AI & Digital Verdict

Case law on AI, digital and data regulations

February 2025

AI & Digital Verdict

AI, digital regulations, and data compliance are rewriting the rules of business across sectors and industries. Are you keeping up?

Presenting the 2024 year in review of the AI & Digital Verdict – your go-to source for the most impactful cases in AI and digital laws from the past year. Packed with expert legal insights, it helps you navigate this dynamic regulatory environment with confidence.

Starting in 2025, we're shifting to a **quarterly format**, providing regular case law insights and expert analysis to keep you ahead of emerging trends. Curated by CMS experts across all CMS RRH jurisdictions, with insights from key UK and US cases, this publication empowers businesses across sectors with clear, actionable takeaways. Stay informed. Stay prepared!

What you'll find inside:

- **Jurisdiction (court/regulator/authority)** – Where the decision was made
- **Key issues** – What was at stake?
- **Outcome** – The decision and its immediate impact
- **Significance** – Why this matters for businesses and compliance
- **AI, digital & data compliance aspect** – Practical implications for your business
- **CMS commentary** – Our legal and business perspective on the ruling and what it means for you

Why read it?

Regulators and courts are setting **new standards for AI accountability, digital compliance, and data governance.** The **AI & Digital Verdict** doesn't just report on cases - it **deciphers trends, highlights regulatory blind spots, and equips you with the foresight to stay compliant and competitive.**

We do this for you.

Whether you're a legal expert, a compliance professional, or a business professional working with AI, digital services, or data-driven strategies, the **AI & Digital Verdict** is designed to help you stay ahead of evolving legal risks.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Austria Federal Administrative Court Austria (BVwG) XXXX vs. Data Protection Authority (W214 2259197-1/14E)	Obligation to provide information on the processing of personal data by a camera installed in a vehicle.	The complaint was upheld and the opposing party violated its information obligation under Article 13 of the GDPR.	Emphasizes the importance of transparency in the processing of personal data by a vehicle.	Violation of the information obligations pursuant to Article 13 GDPR.	The decision provides clarity regarding the information obligations associated with using vehicle cameras for surveillance purposes. "Guard Mode" is a feature designed to protect the vehicle from potential break-ins or theft. When activated, the vehicle's cameras and sensors remain operational, ready to detect and record suspicious activity around the vehicle while it is parked and locked. In this case, the vehicle owners activated Guard Mode, thereby assuming the role of a data controller. As such, they are responsible for ensuring that data subjects are adequately informed about the processing of their personal data.
Austria Supreme Administrative Court (VwGH) Data Protection Authority and G W in D vs. Federal Administrative Court (Ro 2021/04/0008)	Right of access in relation to automated decisions and profiling based on a credit reporting.	The Austrian Federal Administrative Court's decision, which excluded certain profiling-based creditworthiness evaluations from being classified as "automated decisions" under Article 22 (1) GDPR, was overturned due to misinterpretation of GDPR provisions.	Clarification of access obligations; The creation of probability scores based on automated profiling, if they significantly influence subsequent decisions by third parties, qualifies as "automated decisions" under GDPR. This holds even if the profiling entity itself does not directly make the final decision. The probability value determined when granting a loan is thus to be classified as an automated decision within the meaning of Article 22 (1) GDPR and is therefore subject to the right of access.	Analysis of access rights and the conditions governing automated decisions and profiling under Articles 15 and 22 of the GDPR.	Companies engaging in profiling must recognize such activities as automated decisions under GDPR if the results substantially affect individuals. This triggers specific rights under Articles 15 (1) (h) and 22 GDPR, including the right to meaningful information about the logic involved, as well as safeguards ensuring fairness and transparency in the decision-making process. Companies must ensure that they can provide comprehensive access about the logic, scope and effects of their automated decisions and profiling procedures.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Austria Data Protection Authority (DSB) Dieter A *** vs. the Austrian Court of Audit (2024-0.199.724)	Right to secrecy in the context of publication of personal data on a website.	The complaint was dismissed as unfounded. The Austrian Data Protection Authority ruled that the publication of personal data (name, amount, and recipient of a political donation) on the website of the Austrian Court of Audit did not violate the right to secrecy under Article 9 GDPR.	Although the publication of the judgement constitutes a serious intrusion of the complainant's fundamental right to secrecy, it is justified in view of the considerable public interest in transparent party funding.	The interplay between Article 9(2)(g) GDPR, Section 1 Austrian Data Protection Act (DSG), and Section 6 Austrian Political Parties Act (PartG) highlighting the balance between protecting sensitive personal data and ensuring transparency in public interests like political party financing.	This case illustrates the balance between data protection rights and the public interest in transparency. While Article 9 of the GDPR prohibits the processing of sensitive data, such as political opinions, exceptions under Article 9(2)(g) GDPR apply when processing is necessary for substantial public interests and supported by appropriate legal measures. The ruling emphasizes that national legislation mandating transparency must comply with GDPR principles, including proportionality and the implementation of specific safeguards to protect individuals' rights.
Austria Supreme Administrative Court (VwGH) F. W. vs. Data Protection Authority (Ro 2022/04/0031)	Right to secrecy in the context of publishing a teacher's personal data on the school's website.	The appeal was dismissed as unfounded. The publication is lawful as it facilitates communication between the school and the parents/guardians. The right to secrecy was not violated.	Emphasizes the necessity and proportionality of the publication of personal data in the public interest.	Assessment of the necessity and proportionality of data processing in accordance with Article 6 (1) (e) GDPR and Article 5 (1) (c) GDPR.	The authority's ruling emphasizes that processing personal data, such as publishing professional email addresses, can be justified under Article 6(1)(e) GDPR when it serves a task in the public interest. For schools, this includes facilitating direct communication between teachers, students, and parents to improve school operations and educational outcomes. The school was not held accountable for data protection violations, as publishing the official email address was deemed proportionate and aligned with the teacher's professional role. This decision may also apply to other public institutions and, by analogy, to private companies if a legitimate public interest justifies the proportionality of such publication.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Austria Data Protection Authority (DSB) City of N*** vs. Data Protection Authority (2024-0.044.042)	Consultation in accordance with the GDPR on the processing of panoramic images of the road network.	The request for prior consultation was rejected as the formal requirements were not met.	Clarifies that prior consultation under Article 36 GDPR is only mandatory when a high residual risk remains after implementing mitigation measures. It reinforces the need for clear accountability delineation between controllers and processors, and emphasizes that the responsibility to evaluate and mitigate risks lies primarily with the data controller.	Assessment of the formal requirements to conduct a prior consultation under Article 36 GDPR.	Institutions must carry out thorough Data Protection Impact Assessments (DPIAs) and ensure effective risk mitigation to avoid unnecessary reliance on prior consultation. The Data protection authority only conducts a consultation if significant risks remain after mitigation. High risk can be often assumed when new technologies, automated processing (including profiling), or extensive monitoring of public areas are involved. Risks under Article 36 GDPR include not just technical issues but any potential negative impacts on data subjects. This case highlights the importance of clear contracts and well-defined responsibilities in data processing arrangements.
Austria Federal Administrative Court (BVwG) XXXX vs. Data Protection Authority (W 2872251990)	Violation of the right to secrecy by forwarding e-mail correspondance containing personal data to a home care company.	The Austrian Federal Administrative Court upheld a decision from the Data Protection Authority, ruling that a property management company violated data protection law by forwarding an owner's complaint email (including their name, email address, and content) to a third party without legal basis. The court found that the disclosure of personal data was unnecessary for resolving the complaint, and neither contractual obligations nor legitimate interests under GDPR Article 6(1)(b) or (f) justified the data processing.	This case underscores that the principle of data minimization and necessity are key under the GDPR. Personal data should only be processed if strictly required to achieve the intended purpose. Furthermore, vague "data protection clauses" in agreements do not fulfill the requirements for valid consent under Article 7 GDPR, especially if they violate the prohibition of tying consent to contract performance.	Violation of Article 6 and Article 5 GDPR.	Organizations must assess whether data disclosure is essential to achieve legitimate purposes and ensure that any data sharing complies with GDPR principles. They should also ensure that consent clauses meet GDPR requirements and cannot rely on such clauses as a blanket justification for data processing.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Austria Austrian Supreme Court (OGH) Ing. J* vs. City of Vienna (6 Ob 233/23t)	Right of access to personal data under the GDPR and clarification of the proportionality of the obligation to reimburse costs based on the disclosure of a patient's medical history.	The Austrian Supreme Court (OGH) ruled that the plaintiff, a patient, is entitled to receive a free first copy of their medical records without payment of a fee. The court rejected the hospital operator's reliance on an exception to the GDPR's right to a free first copy of personal data, finding that the financial burden of providing such copies does not meet the threshold of an overriding public interest.	This decision reinforces the GDPR's principle that individuals have a fundamental right to access their personal data, including medical records, free of charge for the first copy. It underscores that exceptions to this right, such as financial or public health considerations, must be interpreted narrowly and supported by substantial evidence. The right to a free first copy of the medical history must not be restricted by national regulations.	Assessment of the obligation to provide access in accordance with Article 15 (3) of the GDPR and the restrictions in accordance with Article 23 of the GDPR.	This case highlights the balancing act between the administrative costs incurred by public institutions and the fundamental rights of individuals under GDPR. By prioritizing patients' rights to data access, the court ensures that financial barriers do not undermine transparency or accountability in public healthcare. Hospitals and other data controllers must ensure that they comply with the legal requirements for the provision of free copies of data.
Austria Federal Administrative Court(BVwG) XXXX vs. Data Protection Authority (W108 2285546-1)	The central issue revolved around whether the improper handling of sensitive data (open email distribution containing politically affiliated recipients) constituted a breach of GDPR, and how the liability and proportionality of the fine should be determined under Article 83(1).	The Austrian Federal Administrative Court reduced a GDPR fine to €28,000 from a significantly higher initial amount, citing mitigating factors such as the partial inclusion of sensitive data (Article 9 GDPR) and unintentional violation through negligence. The fine was recalibrated to align with the principle of proportionality under Article 83 GDPR, while still emphasizing the seriousness of the breach and its potential impact on affected individuals' fundamental rights.	The decision reinforces the importance of proportionality and contextual assessment in GDPR enforcement, particularly regarding fines. It also demonstrates the nuanced application of GDPR principles, such as data minimization (Article 5(1)(c)) and safeguards for sensitive data (Article 9). The court's reliance on EDPB guidelines for fine calculation underscores their practical relevance in aligning administrative decisions with EU-wide standards.	Violation of Articles 5, 6 and 9 GDPR.	The case underscores the heightened responsibility for processing sensitive data under GDPR, particularly regarding political opinions. It highlights the necessity for robust technical and organizational measures to prevent breaches and the careful balancing of fines to ensure deterrence without being disproportionate. Companies and organizations should ensure that their data processing processes are GDPR-compliant, especially when using email distribution lists.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Austria Federal Administrative Court (BVwG) XXXX vs. Data Protection Authority (W137 2241630-1)	The key issue revolves around whether the subsidiary and parent company constituted an "economic unit", which determines the shared liability for GDPR breaches.	The BVwG reduced the fine to €50,000 (0.03% of the relevant turnover), significantly lower than the original €4 million. The court justified this by applying GDPR principles of proportionality, effectiveness, and deterrence (Article 83(1) GDPR).	The decision underscores the strict criteria for establishing an "economic unit" under GDPR and EU competition law. It affirms the practical relevance of EDPB Guidelines in fine calculations, even though they are not legally binding. The ruling also highlights the importance of proportional fines and robust data protection measures to avoid severe penalties.	Assessment of the technical and organisational measures referred to in Article 5(1)(f) GDPR in relation to a breach and the resulting liability of an independent subsidiary referred to in Article 83(4)(a) GDPR.	The court's rejection of the economic unit concept in this case - due to the subsidiary's operational independence - clarifies the boundaries of liability and emphasizes that parent companies are not automatically liable for subsidiaries' actions unless clear evidence of control over market behavior exists.
Austria Data Protection Authority (DSB) ORF vs. Data Protection Authority (2024-0.633.166 v) (not final)	Design of the Cookie Banner.	The Data Protection Authority decided that the Austrian Broadcasting Corporation (ORF) must adjust the cookie banner on its website, www.orf.at, within six weeks to obtain valid consent. Users must have an equivalent choice on the first layer between "Accept all cookies" and "Only necessary cookies". Both options must be designed equally in terms of visual presentation, including color, size, contrast, placement, and emphasis. It is prohibited to highlight one option through overly prominent design features such as preferred coloring, larger font size, or more prominent placement. The aim is to ensure a fair and unbiased choice. Accessibility is implicitly required to enable all users to make independent decisions.	By mandating equal visual presentation and accessibility of cookie banner options, this decision sets a clear standard for organizations to avoid coercive design practices ("dark patterns") and ensures that users can make truly informed and voluntary choices. It highlights the necessity of fair, transparent, and accessible data processing practices not only for websites but also for mobile applications. Furthermore, it underscores the growing importance of compliance with both GDPR principles and accessibility standards.	Design of a cookie banner in line with Article 165 (3) Telecommunications Act 2021 and Art 7 GDPR.	According to this (not final) decision of the Data Protection Authority a company's website must also design its cookie banner to meet legal requirements, including neutral, accessible design and ensuring uninfluenced consent. These requirements apply not only to websites but also to mobile applications (apps) that process user data. This decision could serve as a precedent for stricter scrutiny of consent mechanisms across the EU (As the decision is not yet legally binding, the final determination of the Austrian standard for cookie banner design and consent mechanisms under GDPR will depend on the outcome of further proceedings, potentially up to the Austrian Supreme Administrative Court).

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Germany Regional Court of Kiel LG Kiel 6 O 151/23.	Right to an injunction against portal operators regarding incorrect AI-generated content.	The claim for injunctive relief was granted.	Establishes that incorrect AI-generated information is attributable to the portal operator, who uses inadequately programmed AI, even if the operator has no positive knowledge of the inaccuracy.	AI-generated content.	The defendant operates a portal, that focuses on publishing business information about German companies using AI. The information published about the plaintiff was incorrect. The defendant was not aware of the inaccuracy of the information published about the plaintiff, since the incorrect content was AI-generated. The main conclusion of this decision is that the defendant is nonetheless to be regarded as the direct interferer against whom the claim for injunctive relief exists, because the defendant deliberately used AI, which in this case was inadequately programmed.
Austria Supreme Court Jö Bonus Club, OGH 4 Ob 102/23p.	Review of contractual clauses concerning personal data use.	The clause was deemed unlawful.	Establishes that personal data is recognized as consideration for services.	Personal data as consideration.	The provision of personal data, in particular contact and purchasing behavior data by the consumer, constitutes a 'consideration' for the use of the bonus club of a retail chain. The arbitrary withholding of consideration from consumers – namely the advantages and services of the bonus club – constitutes such a gross imbalance between the consumer's data transfer on the one hand and the bonus club's promised consideration on the other hand that it must be considered immoral and therefore null and void.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Germany Supreme Court BGH VI ZR 370/22.	Request for information on contact details of the data protection officer.	The request was rejected.	Establishes that it is not mandatory to state the name of the data protection officer.	Information to be provided where personal data are collected from the data subject under Article 13 GDPR.	When providing the contact details of the data protection officer in accordance with Article 13 (1) (b) of the GDPR, it is not mandatory to state the name. The decisive factor and at the same time sufficient for the data subject is the communication of the information necessary to contact the competent body. If accessibility is guaranteed without stating the name, the name does not have to be provided.
Austria Data Protection Authority, DSB 159.938/2023	Video surveillance in a residential complex.	The surveillance was declared partially permissible and partially impermissible.	The decision defines the parts of the residential complex in which video surveillance is permissible.	Interpretation of Articles 5 and 6 of the GDPR.	In an apartment building with an electronic access system, comprehensive video surveillance of the entrance, lift, stairway and corridor areas represents a disproportionate infringement of the fundamental right to privacy of the residents and their visitors and is therefore not permissible. Video surveillance of refuse rooms, bicycle and pushchair storage rooms and the garage entrance area is permissible in the absence of less intrusive means.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Croatia Data Protection Agency (AZOP) Data Protection Agency v. Company	Failure to provide data subjects the option to give and/or withdraw voluntary and informed consent for cookie-based dana processing for not-essential purposes (e.g., for statistics and marketing, unrelated to the essential functioning of the webpage).	Administrative monetary fine to the data controller in the amount of EUR 20,000.00.	Underscores the necessity of informed and granular consent (i.e. cookie banner) for each data processing purpose.	Violation of GDPR Article 6(1), Article 7 and Article 5(1)(a).	The case exposes legal pitfalls of using deceptive cookie banner practices, such as pre-loading cookies without prior consent or combining multiple purposes (e.g., marketing and statistics) under a single cookie banner consent option. Such practices erode user trust, undermine the validity of consent and violate GDPR rules and principle of transparent processing. Business must prioritize user autonomy and transparency in data processing by implementing granular consent mechanisms that allow users to make distinct choices for each processing purpose.
Croatia Data Protection Agency (AZOP) Data Protection Agency v. Hotels	Unlawful processing of personal data through the use of cookies.	Administrative monetary fine to two hotels in the total amount of EUR 45,000.00.	[TBD once the Croatian DPA's decision is published.]	[TBD once the Croatian DPA's decision is published.]	The yet-to-be-published decisions by the Croatian DPA underscore a crucial point: the importance of lawful data processing via cookies. These fines clearly highlight the Croatian DPA's focus on cookie policies, reinforcing the need for businesses to prioritize compliance in this area.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Croatia Data Protection Agency (AZOP) Data Protection Agency v. Hospital	The hospital failed to implement appropriate technical measures to safeguard its radiological information system, resulting in the irreversible loss of radiological image files. Additionally, the hospital did not report the incident within the mandated 72-hour period after becoming aware of the breach. Furthermore, the hospital failed to enter a data processing agreement with the service provider responsible for the system's implementation and maintenance.	Administrative monetary fine to the hospital in the amount of EUR 190,000.00.	Highlights the importance of implementing appropriate technical measures, such as back-up systems, to prevent the loss of personal data. It also emphasizes the necessity of concluding DPAs and taking corrective actions and reporting breaches within the required timeframe.	Violation of GDPR Article 32 (1)(b); Article 33(1) and Article 28(3).	This case underscores the legal consequences of failing to implement adequate data protection technical measures, such as backup systems. It also emphasizes the importance of promptly and diligently reporting data breaches within the required timeframe. Businesses shall prioritize data security, as the costs of implementation of technical measures are far outweighed by the legal and reputational risks of non-compliance. Ensuring the continuous availability of technical safeguards and clearly defining the obligations of all data subjects through data processing agreements (DPA) is essential to mitigate financial and legal risks.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Türkiye Law proposal submitted to the Grand National Assembly of Türkiye Artificial Intelligence Law Proposal dated 25 June 2024	The proposal is in line with the Medium-Term Programme and the National Action Plan, which include targets for digital transformation and promoting the use of artificial intelligence.	The proposal contains parallel provisions to the EU Artificial Intelligence Law, which has had worldwide impacts.	It is the 1st legislative work on AI.	The proposal imposes various obligations on those who use systems containing artificial intelligence.	The proposal aims to ensure that artificial intelligence is used fairly and safely. Providers, sellers, users, importers, distributors, etc. of systems using this technology are covered by the proposal. There is no classification in the bill, as there is in the EU, only that special measures should be taken for high-risk artificial intelligence systems and that risk assessments are regulated. The aim is to bring benefits to society and to minimise the potential for harm.
Türkiye Personal Data Protection Authority / Regulation Publication On 10 July 2024, the Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad was published.	Within the scope of the Regulation, appropriate safeguards necessary for the transfer of data abroad have been determined, and standard contract models have been developed in this scope.	Standard Contracts, Standard Contract Notification Module.	It is aimed to ensure convenience in reporting data transfer abroad, to establish a certain standard, and to guide the harmonisation processes.	Standard contracts under this Regulation require robust legal, technical and organisational measures, particularly for AI and digital businesses, to ensure that data transfers comply with the PDPL and are in line with international data protection standards.	Standard contracts are intended to be one of the appropriate safeguards for data transfers abroad and to establish a certain standard in this respect. In addition, a notification module has been set up on the authority's website to facilitate notifications concerning the execution of such standard contracts. Moreover, the new data protection rules apply to the transfer of personal data abroad by multinational companies operating in countries that do not provide adequate protection and ensure that adequate protection is provided in writing.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Bulgaria Regional Court – Pazardzhik Decision No. 1667/30.12.2024 on case No. 1700/2024	Establishment/justification of the conclusion of distance loan agreement, proper use of electronic documents.	The court found that the distance loan agreement was duly executed and valid.	Confirms which are the circumstances to be proven by the supplier in connection with the conclusion of the distance credit agreement, including obligations to provide information to the consumer and that it has obtained the consumer's consent to the conclusion of the agreement.	The Electronic Document and Electronic Certification Services Act - shall apply to proof of pre-contractual information as well as to other statements. Pre-contractual information as well as statements made by telephone, other means of voice communication at a distance, video or e-mail shall be recorded with the consent of the other party and shall have evidentiary value for establishing the circumstances contained therein.	Suppliers of distance financial services (banks, other financial institutions) should be aware of the legal requirements for providing such services and to ensure that all actions during the electronic process are duly executed and can be verified/proved in a potential legal dispute.
Bulgaria Bulgaria Supreme Administrative court Decision No. 12730/25.11.2024 on case No.7135/2024	Inaction and noncompliance of the obligation to ensure and to take appropriate technical measures for processing personal data by the National Revenue Agency.	National Revenue Agency was sued to pay compensation for non-pecuniary damages to a person due to inaction of the authority.	The data processor is liable for damages caused to persons due to inaction to take organisational and technical measures in its processing activities that are appropriate in view of the nature, scope, context and purposes of the processing, as well as the existing risks to the rights of the natural persons concerned.	Noncompliance with the data processing obligations to take adequate measures.	The National Revenue Agency was object of a cyber attack in 2019 following which the data of millions of people were revealed/became public. The court decided that even in case of unauthorized access to the personal data by the cyber attack, the agency was obliged but did not take enough measures to secure the processed data of its customers.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Slovenia Administrative Court of Slovenia Judgment No. II U 197/2023-20 (dated October 14, 2024)	Systematic, automated, and continuous GPS tracking of company vehicles constitutes personal data processing of employees who operate such vehicles.	The court upheld the Information Commissioner's practice, emphasizing that GPS tracking requires a valid legal basis, such as legitimate interest under GDPR Article 6(1)(f).	Reaffirmed the necessity of conducting a proportionality test for GPS tracking to ensure compliance with GDPR, balancing employer interests and employee rights.	Legal basis for GPS tracking must adhere to proportionality principles, transparency, data minimization, and other GDPR safeguards, including employee rights and data security.	The ruling emphasizes the importance of assessing proportionality before implementing GPS tracking. Employers should develop clear internal policies, provide transparency to employees, and document compliance efforts to avoid GDPR violations and potential penalties.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Serbia Higher Court in Vranje undisclosed	Lawfully processing personal data by notifying the individual of potential debt collection without explicit consent, in line with data protection laws.	A public utility company that lawfully processed the personal data of a natural person to whom the data relates did not violate his or her right to privacy when it informed him or her (by means of a warning) that the data would be transferred to a debt collection agency for the same purpose for which it was collected - to collect the debt.	Explores the relationship between the interests of the public authorities and individual privacy laws.	GDPR	This case examined whether the data protection laws were violated by the public authority in Serbia, by processing sensitive personal data without explicit consent, bringing the question of balance between the public interest and privacy rights, which underlines the need for clearer legal frameworks regarding the transparency in data processing by public authorities.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Montenegro Administrative Court of Montenegro Multiple decisions regarding the same subject	Failure of the Public authority to act upon the request for access to information and the appeal of the Claimant.	All claims were dismissed due to procedural reasons.	Highlighting the importance of compliance with legal standards.	Freedom of information; digital.	All claims were filed against the same administrative body for failing to decide on appeals related to requests for access to information. However, all claims were dismissed because the claimant failed to provide proof that the appeals were properly submitted and received. Specifically, the appeals were submitted via email without obtaining a confirmation of receipt, as required by law. This underscores the importance of transparency and accountability on the part of public authorities, as well as the responsibility of individuals seeking information to ensure the proper submission of their requests to effectively protect their rights.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Ukraine Ukraine Supreme Court Anonymized individual v. Financial Institution	Features of entering into a loan agreement electronically.	Claim to recognize invalid the loan agreement entered into electronically denied.	The decision reinforces the growing importance and legal recognition of electronic agreements in modern commerce.	Compliance with the Law of Ukraine "On Electronic Commerce", especially regarding electronic signatures and secure systems.	This ruling highlights the need for organizations to integrate digital compliance measures across operational and legal frameworks. IT departments should focus on implementing secure and reliable information systems to support electronic transactions, while legal teams ensure contract terms and digital signature practices are aligned with regulatory requirements.
Ukraine Kyiv District Administrative Court Gambling Company v. State Tax Service	Whether a gambling electronic money substitute (EMS) is a product; whether transactions involving EMS constitute purchase-sale operations.	The court ruled that EMS used by players to participate in online gambling are not products under national legislation.	This decision underlines the evolving challenges of regulating digital transactions and virtual assets, particularly in the online gambling industry.	It highlights the importance of clear legislative frameworks for defining digital assets and their compliance requirements as well as lack of said regulation in Ukraine.	The case emphasizes the need for businesses operating in digital ecosystems, especially those handling payments or virtual assets, to align IT and legal processes with regulatory demands. Organizations must also ensure their contractual arrangements with third-party service providers, such as payment intermediaries, address compliance requirements.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
Slovakia Supreme Court of the Slovak Republic 4Cdo/18/2024	An individual discovered an archive box containing 483 original documents with sensitive personal data of customers from a major provider in an unsecured wastepaper storage area behind the company's store.	The Supreme Court set aside the judgment of the Regional Court and remanded the case to it for further proceedings.	The case is one of the few decided in the past year that involves data protection aspects. Additionally, it concerns a large amount of personal data from original documents executed with customers and left unattended behind the store.	The documents contained highly sensitive information, including names, addresses, birth registration numbers, ID numbers, phone numbers, SIM card details, and personal signatures.	Ensuring that companies and their subcontractors handle personal data responsibly is crucial. It is also important to eliminate similar risks of unauthorized access to sensitive information and to prevent the improper disposal of hard copy documents containing personal data.
Slovakia Supreme Court of the Slovak Republic 9Cdo/88/2023	At the heart of the dispute between the customer and a major bank in Slovakia is the customer's agreement that all calls to the company's call center can be recorded, stored for 10 years and used as evidence in court or arbitration if necessary.	The Supreme Court dismissed the extraordinary appeal, thereby upholding the decision of the Regional Court. At the instance of the appellate court, it was decided that the clause in the contract stating, 'the client agrees that all their calls with the company's call center can be recorded, stored for 10 years, and used as evidence in court or arbitration if needed,' is unfair contractual term.	Although the case concerns unfair terms, it is also relevant in relation to the storage of personal biometric data in the context of the unfair term.	The relevance of the case lies in the use of biometric data without the explicit consent of the individual and without clear and demonstrable information being provided to the consumer about the use of their biometric data, combined with the storage of the data for 10 years.	The key takeaway from this case is that contractual clauses requiring clients to consent to the recording and storage of their calls for extended periods solely for the benefit of the company in potential legal disputes can be deemed unfair and unacceptable. This decision underscores the importance of ensuring that contractual terms respect consumer rights, provide transparency, and comply with legal standards, particularly regarding the handling of sensitive data. It also highlights that consumer consent must be informed, voluntary, and not imposed through imbalanced or one-sided agreements.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
UK UK Supreme Court Thaler v. Comptroller-General of Patents (DABUS AI Case)	The case centered on whether an AI system, such as DABUS, could be recognized as an inventor on a patent application under the UK Patents Act 1977. It raised questions about the interpretation of the term "inventor" and whether existing laws could accommodate AI-generated innovations.	The UK Supreme Court ruled that under the Patents Act 1977, only a natural person can be named as an inventor. AI systems, like DABUS, cannot hold such status.	This landmark decision shapes the legal recognition of AI in intellectual property law, highlighting the limitations of current IP frameworks in accommodating AI-generated innovations. It also sparks discussions on legislative reforms to address AI's growing role in innovation.	The ruling underscores the need for organizations leveraging AI in R&D to consider human oversight in the inventive process to ensure compliance with existing patent laws.	This decision clarifies the legal boundaries for AI systems in intellectual property and could influence patent frameworks globally as AI-driven innovation increases.
UK UK Court of Appeal Emotional Perception AI Ltd v. Comptroller-General of Patents	This case addressed whether inventions involving artificial neural networks (ANNs - foundation of the ML systems on which AI systems are based.) fall under the "computer programs" exclusion in the UK Patents Act 1977. The Court considered whether the invention provided a technical contribution beyond the computer program itself, which would allow it to qualify for patent protection under UK law.	The UK Court of Appeal overturned the High Court's ruling and determined that inventions using ANNs could be excluded from patentability unless they demonstrate a technical contribution beyond the implementation of a computer program.	The decision reaffirms the boundaries of patent protection for AI-related inventions under UK law, creating a high threshold for patent eligibility for software-based innovations. This ruling highlights the need for inventors to demonstrate a clear technical contribution to avoid falling under the "computer programs" exclusion.	The judgment underscores the importance of aligning AI innovation with existing legal frameworks, emphasizing the need for a robust demonstration of technical contribution when seeking patent protection for AI-driven inventions.	This case illustrates the ongoing challenge of balancing innovation and legal constraints in the field of AI, with significant implications for companies investing in AI-driven technologies and seeking intellectual property protection.

Jurisdiction (court / authority) Case/Decision Name	Key issues	Outcome	Significance	AI, Digital and Data compliance aspect	Comment
US District Court for the Northern District of California Andersen v. Stability AI	This case addressed whether Stability AI unlawfully used copyrighted artworks to train its AI models, resulting in AI-generated images that closely resembled the original works. The lawsuit raised critical questions about copyright infringement and fair use in the context of AI training datasets.	In August 2024, the court partially granted and partially denied motions to dismiss the first amended complaint, allowing certain copyright infringement claims to proceed.	This case is a landmark in defining the legal boundaries for AI training processes and copyright law. It highlights the need for clear legal frameworks governing the use of copyrighted materials in AI development and training datasets.	The lawsuit demonstrates the importance of ensuring that AI training data is sourced ethically and legally to comply with copyright laws. AI developers must assess and document permissions for training datasets to mitigate legal risks.	This case sets a significant precedent for how copyright law applies to AI technologies and could shape future industry practices.
US District Court for the District of Delaware Getty Images v. Stability AI	Getty Images filed a lawsuit against Stability AI for allegedly using its copyrighted images without authorization to train AI models, thereby violating intellectual property rights. The case raises issues regarding the unauthorized use of copyrighted material in AI training datasets.	The court denied Stability AI's motion to dismiss and set a trial date for summer 2025 to determine the validity of Getty's copyright infringement claims.	This case highlights the growing tension between AI innovation and intellectual property protection. It underscores the need for AI developers to navigate licensing agreements carefully and respect copyright laws to avoid litigation.	The case emphasizes the importance of implementing compliance protocols for AI training processes. Companies must ensure proper licensing and documentation when using third-party data to train AI systems.	This case could lead to stricter regulations on the use of copyrighted material in AI development, influencing the way AI companies handle training data globally.

Key contacts

Daniela Karollus-Bruner
Partner, Austria
E daniela.karollus-bruner@cms-rrh.com

Martina Gavalec
Partner, Slovakia
E martina.gavalec@cms-rrh.com

Country contacts

Johannes Juranek
Managing Partner, Austria
E johannes.juranek@cms-rrh.com

Christina-Maria Schwaiger
Lawyer, Austria
E christina-maria.schwaiger@cms-rrh.com

Karmen Sinožić
Senior Associate, Croatia
E karmen.sinozic@bmslegal.hr

Dr Döne Yalçın
Managing Partner, Türkiye; Partner, Austria
E doene.yalcin@cms-rrh.com

Arda Özkan
Associate, Türkiye
E arda.oezkan@cms-rrh.com

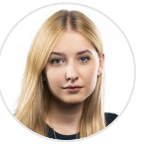
Antonia Kehayova
Counsel, Bulgaria
E antonia.kehayova@cms-rrh.com

Desislava Anastasova
Senior Associate, Bulgaria
E desislava.anastasova@cms-rrh.com

Nejc Vrankar
Lawyer, Slovenia
E nejc.vrankar@cms-rrh.com

Milica Tomić
Lawyer, Serbia, Montenegro
E milica.tomic@cms-rrh.com

Maria Orlyk
Managing Partner, Ukraine
E maria.orlyk@cms-rrh.com



Diana Valyeyeva
Lawyer, Ukraine
E diana.valyeyeva@cms-rrh.com

Martina Gavalec
Partner, Slovakia
E martina.gavalec@cms-rrh.com

Andrej Čierny
Junior Associate, Slovakia
E andrej.cierny@cms-rrh.com

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

Further information can be found at **cms.law**