident may also lead to investigation, remediation work, disruption and loss of trust. Depending on the facts, other legal or contractual consequences can arise. This guide focuses on GDPR exposure, not a full assessment of AI Act, sectoral or national-law duties.

[1] GDPR Article 83 - full text (independent reproduction)

RESPONSE / FICTIONAL SCENARIO

From shadow AI to an approved workflow.

01 / Contain and establish facts

Stop further unauthorised sharing. Record the account, settings, information, recipients and timing. Restrict access, preserve evidence appropriately and involve the security lead and DPO. Deleting a chat does not prove every downstream copy has disappeared.

02 / Assess notification duties

For a personal-data breach, the controller must notify the authority without undue delay and, where feasible, within 72 hours of awareness, unless the breach is unlikely to risk individuals' rights and freedoms. Document the breach and assessment. A processor informs the controller without undue delay. [2]

03 / Consider the affected people

Where a breach is likely to create a high risk, communication to affected people is generally required without undue delay, subject to Article 34 exceptions. Have the responsible team assess the actual circumstances. [3]

04 / Give employees an approved route

Define permitted tools and data classes, train staff, and offer a useful approved alternative. Scope a knowledge or reporting agent with restricted sources, a confirmed model boundary, retention rules and human review. Test it with representative work before wider use.

[2] GDPR Article 33 - notification duties

[3] GDPR Article 34 - informing affected individuals

PROCUREMENT / EVIDENCE BEFORE CLAIMS

EU residency is a scope. Compliance is an ongoing duty.

Verify the whole data path

Ask for exact countries for storage, inference, logs and backups, plus support access, subprocessors and integrations. Record the scope and exclusions in the contract. A European region is not necessarily EU-only, and residency does not resolve every access or transfer issue.

Distinguish product plans and settings

OpenAI states that business-product data is not used for model training by default. Eligible ChatGPT Enterprise/Edu customers can have residency controls, but Europe includes the EEA and Switzerland. Storage and inference are separate; some metadata and external integrations fall outside the selected boundary. Verify the actual account and enabled features. [4, 5]

What an Eorvo assessment should establish

A data-flow map; approved providers and contracts; lawful-basis and DPIA review where needed; access, retention and deletion controls; incident ownership; and tested deployment settings. These are assessment deliverables to agree, not a claim that this website already meets an EU-only hosting requirement. [6]

[4] OpenAI - business data privacy

[5] OpenAI - residency and inference residency

[6] EDPB - privacy by design and impact assessments

Official GDPR publication (EUR-Lex)

No deployment can promise zero risk. Confirm the legal assessment and contractual scope before processing sensitive data.