

# Newsletter

## Tech / Data

3rd QUARTER - 2026

### AI Act: New transparency obligations for AI-generated content now apply

Since 2 August 2026, Article 50 of the AI Act has introduced new transparency requirements for content generated or manipulated using artificial intelligence. Companies must inform the public when certain synthetic content, such as deepfakes, is used, with potential penalties of up to €15 million or 3% of worldwide annual turnover for non-compliance.

# In this issue

€2.33 million fine for Boohoo: misleading crossed-out prices and product composition claims **3**

---

Reporting videos to YouTube: a blocking request based on non-infringing content engages the liability of its author **4**

---

Anti “ultra-fast fashion” law: a ban on promotion by influencers from 1 January 2027 **5**

---

Removal of content on Instagram: the judge distinguishes threatening or harassing content from defamatory accusations **6**

---

Breaking news AI Act: what Article 50 changes regarding transparency of AI-generated content **7**

---

Adoption of the reform of the Union Customs Code: an increased role for e-commerce platforms **8**

---

France Travail: €5 million fine for security flaws identified but not corrected in time **9**

---

ChatGPT, Reddit and Roblox designated under the DSA: reinforced obligations by the end of the year **10**

---

Telephone canvassing: prior consent becomes the rule from 11 August 2026 **11**

---

---

|                                                                                             |           |
|---------------------------------------------------------------------------------------------|-----------|
| First notification of a personal data breach attributed to an artificial intelligence agent | <b>12</b> |
|---------------------------------------------------------------------------------------------|-----------|

---

|                                                                                                            |           |
|------------------------------------------------------------------------------------------------------------|-----------|
| Breaking news AI Act: first formal requests for information from the European AI Office to model providers | <b>12</b> |
|------------------------------------------------------------------------------------------------------------|-----------|

---

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| Uber fined €824.99 million for automated decisions deactivating accounts | <b>13</b> |
|--------------------------------------------------------------------------|-----------|

---

|                                                                                                  |           |
|--------------------------------------------------------------------------------------------------|-----------|
| Cyberattack on the Hôpital privé de la Loire: €500,000 fine for breaches of health data security | <b>14</b> |
|--------------------------------------------------------------------------------------------------|-----------|

---

|                                                                                                                                          |           |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Unfair competition: holding confidential information on a former employee's computer characterises its appropriation by the new employer | <b>15</b> |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------|

---

## LATEST NEWS - TECHNOLOGIES



## €2.33 million fine for Boohoo: misleading crossed-out prices and product composition claims

---

On 20 August 2026, the French Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF) announced that the British online clothing retailer Boohoo had agreed to pay a fine of €2.33 million as part of a criminal settlement. The sanction follows an investigation into the prices of several hundred products.

DGCCRF officers found misleading commercial practices regarding the reality of the advertised promotions: some prices were increased before the promotion was applied, so as to artificially inflate its scale, and other promotions previously applied were not taken into account. In total, 95% of the advertisements inspected were non-compliant: four out of ten offered no price reduction at all, 7% offered a smaller reduction than advertised, and nearly half in fact corresponded to a price increase.

These practices constitute a misleading commercial practice, as defined in Article L. 121-2 of the French Consumer Code, in particular where it relies on false or misleading indications concerning the price or its promotional nature. Price reduction announcements are also governed by Article L. 112-1-1 of the same Code, which requires the trader to indicate the prior price applied before the reduction. Article L. 132-2 of the French Consumer Code provides that misleading commercial practices are punishable by up to two years' imprisonment and a fine of up to **€300,000 or 10% of the average annual turn-over**.

The investigation also revealed failures relating to the composition of textile and footwear products: the terms "leather" or "suede" were used to describe synthetic products, and some information was non-compliant or incomplete.

- This case is a reminder that the crossed-out price, the percentage discount and the statements on product composition are commercial information capable of influencing the purchasing decision. The trader must be able to demonstrate that the displayed price, the announced discount and the characteristics of the product correspond to reality.

## LATEST NEWS - TECHNOLOGIES

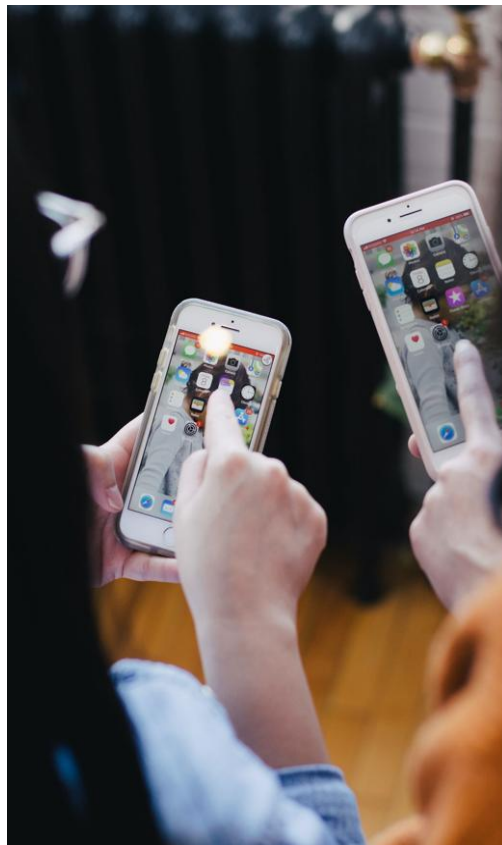
### Reporting videos to YouTube: a blocking request based on non-infringing content engages the liability of its author

Paris Judicial Court (Tribunal judiciaire), 3rd chamber, 2nd section, 19 June 2026, case no. RG 24/03517

By a judgment of 19 June 2026, the Paris Judicial Court ordered a production company to pay €22,000 in damages for having obtained the blocking of videos on YouTube when those videos were not unlawful.

The producer, the author and the director of the programme "Les Incorrigibles" complained that the association Observatoire du conspirationnisme had included, in the opening credits of its programme "Les Déconspirateurs", two-second extracts from two of their programmes. They relied on copyright infringement and, in the alternative, unfair competition. The production company had also requested the blocking of the association's videos on YouTube, and 22 videos became unavailable from February 2024.

The court first dismissed the infringement claim. In its view, the set (a bench against a plain background), the position of the interlocutors and the alternation of wide and close-up shots belong to the common practice of television interviews: their combination is merely an assembly of commonplace elements, showing no free and creative choices. The programme format and the two programmes concerned are therefore not protected by copyright. In the absence of a protected work, the court did not examine the short quotation exception, relied on in the alternative by the association. The claims of unfair competition and parasitism were also dismissed: the two-second extracts serve to illustrate the association's argument in a debate of general interest, and the programme's logo remains visible.



On that basis, the court held the blocking request to be wrongful. It recalled that a notification to a host is not wrongful in itself, since it makes it possible to put an end to unlawful content (Article 6 of the French Law on Confidence in the Digital Economy (LCEN), then Articles 6 and 16 of the Digital Services Act). However, where it comes from a person with a commercial interest, the notification is made at the risk of its author: it is wrongful if it seeks a prohibition that is not justified, which is assessed objectively, in light of the substantive rules, irrespective of the author's good faith. Since the videos were not infringing, they could not be prohibited, and the production company, which had an economic interest in the blocking, incurs liability. By contrast, it was not established that the author and the director, personally, were behind the blocking.

The court rejected the claim for compensation of an economic loss of €41,200, as the association's videos were not monetised. It did, however, award compensation for non-material damage, set at €1,000 per video, i.e. €22,000 for 22 videos blocked for more than two years. The association's claim for abusive proceedings was rejected, and the claimants were ordered jointly and severally to pay the costs and €7,000 to the association under Article 700 of the French Code of Civil Procedure.

- This decision calls for verifying, before any report to a platform, that the content is unlawful under the right relied upon the risk of liability exists even in the absence of bad faith.

## LATEST NEWS - TECHNOLOGIES

### Anti “ultra-fast fashion” law: a ban on promotion by influencers from 1 January 2027

Law no. 2026-602 of 8 July 2026 aimed at reducing the environmental impact of the textile industry (JORF of 9 July 2026)

Law no. 2026-602 of 8 July 2026 aimed at reducing the environmental impact of the textile industry was promulgated on 8 July 2026 and published in the Official Journal of 9 July 2026. It introduces into the French Environmental Code the notion of “ultra-express fashion” (Article L. 541-9-1-1).

Ultra-express fashion covers the industrial and commercial practices of producers that reduce the period of use or the lifespan of textile products, owing to the placing on the market of a high number of new product references and the low incentive to repair these products. These two elements are cumulative. Where an online interface (marketplace, platform) allows the distance selling of such products, the practice is assessed under the same conditions. The thresholds relating to the number of references and the criteria for the low incentive to repair, by brand and by sales channel, will be set by a Conseil d’État decree.

As regards influencers, Article 7 of the law inserts a paragraph IV bis into Article 4 of Law no. 2023-451 of 9 June 2023 on commercial influence. It prohibits any person carrying out a commercial influence activity by electronic means, whether for consideration or free of charge and whatever the form of consideration, from any direct or indirect promotion of products falling within ultra-express fashion and of brands resorting to this practice. The penalty incurred is an administrative fine of up to €100,000, imposed under the conditions laid down in Book V of the French Consumer Code. This prohibition enters into force on 1 January 2027.

Article 6 prohibits more broadly advertising relating to ultra-express fashion products or promoting, directly or indirectly, brands resorting to this practice (Article L. 229-61-1 of the French Environmental Code). For these products, the word “free” may no longer be used as a marketing or promotional tool.

The law contains other measures, in particular the obligation for the platforms concerned to display messages encouraging sobriety, reuse and repair, the display of places of manufacture next to the price for products sold online, and a modulation of producers’ contributions to the eco-organisation, which may take the form of per-product penalties.

The central question remains which brands will be covered. It will depend on the Conseil d’État decree, which will set the thresholds and criteria applicable by brand and by sales channel. Influencers will no longer be able to promote the brands falling within its scope from 1 January 2027.



## LATEST NEWS - TECHNOLOGIES

### Removal of content on Instagram: the judge distinguishes threatening or harassing content from defamatory accusations

Paris Judicial Court (Tribunal judiciaire), accelerated procedure on the merits, 31 August 2026, case no. RG 26/53322



By a judgment of 31 August 2026, the President of the Paris Judicial Court clarified which content a host may be required to remove. A booking agency and two DJs brought proceedings against Meta Platforms Ireland, the host of Instagram, seeking the deletion of an account followed by more than 57,000 subscribers and of its posts (death threats, harassment, photomontages, disclosure of an address, accusations of sexual abuse), which their reports to Instagram had not led to being removed.

The judge recalled the framework. A removal measure may be ordered only if it is justified by the harm, necessary and proportionate with regard to the freedom of expression and the right to privacy of the author of the statements. Where the action is brought by the person targeted against the host and not against the author of the content, no adversarial debate takes place on the reality of the infringement: only manifestly unlawful content can then justify removal, even partial.

What was accepted: threats and harassment. The judge held that the stories with a threatening and harassing tone, which pepper the whole account, were capable of constituting in particular death threats, cyberharassment, doxing and unreported photomontages, and that their deletion was justified. Meta having removed them during the proceedings, the claim was declared moot and Meta was ordered to pay the costs, the claim having been well founded and having succeeded only after the summons.

What was refused: the removal of the accusations of sexual abuse. These imputations are capable of constituting public defamation, but their defamatory nature is not enough to make them manifestly unlawful: defamation may be set aside if proof of truth is provided or if the good faith defence is accepted. The judge noted that, despite the retaliatory motives of the account's author, the circumstances do not rule out that these revelations are well founded, and their removal cannot be ordered as long as their author has not been able to defend himself. The deletion of the entire account, at the risk of affecting lawful content, and the request for keyword filtering, too broad and which would have made inaccessible content whose removal is not permitted, were also rejected. The requests concerning two other accounts were rejected for lack of evidence establishing the existence of the content.

- In practice, an action against the platform makes it possible to have manifestly unlawful content removed, such as threats and harassment, but not defamatory accusations: proceedings against the author of the statements remain necessary in the latter case.

## LATEST NEWS - TECHNOLOGIES

### AI Act: what Article 50 changes regarding transparency of AI-generated content

Regulation (EU) 2024/1689 of 13 June 2024 (AI Act)



Article 50 of the AI Act has applied since 2 August 2026. It is not limited to a labelling obligation: it establishes a transparency regime that distinguishes between providers and deployers of AI systems.

Providers must incorporate a machine-readable marking making it possible to identify synthetic content, in an effective, interoperable and robust manner. This obligation covers text, audio, visual or audiovisual content generated by AI, but excludes mere assistive functions and non-substantial modifications.

Business users, referred to as deployers, must for their part make a visible disclosure in two main situations: when they disseminate a “deepfake”, i.e. content falsely appearing to be an authentic person, object, place or event, and when they publish text generated or manipulated by AI in order to inform the public on a matter of public interest, without human review or editorial responsibility for its content.

Three lessons can be drawn. Technical marking is the provider’s responsibility, while the signalling perceptible to the public falls on the deployer, which requires contractual and technical coordination between the tool’s publisher, the user company, its agencies and the distribution platforms. The existence of genuine human editorial control conditions the transparency obligation for texts of public interest. Finally, compliance requires being able to prove it: identifying the tools used, tracing the generation process, measuring human intervention, qualifying the content and determining who bears the obligation.

Penalties may reach **€15 million or 3% of worldwide annual turnover**.

- Therefore have an interest in mapping their uses and documenting their editorial governance and the liabilities reflected by each party in their contracts.



## LATEST NEWS - TECHNOLOGIES

### Adoption of the reform of the Union Customs Code: an increased role for e-commerce platforms

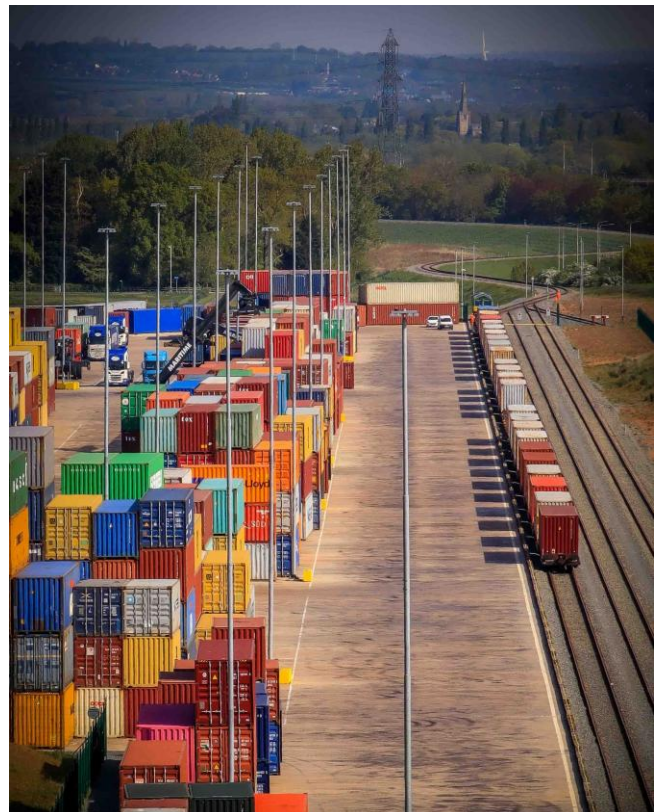
European Parliament, legislative resolution of 16 September 2026, P10 TA(2026)0290 (procedure 2023/0156(COD))

On 16 September 2026, the European Parliament approved, at second reading, the Council's position on the regulation establishing the Union Customs Code and the European Union Customs Authority, and repealing Regulation (EU) No 952/2013. The act is thus adopted in accordance with the Council's position. It must be signed and then published in the Official Journal of the European Union, and will enter into force on the day following its publication, the new rules becoming fully applicable after a period of twelve months.

This reform responds to the increase in the number of parcels shipped from third countries directly to European consumers. It strengthens the involvement of platforms in customs formalities: sellers and platforms established in the Union, or holding the status of authorised economic operator or trusted operator, that sell goods from third countries at a distance to European consumers will be treated as importers. They will have to transmit the required data to the customs authorities, pay or guarantee payment of the applicable duties and charges, and ensure the compliance of the goods. In the event of repeated breaches, they will face a fine of between **1% and 6% of the value of the goods** imported into the Union during the previous twelve months, as well as a suspension or withdrawal of their customs statuses.

The reform also introduces a handling fee applicable to goods ordered from online shops in third countries and shipped directly to European consumers. Its amount will be set by the European Commission and reviewed every two years, and Member States will have to begin collecting it by 1 November 2026 at the latest. This fee may be reduced under certain conditions.

Finally, it provides for the creation of the EU Data Hub, an IT system intended to centralise and exploit the data necessary for customs operations, which is to replace at least 111 IT systems currently used by European customs authorities. Its use will be optional from 2031 and will become mandatory from 2034. A "Trust and Check" regime is also created for businesses that comply with customs rules and cooperate transparently with the authorities: they will benefit from less frequent controls and greater payment flexibility, the authorised economic operator status being maintained in parallel.



## PERSONAL DATA NEWS



### France Travail: €5 million fine for security flaws identified but not corrected in time

CNIL, restricted committee, deliberation no. SAN-2026-003 of 22 January 2026

On 22 January 2026, the CNIL imposed a €5 million fine on France Travail for several security shortcomings that the organisation had itself identified, but failed to address in a timely manner. This decision resonates particularly in light of the recent cyberattack disclosed against the French tax authority (DGFiP) and serves as a timely reminder of the importance of promptly implementing identified security measures.

Between 6 February and 5 March 2024, attackers used social engineering techniques to impersonate several employee accounts of the CAP EMPLOI structures, which accessed France Travail's business application used to support jobseekers with disabilities. The data of 36,820,828 persons was exfiltrated, in particular civil status, social security number, postal address, contact details and jobseeker status. The breach was notified on 8 March 2024.

The CNIL found four breaches. The first concerns the robustness of authentication: accounts were locked only after 50 unsuccessful attempts, as against a maximum of 10 under its recommendation, with no compensating measure. This breach was upheld even though it was not exploited by the attackers, compliance being assessed with regard to the appropriateness of the measures and not the attack scenario that occurred. The second, the most serious, is the absence of multifactor authentication: the 2022 impact assessments had identified the risk and planned a rollout in 2023, postponed to April 2024. The other two concern the use of the application's activity logs and access authorisations, CAP EMPLOI advisers being able to consult the data of all jobseekers, which exceeded what was strictly necessary.

France Travail argued that the CAP EMPLOI structures, as joint controllers, should bear part of the security measures. The CNIL rejected this argument: the agreements placed the technical security of the tools and the control of access authorisations on France Travail, and it was for France Travail to steer the security measures of its information system. It also rejected the argument that an establishment of this type escapes the fine: the exclusion provided for processing "carried out by the State" is interpreted strictly, and France Travail, which has legal personality, is financed by the State for only one third.

The CNIL found gross negligence, the impact assessments having listed the risks that materialised more than two years later. The €5 million fine, against a legal ceiling of €10 million, is accompanied by an injunction to demonstrate compliance, subject to a penalty of €5,000 per day of delay. This decision is a reminder that an impact assessment that identifies a risk and plans a measure can be turned against the controller if the measure remains deferred: any postponement must be dated, reasoned and accompanied by an interim measure.

## PERSONAL DATA NEWS

### **ChatGPT, Reddit and Roblox designated under the DSA: reinforced obligations by the end of the year**

---

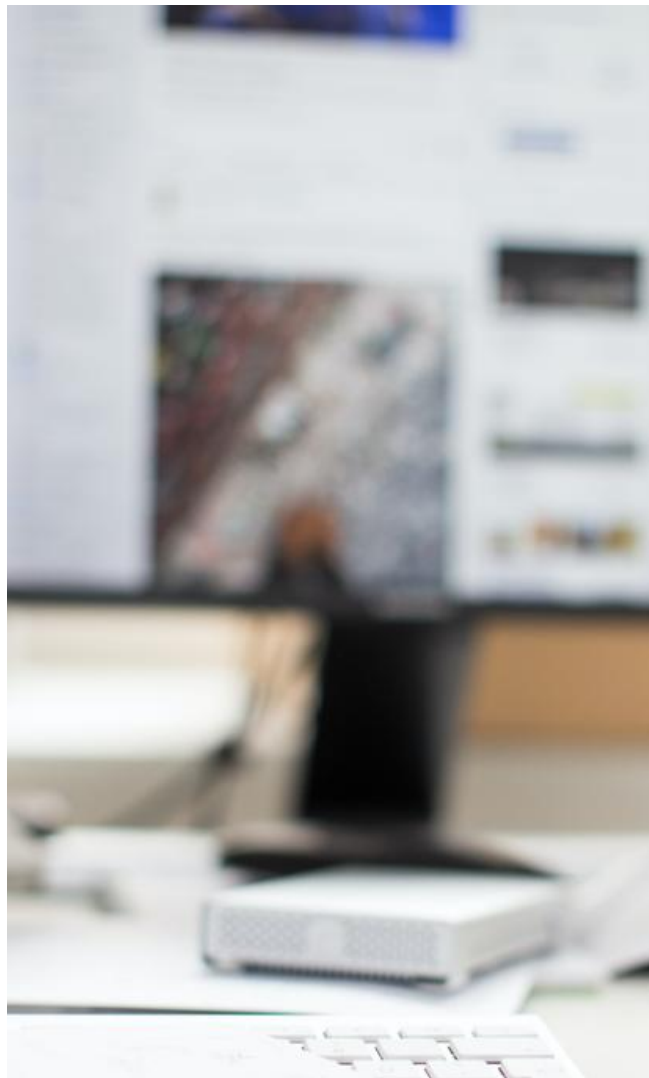
European Commission, Regulation (EU) 2022/2065 (DSA)

On 31 August 2026, the European Commission designated ChatGPT as a very large online search engine, a first for an artificial intelligence service, as well as Reddit and Roblox as very large online platforms. Each of these three services reports at least 45 million monthly active users in the Union, the threshold from which these rules apply.

The Commission considers ChatGPT to be a hybrid service falling within the category of online search engines, since it can respond to users' queries by searching the Internet.

The three services have four months to comply with the additional obligations provided for by the DSA: annual assessment of systemic risks (illegal content, effects on minors, public health, electoral processes, fundamental rights), mitigation measures for these risks, annual independent compliance audits, and transparency of recommendation algorithms, with an option without profiling and data access for vetted researchers.

This designation also gives the Commission investigatory powers enabling it to examine the functioning of these services. It will supervise their compliance in cooperation with the Irish regulator Coimisiún na Meán for ChatGPT and Reddit, and with the Dutch Authority for Consumers and Markets for Roblox.



## PERSONAL DATA NEWS

### Telephone canvassing: prior consent becomes the rule from 11 August 2026

Law no. 2025-594 of 30 June 2025 against all forms of fraud in public aid



Since 11 August 2026, telephone canvassing of consumers has been prohibited in principle, pursuant to Article 13 of Law no. 2025-594 of 30 June 2025, which amends in particular Articles L. 221-16 and L. 223-1 et seq. of the French Consumer Code.

The opt-out regime, under which the professional could call as long as the person had not objected, disappears in favour of a prior consent ("opt-in") regime: consent must be freely given, specific, informed, unambiguous and revocable. The main exception concerns an ongoing contract, where the call relates to its subject matter, including to offer complementary products or services.

The CNIL has updated its practical guides on commercial prospecting. It integrates the new regime for telephone communications aimed at consumers and clarifies the boundary between three types of communications: commercial (promotion, which requires consent), transactional (order confirmation, invoice, password) and relational (customer follow-up, without promotional purpose).

- Obtaining valid consent is not enough, however: it must also be possible to prove that it was lawfully obtained. The professional must be able to trace when it was given, the channel used, the purpose, the version of the form in force on that date and its retention over time. The challenge is therefore both evidential and operational.

## PERSONAL DATA NEWS

### First notification of a personal data breach attributed to an artificial intelligence agent

---

The Spanish Data Protection Agency (AEPD) has received the first notification of a personal data breach attributed to an artificial intelligence agent. The agent reportedly managed to detect the vulnerabilities of an application processing such data, then to break into it in order to access the information and modify invoices.

Without concluding that there is a statistical trend, the AEPD points out that the malicious use of artificial intelligence tools is already common, in particular in phishing operations, and warns of the worsening of the threat linked to the development of these tools.

- According to the AEPD, this notification requires existing security arrangements to evolve. Controllers must now include attacks using artificial intelligence in their risk analyses, re-examine their reaction times, strengthen platform authentication mechanisms and put in place automated detection systems.



### Breaking news AI Act: first formal requests for information from the European AI Office to model providers

---

The European AI Office has sent its first formal requests for information to several providers of general-purpose AI models. The Executive Vice-President of the Commission, Henna Virkkunen, presented this step as a first stage in the enforcement of the AI Act.

Two categories of requests were sent. The first concerns model safety, independent external evaluations and the monitoring of models once placed on the market. The second concerns the summaries of the content used for training the models, and targets providers that have not published details on this subject or taken part in the informal compliance dialogues conducted with the AI Office. This second category has copyright implications, as rights holders need these summaries to determine whether their works have been used.

These requests are legally binding: providing inaccurate, incomplete or misleading responses constitutes a breach liable to a fine. At this stage, however, they do not amount to a finding of infringement of the AI Act, and no restrictive measure has been taken against any model.



## PERSONAL DATA NEWS



### Uber fined €824.99 million for automated decisions deactivating accounts

---

In August 2026, the Dutch Data Protection Authority imposed a fine of €824.99 million on Uber. It criticises Uber for having deactivated drivers' accounts through automated systems, in breach of Article 22 of the GDPR.

The proceedings originate in a complaint filed in France in 2020 with the CNIL by the Ligue des droits de l'homme, which represented 171 drivers. As Uber has its main establishment in the Netherlands, the Dutch authority was the lead authority under the one-stop-shop mechanism, the CNIL having nevertheless been involved in the investigation. This is the third sanction imposed in this case, after a fine of €10 million in 2023 for failures to inform drivers and a fine of €290 million in 2024 for transfers of data outside the European Union.

The authority found that, between 2018 and 2022, account deactivations in cases of suspected fraud (for example detours to increase the fare) or low ratings by customers had been decided without any human intervention. It classifies them as automated individual decisions within the meaning of Article 22 of the GDPR, which significantly affect drivers since deactivating the account paralyses their activity and deprives them of income. It also found that drivers were not sufficiently informed about the process leading to deactivation.

Uber disputes part of the facts, considers the sanction disproportionate and has announced that it will appeal. This fine would be the second largest imposed under the GDPR, after the €1.2 billion fine imposed on Meta in 2023.

- Any organisation that excludes, suspends or rates individuals in an automated manner must ensure that human intervention in the decision-making process is genuine.

## PERSONAL DATA NEWS

### Cyberattack on the Hôpital privé de la Loire: €500,000 fine for breaches of health data security

CNIL, restricted committee, deliberation no. SAN-2026-009 of 21 July 2026

The CNIL imposed a fine of €500,000 on the Hôpital privé de la Loire (HPL), an establishment of the Ramsay Santé group, following a cyberattack of exceptional magnitude. On 1 July 2025, the establishment discovered that an attacker had broken into its electronic patient record. The attacker had exfiltrated 524,867 records containing in particular civil status and health data, social security numbers, contact details and copies of identity cards, as well as the data of 202,246 trusted third parties. Having received the notification and nine complaints, the CNIL carried out an on-site inspection.

Recalling, following the Court of Justice of the European Union, that Article 32 of the GDPR establishes an obligation of means which may be breached where security measures are insufficient in light of the identified risks, the restricted committee noted five failings: the absence of two-factor authentication for external remote access, contrary to the framework applicable to digital health services; insufficient partitioning of patient records; the absence of automated, real-time analysis of application logs; the transmission to all external practitioners of the same temporary password by a third party; and the permanent and uncontrolled access of the software publisher to the patient record.



A breach of Article 34 of the GDPR was also found. While patients were properly informed, no direct communication was sent to the 202,246 trusted third parties concerned, the publication of a press release on the establishment's website not satisfying the requirement of individual information, all the more so as these persons have no reason to consult it.

To determine the ceiling and the amount of the fine, the restricted committee applied the notion of "undertaking" within the meaning of Articles 101 and 102 TFEU and thus took into account the Ramsay Santé group, of which the hospital is a subsidiary. Although this is a decision on its particular facts, its reasoning provides lessons for all healthcare establishments using an electronic patient record. The deliberation may be appealed to the Conseil d'État within two months of its notification.

## PERSONAL DATA NEWS

### Unfair competition: holding confidential information on a former employee's computer characterises its appropriation by the new employer

French Court of Cassation (Cour de cassation), Commercial Chamber, 2 September 2026, appeal no. 25-12.718, published in the Bulletin

By a judgment of 2 September 2026 published in the Bulletin, the Commercial Chamber of the French Court of Cassation held, on the basis of Article 1240 of the French Civil Code, that the appropriation of confidential information belonging to a competing company, brought by a former employee, constitutes an act of unfair competition, even where that employee is not bound by a non-compete clause. It adds that the mere holding of that information on the employee's work computer is sufficient to characterise its appropriation by the new employer.

In this case, an employee of the company Fluides service distribution (FSD) had resigned with effect from 28 September 2018 in order to join a competing company, EPAI, on 1 October 2018, his contract being transferred in 2019 to a subsidiary of the latter, which became GSIS. FSD had had recorded on the former employee's work computer the presence of a file belonging to it, containing its customers' contact details, as well as several price offer templates, and had summoned both companies in 2021.

The Toulouse Court of Appeal had rejected the claims against GSIS and limited to €283 the damages payable by EPAI, on the ground that the former employee's holding of the documents did not prove their appropriation by his new employers, who denied having knowledge of them. The Court of Cassation overturned this reasoning: in so ruling, when the mere holding of that information on the work computer characterises its appropriation by the new employer, the Court of Appeal failed to draw the legal consequences of its own findings. It follows that the victim company does not have to show that the new employer knew the origin of the files or that it had actually used them.

The judgment is quashed insofar as it rejects the claim for an order against GSIS and limits to €283 the order against EPAI. The case is remitted to the Bordeaux Court of Appeal, which will have to re-examine the liability of the companies concerned and the extent of FSD's economic loss.





Stéphanie Berland

**Partner**

T: +33 1 40 69 26 63

E: s.berland@dwf.law



Emmanuel Durand

**Partner**

T: +33 1 40 69 26 83

E: e.durand@dwf.law



Florence Karila

**Partner**

T: +33 1 40 69 26 57

E: f.karila@dwf.law



Anne-Sylvie Vassenaix-Paxton

**Partner**

T: +33 1 40 69 26 51

E: as.vassenaix-paxton@dwf.law

### **About this newsletter**

*This newsletter is published under the supervision of **Stéphanie Berland**, Partner.*

*The firm warmly thanks Méliissa Boudjella for her assistance in the preparation of this publication.*

DWF is a leading global provider of integrated legal and business services.

Our Integrated Legal Management approach delivers greater efficiency, price certainty and transparency for our clients.

We deliver integrated legal and business services on a global scale through our three offerings; Legal Services, Legal Operations and Business Services, across our key market groups. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

© DWF, 2026. DWF is a global legal services, legal operations and professional services business operating through a number of separately constituted and distinct legal entities. The DWF Group comprises DWF Group Limited (incorporated in England and Wales, registered number 11561594, registered office at 20 Fenchurch Street, London, EC3M 3AG) and its subsidiaries and subsidiary undertakings (as defined in the UK's Companies Act 2006). For further information about these entities and the DWF Group's structure, please refer to the Legal Notices page on our website at [www.dwfgroup.com](http://www.dwfgroup.com). Where we provide legal services, our lawyers are subject to the rules of the regulatory body with whom they are admitted and the DWF Group entities providing such legal services are regulated in accordance with the relevant laws in the jurisdictions in which they operate. All rights reserved. This information is intended as a general discussion surrounding the topics covered and is for guidance purposes only. It does not constitute legal advice and should not be regarded as a substitute for taking legal advice. DWF is not responsible for any activity undertaken based on this information and makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability or suitability of the information contained herein.

[dwfgroup.com](http://dwfgroup.com)