When Employees Share Confidential Data w Breach?

31 OCTOBER 2026

Vitalina Petryk

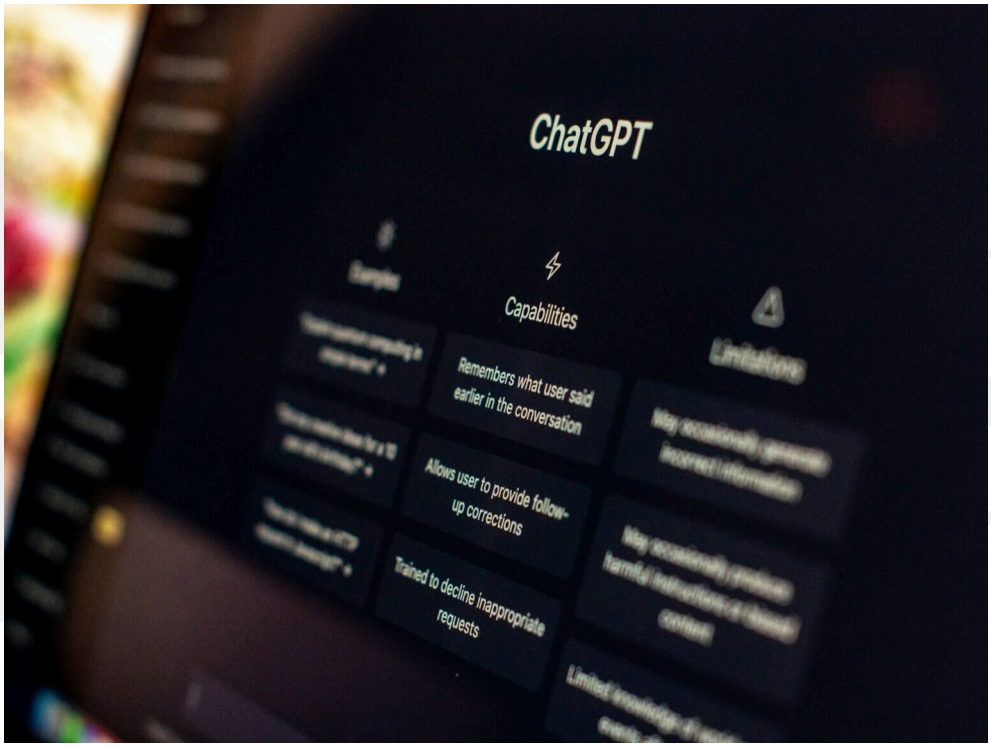


Photo by Emiliano Vittoriosi on Unsplash

Introduction

An employee receives a lengthy workplace document containing personal information about colleagues, clients and business partners. To complete an assignment more efficiently, the employee uploads the entire file to their personal ChatGPT account and requests a summary. The document also contains confidential commercial information. Within seconds, ChatGPT produces the requested response. The employee completes the assignment, deletes the conversation and continues working. Nobody discovers the upload, and no damage is reported.

From the employee's perspective, nothing unusual has happened. The document was not posted publicly, the information was not deliberately

shared with a competitor, and ChatGPT performed the requested task. Nevertheless, the file has been transmitted to an external service provider without the employer's authorisation.

This raises a more precise question than whether ChatGPT is generally compatible with the General Data Protection Regulation (GDPR): can an employee's unauthorised upload itself constitute a personal data breach, even without a subsequent leak or evidence of harm?

This paper examines that question through the GDPR's distinction between processing personal data and a personal data breach, OpenAI's published data-processing practices, and the consequences of an unauthorised disclosure. It argues that a breach can occur at the moment of unauthorised transmission, while regulatory notification, liability and compensation remain separate questions.

What Happens to the Data After an Employee Uploads It?

When an employee uploads a workplace document to ChatGPT, the information is transmitted to OpenAI for processing. Under Section 1 of OpenAI's European Privacy Policy, uploaded files and prompts are classified as "User Content". Section 2 explains that OpenAI processes such information to provide its services, including generating responses, and may also use content to improve its models (OpenAI, 2026).

In the present scenario, the employee uses a personal ChatGPT account with the "Improve the model for everyone" setting enabled. According to OpenAI's Data Controls FAQ, content submitted through personal accounts may be used for model training unless the user disables this setting (OpenAI, n.d.-a). Therefore, the workplace document becomes eligible for model-improvement processing. This does not mean that the document has necessarily been used to train a model, but the employee has allowed this additional use of the information.

The European Data Protection Board (EDPB) specifically addresses this practice in its *Report of the Work Undertaken by the ChatGPT Taskforce*. Paragraph 21 identifies file uploads as part of the information submitted to ChatGPT, while paragraph 22 emphasises that individuals must be clearly informed when such content may be used for training purposes (EDPB, 2024, paras. 21-22).

Importantly, deleting the conversation does not immediately erase the uploaded information. Under Section 4 of OpenAI's European Privacy Policy, deleted personal data is generally removed from its systems within 30 days, subject to exceptions, including legal and security-related retention (OpenAI, 2026). Moreover, files saved separately in ChatGPT's Library remain there even after the associated conversation is deleted (OpenAI, n.d.-b).

Consequently, the employee has already transferred workplace information to an external service provider, regardless of whether the document is

subsequently used for training or publicly disclosed. Deleting the conversation does not undo that transfer. The legal question is therefore whether the employee was authorised to disclose the information to OpenAI in the first place.

When does an Upload Become a GDPR Breach?

Not all confidential workplace information is protected by the GDPR. Under Article 4(1), personal data means information relating to an identified or identifiable natural person. While names, signatures and contact details fall within this definition, confidential business strategies and proprietary source code do not necessarily qualify.

The distinction is illustrated by the Samsung Electronics incidents of 2023. Employees reportedly uploaded confidential source code and internal information to ChatGPT while performing work-related tasks. Samsung subsequently restricted the use of generative AI tools on company devices and networks (Park, 2023). Although no judicial finding of unlawful disclosure arising specifically from these uploads was identified, the incidents demonstrate that employee use of ChatGPT can create confidentiality risks beyond personal data protection. Under EU law, such information may also qualify for protection as a trade secret, provided that it meets the requirements of Article 2(1) of Directive (EU) 2016/943.

In the present scenario, however, the uploaded document also contains personal data. Its transmission to ChatGPT therefore constitutes processing under Article 4(2) GDPR. Articles 29 and 32(4) require employees acting under a controller's authority (in this case, the employer) to process personal data only on instructions, unless otherwise required by law. The employee was authorised to use the document for work, but not to disclose its contents to an external AI provider.

Nevertheless, unauthorised processing and a personal data breach are not identical. Article 4(12) GDPR defines a personal data breach as a breach of security resulting in, among other things, unauthorised disclosure of or access to personal data. It does not require public publication or evidence of subsequent misuse.

The European Data Protection Board (EDPB) illustrates this distinction in Case No. 09 of its Guidelines 01/2021. An insurance agent accidentally gained access to information concerning approximately two dozen customers outside his authorised scope. Although the agent immediately reported the incident and deleted the file, the EDPB classified it as a confidentiality breach (EDPB, 2022, paras. 78-79). Due to the limited risk and effective mitigation, internal documentation was considered sufficient, without notifying the supervisory authority or affected individuals (paras. 80-82).

Applying this reasoning, the employee's upload of identifiable workplace information to an unauthorised external AI provider amounts to an unau-

thorised disclosure. On the established facts, there is a strong legal basis for classifying the incident as a personal data confidentiality breach under Article 4(12) GDPR. The relevant event is the unauthorised disclosure itself, not whether the information is subsequently leaked or misused. Whether the breach must be reported, and whether the employer or employee faces legal consequences, requires a separate assessment.

No Discovery, No Consequences?

The fact that the employer does not discover the upload does not change whether an unauthorised disclosure occurred. However, discovery affects the obligations that follow. Under Article 33(1) GDPR, a controller must notify the supervisory authority within 72 hours of becoming aware of a personal data breach, where feasible, unless the breach is unlikely to pose a risk to individuals' rights and freedoms. Article 34(1) requires informing affected individuals only where a high risk is likely. Nevertheless, Article 33(5) requires controllers to document personal data breaches even when notification is unnecessary (EDPB, 2022, paras. 7, 15). Furthermore, compensation is not automatic. Under Article 82(1), an infringement must cause actual material or non-material damage for compensation to be awarded (*MediaMarktSaturn*, C-687/21, paras. 58-61). Thus, an undiscovered upload may constitute a breach without immediately triggering an investigation, fine or compensation claim.

Who Bears Responsibility?

When an employee uploads confidential workplace information to ChatGPT without authorisation, responsibility does not necessarily rest with the employee alone. Under Article 4(7) GDPR, the employer ordinarily acts as the data controller, while Articles 29 and 32(4) require employees processing personal data under its authority to follow its instructions.

In *BL v MediaMarktSaturn Hagen-Iserlohn GmbH* (Case C-687/21), the Court of Justice held that an employee's accidental disclosure of personal data does not automatically establish that the employer implemented inadequate security measures. The appropriateness of those measures must be assessed under Articles 24 and 32 GDPR, considering the safeguards actually implemented (CJEU, 2024a, paras. 41-45).

However, an employer cannot simply escape responsibility by claiming that its employee disobeyed instructions. In *GP v juris GmbH* (Case C-741/21), the Court clarified that an employee's failure to follow instructions is insufficient, by itself, to exempt the controller from liability under Article 82(3) GDPR. The controller must demonstrate that it is not responsible for the event giving rise to the damage (CJEU, 2024b, paras. 47-54).

Applied to the present scenario, the employer's responsibility therefore depends on more than the existence of an internal prohibition. Its actual security measures, employee instructions and supervision are legally

relevant. Meanwhile, the employee may separately face disciplinary or contractual consequences for disclosing confidential information contrary to workplace obligations. An employee's unauthorised upload may therefore create consequences for both parties, but their legal responsibilities must be assessed separately.

Conclusion

Uploading confidential workplace information to ChatGPT is not automatically a GDPR breach, particularly where the information does not concern identifiable individuals. However, where personal data is transmitted to an unauthorised external service, the disclosure can constitute a personal data breach under Article 4(12) GDPR, even without public exposure or proven misuse.

The absence of immediate harm does not undo the disclosure, although notification, compensation and liability remain subject to separate legal requirements. As the examined case law demonstrates, employee misconduct does not automatically establish employer negligence, nor does it necessarily exempt the employer from responsibility.

Ultimately, the legal risk arises not from using ChatGPT itself, but from disclosing information beyond the employee's authority and the organisation's established safeguards.

References

Court of Justice of the European Union. (2024a, January 25). *BL v MediaMarktSaturn Hagen-Iserlohn GmbH* (Case C-687/21, ECLI:EU:C:2024:72). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0687

Court of Justice of the European Union. (2024b, April 11). *GP v juris GmbH* (Case C-741/21, ECLI:EU:C:2024:288). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0741

European Data Protection Board. (2022). *Guidelines 01/2021 on examples regarding personal data breach notification* (Version 2.0). https://www.edpb.europa.eu/documents/guideline/guidelines-012021-on-examples-regarding-personal-data-breach-notification_en

European Data Protection Board. (2023, April 4). *Guidelines 9/2022 on personal data breach notification under GDPR* (Version 2.0). https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

European Data Protection Board. (2024, May 23). *Report of the work undertaken by the ChatGPT Taskforce*. https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

European Parliament & Council of the European Union. (2016a). Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. *Official Journal of the European Union, L 157*, 1–18. https://eur-lex.europa.eu/eli/dir/2016/943/oj

European Parliament & Council of the European Union. (2016b). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

OpenAI. (n.d.-a). *Data controls FAQ*. https://help.openai.com/en/articles/7730893-data-controls-in-chatgpt

OpenAI. (n.d.-b). *File storage and Library in ChatGPT*. https://help.openai.com/en/articles/20001052-file-storage-and-library-in-chatgpt/

OpenAI. (2026, August 24). *Europe privacy policy*. https://openai.com/policies/eu-privacy-policy/

Park, K. (2023, May 2). *Samsung bans use of generative AI tools like ChatGPT after April internal data leak*. TechCrunch. https://techcrunch.com/2023/05/02/samsung-bans-use-of-generative-ai-tools-like-chatgpt-after-april-internal-data-leak/

EPIS