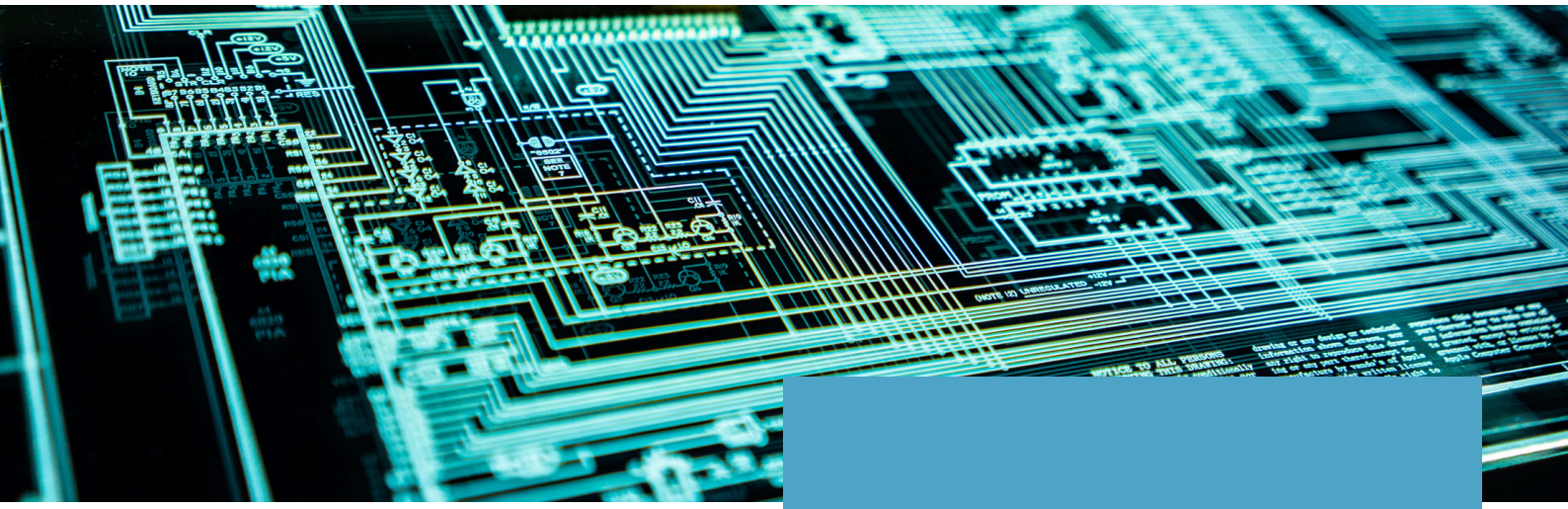
NEWSLETTER

TECH / DATA



IN THIS ISSUE

X is not a "gatekeeper"

After analysis, the European Commission has concluded that the social network X (formerly Twitter) does not meet DMA criteria to be designated as a "gatekeeper"

LATEST NEWS - TECHNOLOGIES

Abritel wins against the City of Paris

Paris Cours of appel, Pôle 1 - Ch. 3, 22 October 2024, Ville de Paris / Homeaway UK Limited & EG Vacation Rentals Ireland Limited

The Court of Appeal has ruled on the dispute between the City of Paris and Homeaway UK Limited and EG Vacation Rentals Ireland Limited, which operate the Abritel platform, accused of failing to transmit certain data on rentals of furnished holiday accommodation for 2018 and 2019, in breach of the French Tourism Code. The City of Paris, seeking a fine of €93.75 million, had its claims rejected at first instance, a decision it contested on appeal.

In this dispute, the City of Paris relied on several provisions of the French Tourism Code. According to article L. 324-2-1, any online intermediation platform must provide local authorities, at their request, with information on the number of days that furnished tourist accommodation has been rented through its intermediary. This obligation is part of a series of regulations designed to control short-term lets and prevent properties from being turned into exclusively tourist lets. Under articles R. 324-2 and R. 324-3, local authorities may require information to be sent once a year, with a one-month deadline for electronic transmission. The City of Paris criticised Homeaway UK Limited for failing to provide this information, which, in its view, constituted a breach of these regulatory and legislative provisions.

In its analysis, the Court first considered that the online matchmaking services provided by Homeaway come under the heading of "information society services" and are therefore covered by European Directive 2000/31/EC. According to this directive, online services are subject to the rules of the country in which the company is established, in this case the United Kingdom for Homeaway UK Limited before 2021, which means that the additional obligations imposed by the French Tourism Code cannot apply.

The Court then examined the possible derogations from the principle of free movement of services provided for in the Directive. It pointed out that the Member States may impose additional obligations on grounds of public policy or consumer protection, but that such measures must be proportionate, specific and targeted. The Court concluded that the aforementioned articles of the Tourism Code did not meet these criteria, being general and applying indiscriminately to all online rental platforms. These provisions were therefore inapplicable to the defendants.

In addition, the Directive requires any Member State notifying restrictive measures to inform the European Commission in advance, which France had not done in respect of these provisions of the Tourism Code. This procedural failure reinforced the Court's position that these obligations do not apply to businesses established in another EU Member State.

The Court also found that the French data transmission requirements imposed a significant administrative burden on the two companies, resulting in technical and organisational adaptations that were incompatible with the legal framework in Homeaway's country of origin. These additional constraints, which were not provided for in the country of establishment, contradicted the principle of freedom to provide services established by the Directive.

In conclusion, the Court of Appeal confirmed the decision of the court of first instance, rejecting the claims of the City of Paris on the grounds that the obligations of the Tourism Code were not enforceable against the defendant companies by virtue of the European Directive. It also ordered the City of Paris to pay costs and the sum of €20,000 to Homeaway UK Limited.

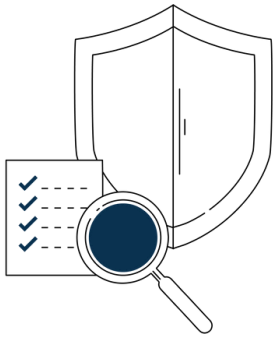
LATEST NEWS - TECHNOLOGIES

Bill on the resilience of critical infrastructures and the strengthening of cybersecurity submitted to the Senate

Bill on the resilience of critical infrastructures and the strengthening of cybersecurityei_prmd2412608l_cm_15.10.2024.pdf

On 15 October 2024, the Council of Ministers presented a bill on the resilience of critical infrastructures and the strengthening of cyber security, aimed at transposing three European directives to strengthen national security and the fight against cyber threats. The bill is accompanied by an impact assessment.

Directive - 2022/2557 - EN - EUR-Lex
Directive - 2022/2557 - EN - CER - EUR-Lex

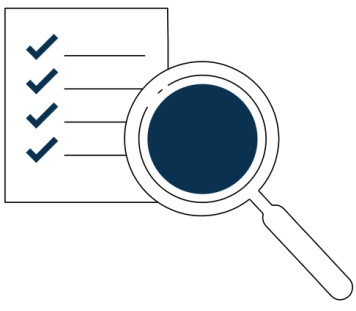


In particular, this text transposes Directive (EU) 2022/2557 on the resilience of critical entities, which requires Member States to guarantee a minimum level of protection for their critical infrastructures, covering sectors such as energy, health and digital infrastructures.

Directive - 2022/2555 - EN - EUR-Lex

The second directive to be transposed is Directive (EU) 2022/2555, known as NIS2. This extends cybersecurity obligations to entities classified as essential and important, in response to the increase in cyberattacks targeting SMEs, local authorities and hospitals. In France, this extended framework will cover some 15,000 entities in 18 sectors.

Regulation - 2022/2554 - EN - DORA - EUR-Lex
Directive - 2022/2556 - EN - EUR-Lex



Finally, the project includes the Digital Operational Resilience Act Regulation (DORA) and the associated Directive (EU) 2022/2556, which impose specific cybersecurity standards on financial entities, with application scheduled for January 2025. Together, these measures specify digital resilience and risk management obligations for the financial sector, ensuring harmonised cybersecurity rules across the EU.

LATEST NEWS - TECHNOLOGIES

Cyber resilience regulation: Council adopts new law on security requirements for digital products

Regulation on horizontal cyber security requirements for products with digital components (Cyber Resilience Regulation), 10 October 2024

On 10 October 2024, the Council of the EU adopted a new regulation on cybersecurity requirements for products with digital elements, such as cameras, fridges and connected toys, to ensure their security before they are placed on the market ("Cyber Resilience Regulation"). This regulation aims to fill gaps in the existing legislative framework by securing digital products throughout their lifecycle and across the supply chain. It introduces EU-wide cybersecurity standards for the design, development and market availability of hardware and software products, limiting the overlap of regulations in different Member States. Compliant products will bear the CE mark, indicating their conformity with safety, health and environmental requirements.

The regulation applies to products connected directly or indirectly to a network, with exceptions for those already subject to cybersecurity requirements (medical devices, aeronautics, automobiles). It also aims to inform consumers about the cybersecurity features of the products they buy.

The Cyber Resilience Regulation will enter into force 20 days after its publication in the Official Journal of the EU, with application expected within 36 months, with some provisions due to apply earlier.

The Commission concludes that X's online social network service should not be designated as a gatekeeper within the meaning of the Digital Markets Act (DMA).

On 16 October 2024, the Commission decided that X's online social networking service would not be designated as a "gatekeeper" within the meaning of the Digital Markets Act (DMA). This decision comes after an investigation launched on 13 May 2024, following X's statement refuting this 'gatekeeper' status. X had argued that the social network was not a key gateway between businesses and consumers, despite apparently meeting the quantitative thresholds stipulated by the DMA. X argued that its service does not play a central role in enabling business users to connect directly to end users, thus excluding it from "gatekeeper" status under the DMA.

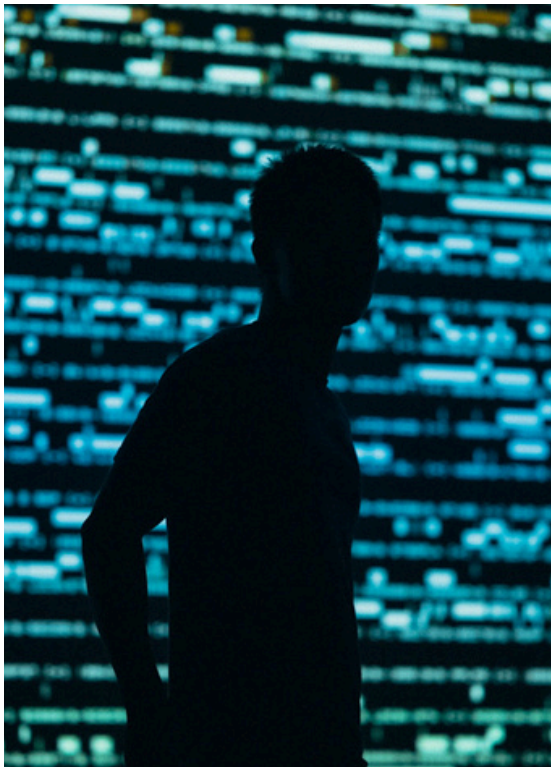
After examining the arguments and contributions of the stakeholders concerned and consulting **the Advisory Committee on Digital Markets**, the Commission concluded that the social network service provided by X did not fulfil the role of "gatekeeper", as X did not represent an important gateway enabling companies to reach end users directly.

The Commission will continue to monitor the market for this service for any significant changes. **The non-confidential version of the decision will be available on the website of the Commission's market regulator.**

PERSONAL DATA NEWS

1er European Commission report on the review of the functioning of the adequacy decision of the EU-US framework for the protection of personal data

eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0451

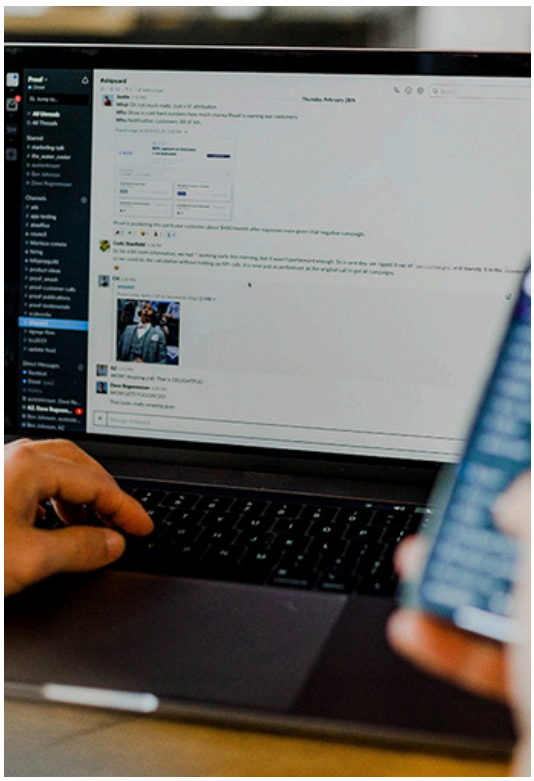


The European Commission published a report on 9 October 2024 stating that the EU-US Data Privacy Framework now guarantees that the data of Europeans is not misused when it is transferred to the United States. This framework was put in place in 2023 after the CJEU invalidated two previous data transfer agreements, known as the Privacy Shield and Safe Harbor.

The Commission considers that the US authorities have put in place the necessary structures and procedures to ensure that this framework functions properly, and in particular welcomes the establishment of a US supervisory authority. More than 2,800 US companies are currently certified under the agreement, enabling them to exchange data more easily and at lower cost, according to the report.

However, privacy defenders are still expressing fears that the framework still contains many loopholes.

CNIL: penalties of €250K and €150K imposed on two fortune-telling services for excessive retention of personal data and collection of sensitive data without consent



https://www.cnil.fr/fr/voyance-en-ligne-sanctions-de-250-000-et-150-000-euros-cosmospace-telemaque

On 26 September 2024, the CNIL imposed penalties on COSMOSPACE and TELEMAQUE, notably for keeping personal data in an excessive manner, collecting sensitive data without valid consent, and for failing to comply with the rules governing commercial canvassing operations.
As a result, the Restricted Section - the CNIL body responsible for imposing penalties - imposed a fine of 250,000 euros on COSMOSPACE and 150,000 euros on TELEMAQUE. These fines were adopted in cooperation with some fifteen of the CNIL's European counterparts in both cases.

The amount of these fines was decided on the basis of the seriousness of the breaches, the number of people concerned - the database shared by the two companies contains the data of more than 1.5 million people - and the sensitivity of the data processed. The financial situation and structure of the companies were also taken into account, in order to set dissuasive but proportionate fines.

PERSONAL DATA NEWS

EDPS: ePrivacy Directive guidelines

Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, EDPB

The emergence of new tracking methods aimed at replacing existing tracking tools (e.g. cookies, due to the cessation of support for third-party cookies by certain browser providers) and creating new business models has become a major issue for data protection.

On 16 October 2024, the European Data Protection Committee EDPS published Guidelines 2/2023 on the technical scope of Art. 5(3) of the ePrivacy Directive, clarifying what is covered by "storing or accessing information" in cases such as:

- URL and pixel tracking
- Local treatment
- IP-based tracking
- IoT Reports
- unique identifiers.

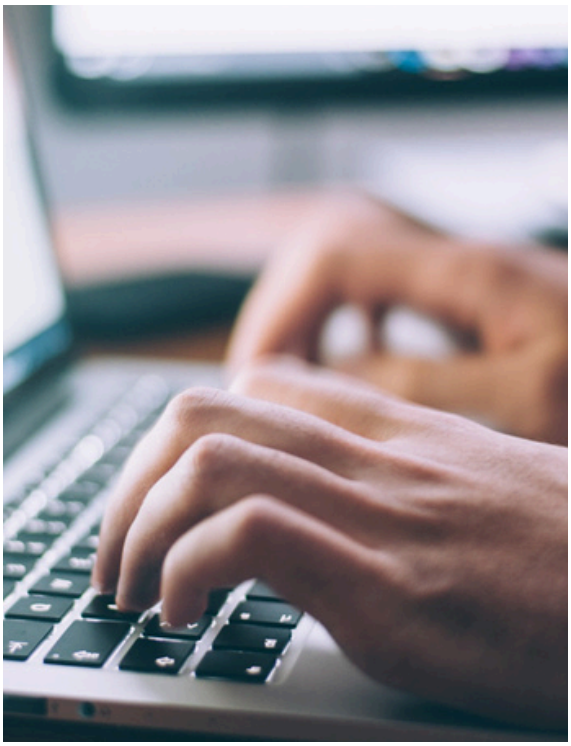
Although these transactions fall under Article 5(3), it is still unclear whether consent or exemption is required. The EDPB has not yet answered this question.

Publication by the EDPS of the 2025 themes

CEF 2025: EDPB selects topic for next year's Coordinated Action | European Data Protection Board

At its October 2024 plenary, GDPS the European Data Protection Committee (EDPS) chose the theme of its fourth coordinated enforcement action (CEA), which will focus on the implementation of the right to be forgotten by data controllers. Data Protection Authorities (DPAs) will join this action on a voluntary basis in the coming weeks and the action itself will be launched in the first half of 2025.

The right to be forgotten (Article 17 of the RGPD) is one of the most frequently exercised data protection rights and one about which data protection authorities often receive complaints. One of the aims of this coordinated action will be to assess the implementation of this right in practice.



PERSONAL DATA NEWS

EDPS adopts opinion on subcontractors

Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s) | European Data Protection Board

The EDPS has adopted an opinion on certain obligations arising from the use of processor(s) and sub-processor(s). It concerns situations in which data controllers rely on one or more processors and sub-processors. In particular, it addresses issues relating to the interpretation of certain obligations of controllers relying on sub-processors and sub-sub-processors, as well as the content of contracts between controllers and sub-processors, as set out in Article 28 of the ODPR.

The Opinion explains that controllers should have information at all times about the identity (i.e. name, address, contact person) of all sub-processors, subsequent sub-sub-processors, etc., in order to best fulfil their obligations under Article 28 of the GDPR. In addition, the controller's obligation to verify whether sub-processors provide "sufficient guarantees" should apply regardless of the risk to the rights and freedoms of data subjects, although the extent of this verification may vary, in particular depending on the risks associated with the processing. Furthermore, while the original processor must ensure that it itself proposes processors with sufficient guarantees, the final decision and responsibility for engaging a specific processor remains with the controller.

The EDPS considers that under the GDPR, the controller is not obliged to systematically require subcontracting contracts to provide for data protection obligations to be transmitted throughout the processing chain. However, it is up to the controller to assess whether it is necessary to request a copy of these contracts or to examine them in order to demonstrate compliance with the GDPR.

In addition, where transfers of personal data outside the European Economic Area take place between two (sub)processors, the processor as exporter of the data should prepare the relevant documentation, in particular as regards the reason for the transfer used, the impact assessment of the transfer and any additional measures. However, as the controller is still required to provide "sufficient guarantees", it should assess this documentation and be able to present it to the competent data protection authority.

PERSONAL DATA NEWS

EDPS adopts guidelines on legitimate interest

Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Data controllers need a legal basis to legally process personal data. Legitimate interest is one of the six possible legal bases.

The EDPS Guidelines analyse the criteria set out in Article 6(1)(f) of the GDPR that data controllers must meet in order to lawfully process personal data on the basis of a legitimate interest. It also takes into account the recent judgment of the Court of Justice of the European Union on this issue (C-621/22, 4 October 2024).
To be able to invoke a legitimate interest, the data controller must meet three cumulative conditions:

1. the pursuit of a legitimate interest by the controller or a third party;
2. the need to process personal data in order to pursue the legitimate interest;
3. The interests or fundamental rights and freedoms of individuals do not take precedence over the legitimate interests of the controller or a third party (balancing exercise).

Firstly, only interests that are lawful, clearly and precisely articulated, real and present can be considered legitimate. For example, such legitimate interests could exist in a situation where the person is a customer or in the service of the data controller.

Secondly, if there are reasonable, equally effective, but less intrusive alternatives for achieving the interests pursued, the processing may not be considered necessary. The necessity of processing should also be examined in the context of the data minimisation principle.

Thirdly, the data controller must ensure that its legitimate interests do not override individual interests, fundamental rights and freedoms. In this balancing exercise, the controller must take into account the interests of individuals, the impact of the processing and their reasonable expectations, as well as the existence of additional safeguards that could limit the impact on the individual.

In addition, these guidelines explain how this assessment should be carried out in practice, including in a number of specific contexts such as fraud prevention, direct marketing and information security. The document also explains the relationship between this legal basis and a number of data subjects' rights under the GDPR.

CNIL publishes list of entities audited in 2023

Checks carried out by the CNIL - data.gouv.fr

CONTACTS

Stéphanie BERLAND
Partner
s.berland@dwf.law
+33 1 40 69 26 63

Emmanuel DURAND
Partner
e.durand@dwf.law
+33 1 40 69 26 83

Florence KARILA
Partner
f.karila@dwf.law
+33 1 40 69 26 57

Anne-Sylvie VASSENAIX-PAXTON
Partner
as.vassenaix-paxton@dwf.law
+33 1 40 69 26 51

DWF is a global provider of integrated legal and business services. The firm employs around 4,500 people and operates in 35 cities worldwide. DWF recorded net sales of £435 million in the year ended April 30, 2024. For more information: dwfgroup.com