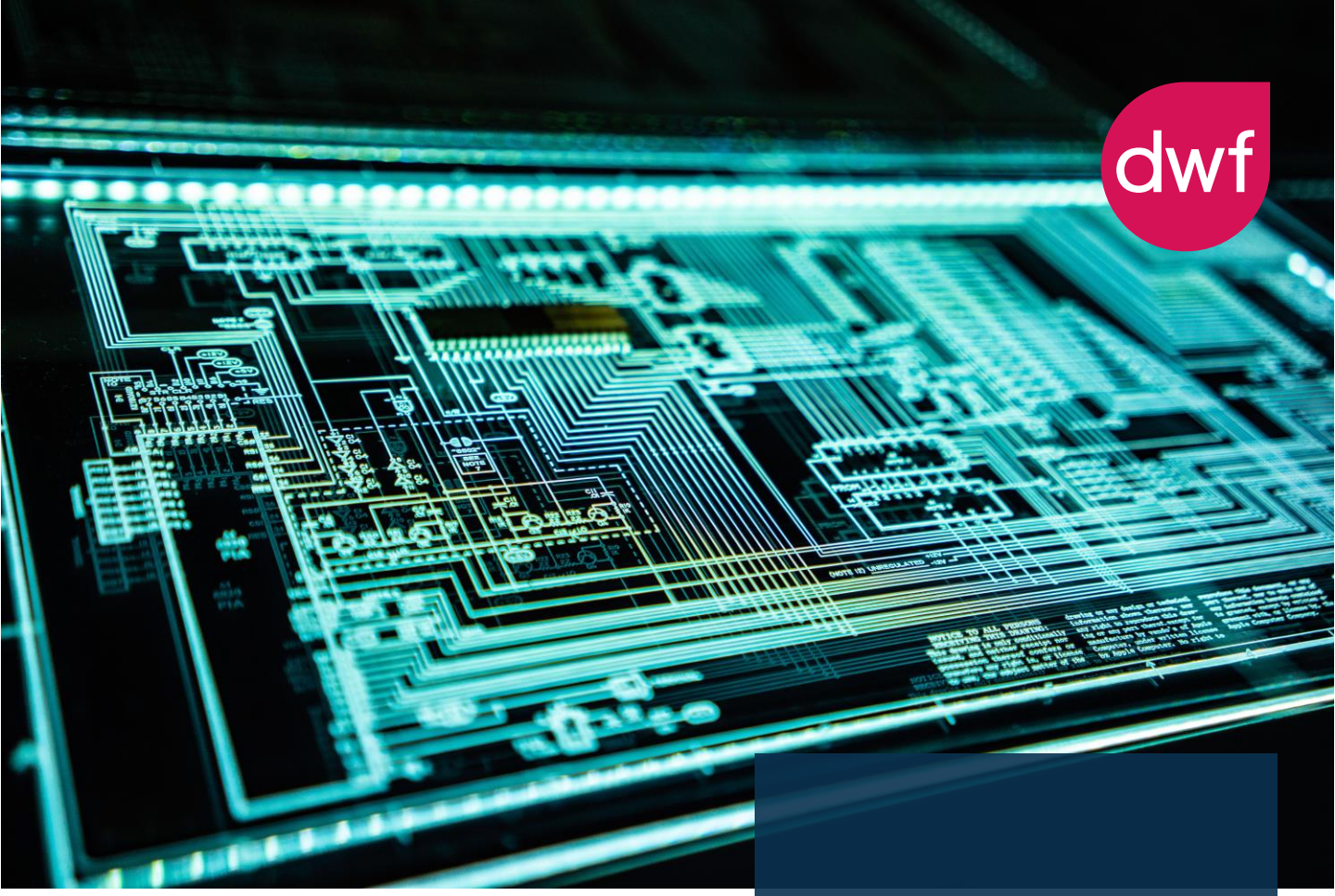


Newsletter

Tech / Data

January – February 2025

EU IA Act: publication of guidelines on prohibited practices

The European Commission is gradually publishing its guidelines for a uniform application of the IA Act

In this issue

LATEST NEWS - TECHNOLOGIES

Two recommendations from the CNIL on the development of innovative and responsible AI

CNIL, recommendations for informing individuals
CNIL, recommendations on individuals' rights

On February 7, 2025, the CNIL published two recommendations to ensure the development of artificial intelligence (AI) in compliance with the General Data Protection Regulation (GDPR). These recommendations, developed following a public consultation, focus on two essential points:

- Firstly, the need to strengthen the information provided to individuals. People must be clearly informed when their personal data are used to train an AI model. This information must be accessible, transparent, and tailored to the specific risks associated with data usage.
- Secondly, the importance of facilitating the exercise of users' rights. European legislation offers concrete solutions to enable citizens to more easily exercise their rights, such as the right of access, rectification, or objection to the processing of their data. The goal is to ensure better control for users over their personal information.

The CNIL also encourages the development of responsible AI that respects privacy. It recommends integrating data protection from the design phase of AI models (privacy by design) and implementing mechanisms to prevent the disclosure of confidential personal data.

The CNIL's stated objective is to reconcile technological innovation with the respect of fundamental rights to strengthen public trust in AI technologies and ensure their responsible and ethical deployment.

European Commission guidelines on prohibited AI practices

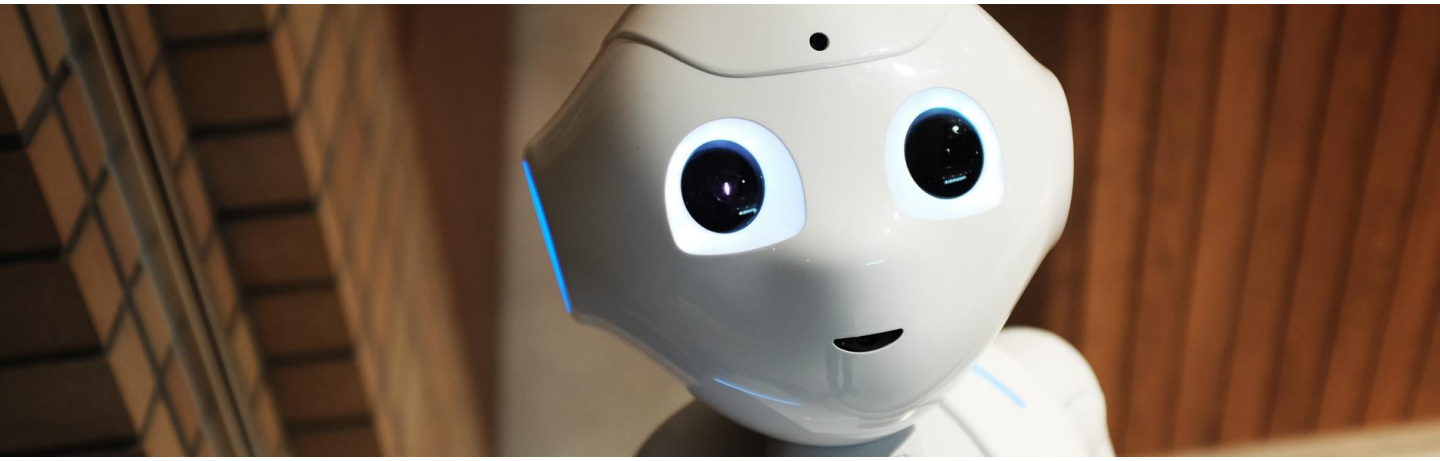
European Commission, guidelines, 2025/02/04

On February 4, 2025, the European Commission published a draft of guidelines detailing artificial intelligence (AI) practices deemed prohibited and unacceptable due to their potential risks to European values and fundamental rights by the AI Act. These guidelines aim to ensure a consistent and effective application of the AI Act across the EU by providing legal explanations and practical examples to help stakeholders understand and comply with the legislation.

These guidelines focus on prohibited AI practices, particularly AI systems that manipulate individuals' decisions or exploit their vulnerabilities, systems that evaluate or classify people based on their social behavior or personal characteristics, leading to unjustified or disproportionate treatment, and systems that identify individuals remotely in real-time in public spaces.

The Commission has approved the draft of these guidelines, which still need to be formally adopted.

LATEST NEWS - TECHNOLOGIES



Opinion of the European Commission on the model for the summary of training data to be provided by AI providers

European Commission, opinion, 2025/01/17

The AI Act requires AI providers to make available to the public a sufficiently detailed summary of the content they use to train their models, in order to allow parties with a legitimate interest to assert their rights. This aims to ensure a balance between the transparency of the data used and the protection of the trade secrets of AI providers.

On January 17, 2025, the European Commission published an opinion on the model to be used to establish this summary.

This model applies to all sources of content, regardless of the stage of their use in AI training. The European Commission has specifically stated that this transparency, implemented through the model, must be simple and understandable for the public while being sufficiently detailed to achieve its objective, which is to help parties with legitimate interests exercise their rights.

The model consists of three sections. The first relates to general information, including the AI model and its provider, as well as the size, modalities, and overall characteristics of the training data.

The second relates to the list of data sources (publicly accessible data, data acquired by the provider, etc.), and the third covers other relevant aspects of data processing, such as measures implemented to ensure compliance with literary and artistic property rights or those implemented to remove undesirable content.

This model is being developed in parallel with the Code of Good Practices, the publication of the third draft of which is expected in the coming months.

LATEST NEWS - TECHNOLOGIES

Expiry of a financial lease contract for IT equipment in case of termination of the maintenance contract

Cass. com., 2025/02/05, No. 23-23.358

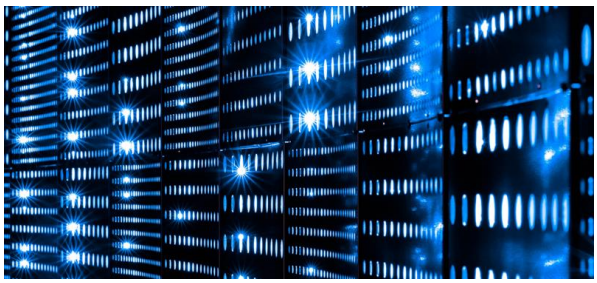
On February 5, 2025, the Commercial Chamber of the Court of Cassation rendered an important decision regarding the expiry of a financial lease contract for IT equipment.

The companies Logar'Auto and Locam had concluded a financial lease contract for office equipment provided by the company Olicopie, which also ensured its maintenance. Due to breaches of its obligations, Nogar'auto terminated the maintenance contract with Olicopie after a formal notice remained unsuccessful. Nogar'auto then notified Locam of the expiry of the financial lease contract, considering that the termination of the maintenance contract justified its end. Olicopie was subsequently placed in liquidation.

Locam sued Nogar'auto to obtain payment of unpaid rents. Nogar'auto defended itself by invoking the expiry of the financial lease contract due to the prior termination of the maintenance contract.

The Court of Appeal of Lyon rejected Nogar'auto's arguments regarding the expiry of the contract and ordered it to pay 10,335.60 euros with interest.

On February 5, 2025, under the provisions of articles 1186, paragraphs 2 and 3, 1124, and 1226 of the Civil Code, the Court of Cassation overturned the decision of the Court of Appeal of Lyon, stating that the termination of the maintenance contract resulted in the expiry of the associated financial lease contract, without the need to involve the maintenance provider, the company Olicopie.



The US Copyright Office takes a position on the protection of AI-generated results

U.S. Copyright Office, Report, 2025/01/09

On January 29, 2025, the US Copyright Office published the second part of its Report on the legal and policy issues related to copyright and artificial intelligence (AI). This part of the report addresses the possibility of copyright protection for AI-generated creations.

According to the report, "existing principles of copyright law are sufficiently flexible to apply to this new technology" and do not require specific legislative changes at this stage. Thus, the US Copyright Office reaffirms that a creation can only be protected by copyright if a human author makes a significant expressive contribution to it. Simply providing a prompt to an AI is not enough to claim copyright. However, a hybrid work, combining AI-generated elements with human and creative modifications, could benefit from protection. The Copyright Office plans to update its guidelines on the registration of works incorporating AI to provide more clarity to creators and businesses.

A forthcoming third part of the report will address another key issue: the use of copyrighted works to train AI models, raising major concerns regarding licensing and legal liability. This issue, which raises significant concerns, particularly regarding respect for copyright, will therefore be at the heart of upcoming debates.

LATEST NEWS - TECHNOLOGIES

The refusal of interoperability by a company can constitute an abuse of dominant position

CJUE, 2025/02/25, C-233/23

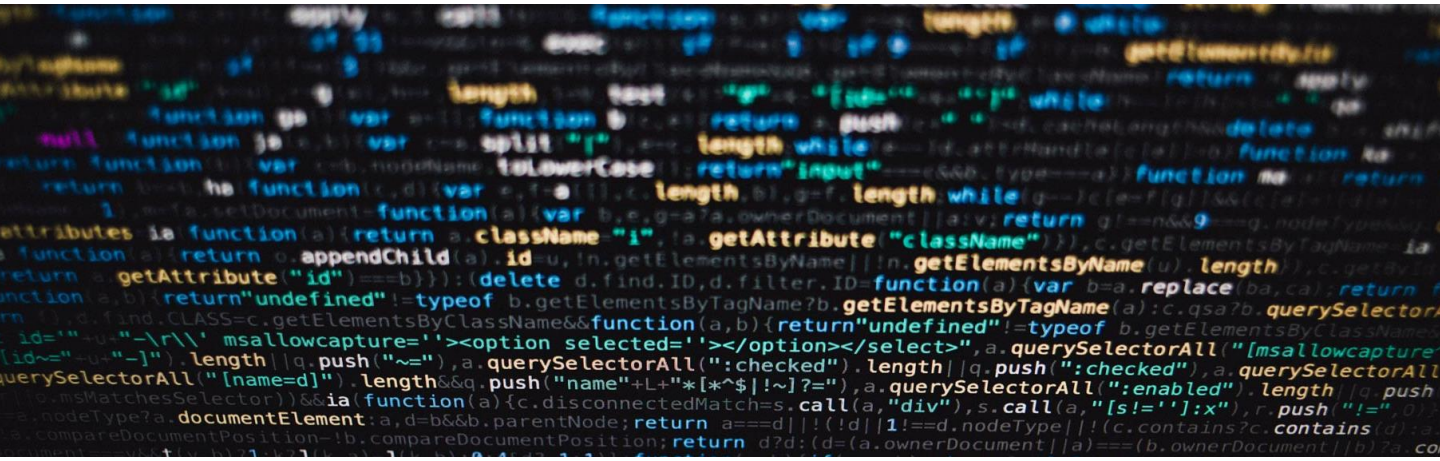
The dispute originates from Google's refusal to make its Android Auto platform interoperable with the JuicePass application, developed by Enel X Italia. Launched in 2018 to facilitate access to electric vehicle charging services, JuicePass was intended to allow users to access charging stations via a digital interface integrated into vehicle infotainment systems. After several requests from Enel X Italia, Google cited security and resource management reasons to refuse this interoperability, thus reserving access to multimedia and messaging applications only.

The AGCM (Autorità Garante della Concorrenza e del Mercato), the Italian competition authority, sanctioned Google, Google Italy, and Alphabet for abuse of dominant position, considering that the refusal of access had an anti-competitive effect by unduly favoring Google's services, particularly its Google Maps application. The AGCM's decision, accompanied by a fine of over 102 million euros, was appealed before the Italian courts, ultimately leading the Italian Council of State to refer preliminary questions to the CJEU regarding the application of Article 102 of the TFEU.

In a judgment dated February 25, 2025, the CJEU affirmed that when a company in a dominant position, having developed a digital platform, refuses to ensure its interoperability with an application developed by a third party, this refusal can be considered an abuse of dominant position. This qualification is retained even if the platform is not strictly indispensable for the commercial exploitation of the application in a downstream market. Indeed, if access to the platform makes the application more attractive to consumers – and especially when the platform was not designed exclusively for the internal needs of the dominant company – a refusal can hinder innovation and distort competition.

In this judgment, the CJEU adapts competition law to the specificities of digital markets. It seeks to ensure that dominant companies cannot block innovation by refusing access to features that, even if not essential for the commercial exploitation of an application, significantly enhances its attractiveness to consumers. This legal framework thus provides a tool to assess potentially abusive behaviors, while taking into account the technical and competitive realities of the digital environment.

LATEST NEWS - TECHNOLOGIES



Possibility of enhanced contractual obligations for hosts regarding the content they publish or store

Cass. com., 2025/01/15, No. 23-14.625

In a ruling dated January 15, 2025, the Commercial Chamber of the Court of Cassation affirmed that hosts could be subject to enhanced contractual obligations regarding the content they publish or store.

In 2013, the company Dstorage concluded a contract with Société Générale, allowing it to offer a secure card payment service to its users. In 2015, the bank decided to terminate this agreement after discovering the presence of illegal content violating intellectual property rights on the platform. The termination decision was based on Article 1.4 of the contract, which provided for such a possibility in the event of proven illegal activities.

Dstorage contested this termination, arguing that it could not be held responsible for the files uploaded by its users and that it had responded to notifications by removing the infringing content. The company then took legal action to request the restoration of the payment service and the award of damages.

In its ruling on January 15, 2025, the Court of Cassation rejected Dstorage's appeal, confirming the decision of the Paris Court of Appeal dated March 3, 2023. The judges thus considered that Article 6 of the Law for Confidence in the Digital Economy allows the parties to a contract to include clauses imposing a monitoring obligation on hosts. In this case, Dstorage had not provided evidence that it had implemented technical measures to prevent the recurrent uploading of illegal content. The bank was therefore entitled to terminate the contract due to the observed breaches.

This ruling illustrates the French courts' intention to hold technical intermediaries accountable in the fight against counterfeiting and intellectual property violations and highlights the need for digital platforms to adopt effective detection and removal systems to avoid contractual sanctions that could impact their activity.

PERSONAL DATA NEWS

EDPB Guidelines on pseudonymization and strengthening cooperation with competition authorities

EDPB, guidelines, 2025/01/17

In guidelines dated January 17, 2025, the EDPB clarifies the definition of pseudonymization and how it applies:

- On the one hand, pseudonymized data always remain information relating to an identifiable natural person. They still constitute personal data.
- On the other hand, pseudonymization can reduce risks and facilitate the use of legitimate interest as a legal basis (Article 6.1.f of the GDPR), provided that all other GDPR requirements are met.

These guidelines have been submitted for public consultation until February 28, 2025.

The EDPB also explains how data protection and competition law interact. It suggests steps to integrate market and competition factors into data protection practices and to ensure that data protection rules are taken into account in competition assessments. It provides recommendations to improve cooperation between regulators. Thus, authorities should consider creating a single point of contact to manage coordination with other regulators.

PERSONAL DATA NEWS

Publication by the CNIL of its strategic plan for 2025 / 2028

CNIL, strategic plan 2025-2028

For 2025/2028, the CNIL proposes a strategic plan with four main axes:

- Promoting ethical and rights-respecting artificial intelligence. The popularization of artificial intelligence goes hand in hand with an increase in potentially malicious or misleading content. In light of this, the CNIL will continue its work to clarify and enrich the legal framework on AI.
- Protecting minors and their data in the digital world. Digital technology and associated risks are omnipresent in the daily lives of minors. In response to these challenges, the CNIL will strengthen its dialogue with children, their surroundings, and the educational ecosystem to create a safer digital environment.
- Making everyone a cybersecurity actor to strengthen trust in digital technology. Recent years have seen a massive increase in cyberattacks involving a large part of the population across various sectors such as health and banking. To combat the risks of personal data theft, a major societal issue, the CNIL, in cooperation with the cybersecurity ecosystem such as ANSSI, will ensure that organizations take appropriate protective measures and raise awareness among individuals about these risks.
- Implementing targeted actions on everyday digital uses. The CNIL will focus on two major everyday digital uses for the French: mobile applications and the issue of digital identity. Regarding mobile applications, it will ensure the compliance of actors and raise awareness among users of its recommendations published in 2024. Regarding digital identity, it will oversee its development and deployment by various public and private actors, ensuring that it complies with regulations and respects individual rights and freedoms.

PERSONAL DATA NEWS

CNIL's assessment of its inspections as part of a coordinated European action

CNIL, assessment of inspections on the right of access

As part of a coordinated European action, the CNIL and several of its European counterparts evaluated the compliance and respect of companies and administrations with the right of access to personal data as provided by the GDPR.

It emerged that, for the most part, companies and administrations have implemented organizational measures to process right of access requests. However, the investigation revealed several shortcomings, including frequent delays in responding to access requests, with many organizations exceeding the one-month deadline imposed by the regulation. Some responses were also incomplete, insufficient, and unsatisfactory, not providing all the requested data.

To address these shortcomings, the CNIL recommends the implementation of more effective internal procedures, better training for the concerned teams, and increased transparency in the communication of information to citizens. The CNIL also reminds of the existence of the guidelines on the right of access adopted by the EDPB in 2023, often forgotten or unknown, although they contain valuable advice.

In case of persistent non-compliance, sanctions may be applied, as the CNIL has already issued several reminders of legal obligations.

Publication by the CNIL of its guide on data transfer impact assessments

CNIL guide to impact assessments for data transfers

At the end of January 2025, following a public consultation, the CNIL published a practical guide on data transfer impact assessments (AITD), aimed at helping organizations transferring data outside the European Economic Area (EEA) to evaluate and ensure a level of protection compliant with the GDPR.

Data transfers outside the European Union are regulated by the GDPR, which requires that these data benefit from a level of protection equivalent to that offered within the European Union. To ensure this level of protection, data controllers and processors must evaluate the legal framework and practices of the recipient country before carrying out the transfer. This analysis is essential to identify and mitigate the risks associated with these transfers, notably by implementing additional safeguards.

In line with the EDPB's recommendations on supplementary measures complementing transfer instruments, the CNIL's guide proposes a non-binding methodology, identifying the preliminary steps to conducting an AITD as well as the steps to follow for its implementation. These include understanding the transfer, identifying the transfer tool used, evaluating the legislation and practices of the destination country, adopting additional measures if necessary, implementing them, and regularly reassessing the level of protection.

PERSONAL DATA NEWS

Non-application of the exoneration clause in case of breach of the duty to inform and advise

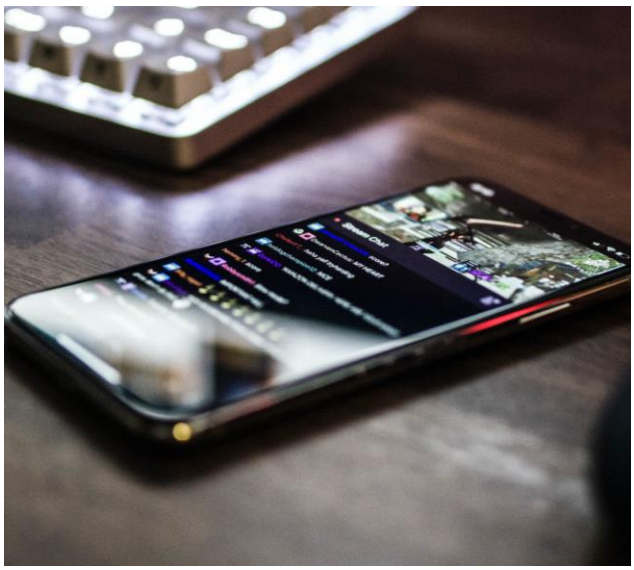
CA Paris, Pôle 5, chambre 11, 2025/01/10, RG No. 22/11677

On January 10, 2025, the Paris Court of Appeal rendered a decision on the application of limitation of liability clauses in the context of providing a software solution.

In 2016, the company Payplug committed to providing Wedoogift (now Glady) with a payment management interface including the "Smart 3-D secure" system, which calculates a real-time risk score associated with each payment to prevent fraudulent banking operations. In 2019, Wedoogift suffered a series of fraudulent operations and ceased working with Payplug. In 2020, Wedoogift sought compensation for the frauds and the release of sequestered funds. In 2022, the Paris Commercial Court ordered Payplug to pay damages to Wedoogift.

On appeal, Payplug invoked various arguments, including that it was not responsible for fraud, that it had fulfilled its duty to inform, and in any case, attempted to rely on the exoneration clause accepted by Wedoogift. Wedoogift, on the other hand, accused Payplug of breaching its duty to inform and advise, argued that the "Smart 3-D" system was not sufficiently secure, and sought compensation for the frauds suffered.

The Court of Appeal confirmed the first-instance judgment and rejected the application of the exoneration clause since Payplug's liability was engaged not for a simple technical failure but for breaching its duty to inform and advise. This behavior constituted a serious fault that falls outside the scope of the limitation clause, which cannot exonerate a service provider when it neglects an essential obligation of the contract. The Court of Appeal thus confirmed the amount of damages set by the Paris Commercial Court at 37,294.90 euros and ordered Payplug to pay costs and irrecoverable expenses amounting to 5,000 euros.



Adoption of the regulation on the European health data space

Regulation on the European Health Data Space

On January 21, 2025, the Council of the European Union adopted a regulation aimed at facilitating the exchange and access to health data within the EU.

This European Health Data Space (EHDS) is part of the "European data strategy" unveiled in 2020 and constitutes the first of nine European data spaces specific to certain sectors and domains defined by the Commission.

On the one hand, this regulation aims to improve individuals' access to their health data. Citizens will benefit from faster and easier access to their electronic health data, whether they are in their home country or another Member State. They will also have better control over the use of these data. EU countries will be required to establish a digital health authority responsible for implementing the new provisions.

On the other hand, this text aims to promote the reuse of data for research and innovation. The EHDS will offer researchers secure access to specific types of anonymized and secure health data, allowing them to exploit the potential of EU health data to inform scientific research, develop better treatments, and improve patient care.

The regulation also aims at the interoperability of electronic health record (EHR) systems by requiring all to comply with the specifications of the European EHR exchange format, while currently, the sharing of health data between Member States is delicate due to varying levels of digitization from one state to another.

The regulation will be formally signed by the Council and the European Parliament and will enter into force twenty days after its publication in the Official Journal of the European Union.

PERSONAL DATA NEWS

The EDPB expands its competences

CJEU, 2025/01/29, joined cases T-70/23, T-84/23, and T-111/23

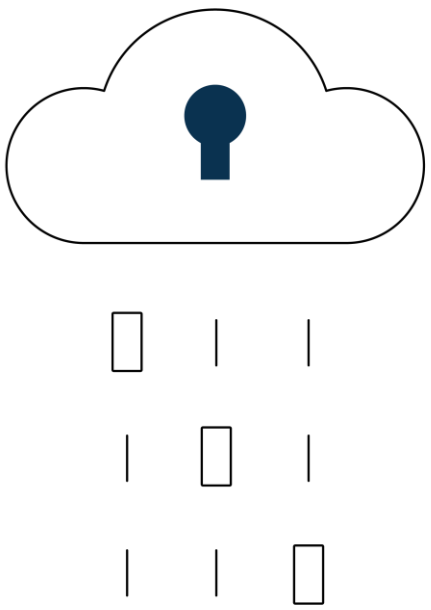
On January 29, 2025, the General Court of the European Union confirmed the competence of the European Data Protection Board (EDPB) to order a national supervisory authority to expand the scope of its investigation and make new decisions in cross-border cases.

In 2018, residents of Austria, Belgium, and Germany filed complaints against Meta, alleging violations of the General Data Protection Regulation (GDPR) in the Facebook, Instagram, and WhatsApp applications, particularly the misuse of personal data for targeted advertising without proper consent. Since Meta's European headquarters is in Ireland, the Irish Data Protection Commission (DPC) was tasked with investigating as the lead supervisory authority and submitted draft decisions to the other concerned supervisory authorities.

No consensus was reached regarding its draft decisions, so the DPC referred the matter to the EDPB under the consistency mechanism. After reviewing these three cases, the EDPB approved a number of objections it found relevant and well-founded but did not agree with the DPC's analysis that the use of data for targeted advertising was compliant with the GDPR based on the notion of "performance of a contract." The EDPB therefore issued three binding decisions requiring the DPC to remove findings related to this analysis from its final decisions and, more broadly, to expand its investigation and develop additional draft decisions.

Challenging this directive, the DPC brought the matter before the General Court of the European Union, arguing that the EDPB had exceeded its competences. In this decision, the General Court of the European Union affirmed that the EDPB had the power to require national authorities to expand their investigations and issue new decisions in accordance with EU law.

This decision strengthens the role of the EDPB in ensuring the consistent application of the GDPR across the European Union while respecting the operational autonomy of national authorities in conducting their investigations. It also highlights the importance of effective cooperation between data protection authorities to ensure uniform and effective application of the GDPR.



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

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 nine key sectors. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

dwfgroup.com