ANDERSEN®

# IP, ICT AND DATA
## INSIGHTS

→ global.andersen.com

02
26

### Subscribe

If you would like to receive updates on IP, ICT and Data Insights from the Andersen team, you can subscribe via **this form**

# Index

**Andersen Global®** was established in **2013** as the international entity surrounding the development of a **seamless professional services model** providing **best-in-class tax and legal services** around the world.

**Andersen Global Chairman and Andersen CEO**
**Mark L. Vorsatz, Andersen (U.S.)**

**+50.000**

Profesionals

**+1000**

Locations Worldwide

Andersen Global is an association of legally separate, independent member firms, comprised of more than 50.000 professionals worldwide, over 3.000 global partners and a presence in more than 1000 locations worldwide. Our growth is a by-product of the outstanding client service delivered by our people, the best professionals in the industry. Our objective is not to be the biggest firm, it is to provide best-in-class client service in seamless fashion across the globe.

Each and every one of the professionals and member firms that are a part of Andersen Global share our core values. Our professionals share a common background and vision and are selected based on quality, like-mindedness, and commitment to client service. Outstanding client service has and will continue to be our top priority.

# Core Values

Our core values are the foundation of our commitment to exceptional client service. They guide our actions and define our culture, ensuring we consistently deliver the highest quality services globally.

| | |
|---|---|
| **Best-in-class** | We aim to be the benchmark for quality in our industry and the standard by wich other firms are measured. |
| **Transparency** | We value open communication, information sharing and inclusive decision making. |
| **Independence** | Our platform allows us to objectively serve as our client's advocate; the only advice and solutions we offer are those that are in the best interest of our client. |
| **Stewardship** | We hire the best and the brightest and we invest in our people to ensure that legacy. |
| **Seamless** | Our firm is constructed as a global firm. We share an interest in providing the highest level of client service regardless of location. |

# Context

Welcome to the Andersen IP, ICT and Data Insights Newsletter, 3rd Edition – February 2026.

This edition brings together key legal, regulatory, and enforcement developments across Europe in the fields of data protection, cybersecurity, artificial intelligence, and digital regulation. With the NIS2 Directive moving closer to national implementation and AI-related compliance frameworks gaining traction, our contributors examine how these changes are reshaping organisational responsibilities and risk management strategies.

Highlights include decisive enforcement actions by data protection authorities in Greece and Poland, clarifying the scope of GDPR access rights, transparency obligations, and the unlawfulness of covert surveillance practices. Several contributions focus on cybersecurity governance, addressing the implementation of NIS2 in Poland, strengthened board-level accountability, and the management of risks across IT and cyber service supply chains.

This edition also covers significant judicial and regulatory developments relating to AI training and copyright in Germany, non-pecuniary damages for data protection breaches in the telecommunications sector, and the growing compliance obligations for online platforms under the Digital Services Act. Additional updates include national assessments of data protection practices and new policy measures aimed at fostering digital innovation and technological investment.

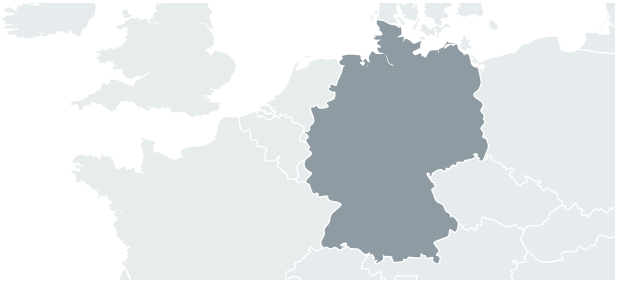
The Andersen IP, ICT and Data Practice continues to be the go-to partner for navigating the complexities of local, European, and international laws in these fields. Our team of specialist lawyers and advisors works with individuals, businesses, and public institutions to design robust IP and data strategies, ensuring compliance while fostering competitiveness and innovation in a fast-changing global economy.

**Themistoklis Giannakopoulos**
IP, ICT and Data
EUROPEAN SERVICE LINE COORDINATOR
✉ themistoklis.giannakopoulos@gr.andersenlegal.com

# Germany

**GmbH Rechtsberatung Steuerberatung**
Member Firm of Andersen Global

**Philipp Wolf**
Senior Associate
philipp.wolf@de.andersen.com



## My lyrics, my rights

CASE LAW

The legal dispute before the Regional Court (LG Munich, Ref. No. 42 O 14139/24) involved the use of well-known song lyrics in training ChatGPT. The court, referencing Article 2 of the EU InfoSec Directive, ruled that 'reproduction' should be interpreted broadly to include all forms of duplication, which encompasses AI training. The lyrics are accessible and can be copied into at least two OpenAI language models and may also be generated as outputs in response to prompts.

Memorisation of the lyrics during training also constitutes reproduction under copyright law. The court considered exceptions in Sections 44b and 57 of the German Copyright Act (UrhG), which allow automated analysis of digital works to identify patterns and trends, including for scientific research, without the rights holder's permission. These exceptions also permit reproduction when the work is only a negligible part of a larger work. However, the court found these exceptions inapplicable, as the law requires that automated analysis must not harm the original authors' ability to profit from their work. The court determined that OpenAI's actions directly impact the rights holders' financial interests.

> The memorization of song lyrics in OpenAI's language model and the reproduction of song lyrics in the outputs constitute infringements of copyright exploitation rights. These are not covered by limitations on text and data mining."

## KI training

CASE LAW

In preliminary injunction proceedings before the Higher Regional Court of Cologne (May 23, 2025, Ref.: 15 UKL 2/25), the court ruled that Meta may process publicly available data of adult users of Facebook and Instagram for the purpose of training generative AI systems. The data processing in question is compatible with the GDPR. The court based its ruling on Article 6(1)(f) of the GDPR. The legitimate interest was deemed to be an economic interest (development and improvement of proprietary AI models in the EU).

The processing is necessary because anonymized and synthetic data do not currently allow for equivalent training.

Notably, the assessment of special categories of data (Article 9 GDPR) is of particular importance. The court assumes that Art. 9(2)(e) GDPR is relevant insofar as users have made their data public themselves. For third-party data, the processing prohibition enshrined in Art. 9 GDPR only applies if there is an active objection. Here, the court clarifies that, regarding the unauthorized use of third-party data, Meta's interest in data processing outweighs the data subjects' protection interests. Serious violations are unlikely anyway and only occur through the application of AI itself. In the court's opinion, a general ban on AI training would contradict the EU's legal objective of striking a balance between data protection and the promotion of innovation.

# Greece

**Andersen in Greece**
Member Firm of Andersen Global

**Foteini Giannaki**
Junior Associate
✉ foteini.giannaki@gr.andersenlegal.com

## Access Denial and Non-Cooperation: Hellenic DPA Fines Totalling €22.000

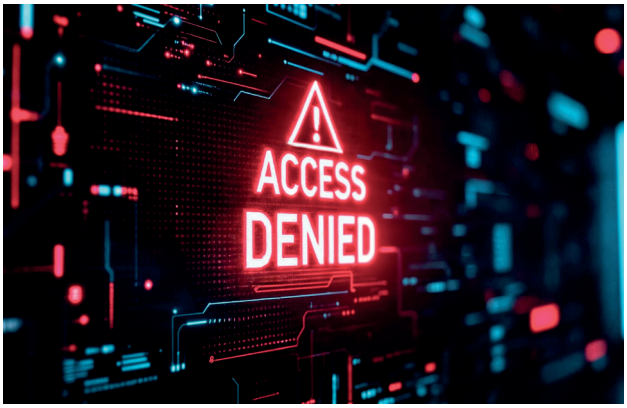
LAW COMMENTARY

The HDPA imposed administrative fines totalling €22.000 on an Insurance Company and its partner entity for infringements of the GDPR.

The case arose from a complaint lodged by an individual insured under a dental coverage program, who had repeatedly exercised his right of access under Article 15 GDPR, requesting copies of recorded telephone conversations with the program's customer service centre. The requests, addressed to both the Insurance Company and the partner company operating the call centre, remained unsatisfied.

The Insurance Company contended that it lacked access to the recordings, which were allegedly under the control of the partner company. However, upon examining the contractual framework, the HDPA found that the partner company had been assigned the technical task of recording and storing calls on behalf of the Insurance Company, which determined the purposes and means of processing and therefore acted as data controller. Its failure to comply with the access request constituted a violation of Article 15 GDPR.

The partner company was also found in breach of Article 31 GDPR for failing to cooperate with the Authority's investigation. The HDPA imposed fines of €20.000 on the Insurance Company and €2.000 respectively on the partner entity, underscoring the fundamental importance of the right of access and the duty of cooperation with the supervisory authority.




> The HDPA fined an Insurance Company & its partner for failing to respect data subjects' access rights and for non-cooperation, imposing fines of €20.000 and €2.000 under Articles 15 and 31 GDPR."

## Banking Secrecy Cannot Override the GDPR Right of Access, Rules Hellenic DPA

LAW COMMENTARY

The HDPA examined a complaint filed by a borrower against a Bank, its non-performing loans company, and its subsidiary real estate entity for refusing access to a valuation report of her mortgaged property, prepared during debt settlement negotiations.

Although the complainant had paid for the valuation, her access request was denied. The Bank invoked confidentiality and the internal nature of the valuation process, while the other entities referred her back to the Bank.

> Banking confidentiality does not exempt controllers from GDPR obligations, the HDPA held, directing the Bank to grant the borrower access to her valuation report and review its internal classification practices."

The HDPA found that the valuation report contained personal data (including the complainant's name, client code, property details and estimated value) and thus fell within the scope of Article 4(1) GDPR. It held that the Bank was the data controller under Article 4(7) GDPR, and its subsidiary real estate company acted as processor under Article 4(8).

The Authority rejected the Bank's reliance on professional or banking secrecy, emphasizing that such confidentiality cannot override the right of access under Article 15 GDPR unless explicitly justified by law.

While no monetary fine was imposed, the HDPA ordered the Bank to reconsider its refusal and comply with the complainant's access request, stressing that banking secrecy cannot be used to circumvent GDPR obligations.

# Italy

**Andersen in Italy**
Member Firm of Andersen Global

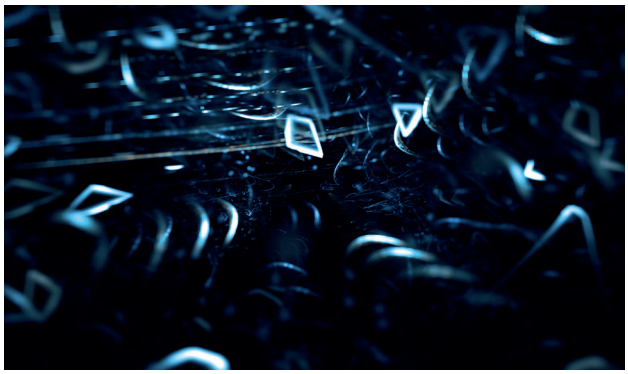
**Paola Finetto**
Partner
✉ paola.finetto@it.andersen.com

## Synergy between NIS2 and AI: An opportunity to strengthen corporate compliance in privacy and cybersecurity

LAW COMMENTARY

Artificial intelligence (AI) is transforming operational processes and sectors that fall within the scope of the NIS2 Directive (EU Directive 2022/2555). The integration of an organizational and security system that complies with NIS2 requirements, enhanced by AI-based solutions, represents a concrete opportunity to increase business resilience and ensure a high level of cybersecurity.

> Conscious integration between NIS2, AI Act, and GDPR."



On the one hand, the NIS2 Directive introduces strict obligations in terms of risk management, incident response, business continuity, and cybersecurity governance; on the other hand, the use of AI can enhance an organization's ability to detect threats in a timely manner and automate response actions. However, it is essential that these technologies are used in an ethical, responsible manner that complies with personal data protection legislation.

Ultimately, conscious integration between NIS2, AI Act, and GDPR allows for the development of privacy-friendly AI solutions that can ensure high security standards while reducing response times to cyberattacks. To achieve a truly integrated compliance system, it is nevertheless necessary to adopt a robust governance strategy and a risk-based approach. This involves assessing the risks associated with the use of specific AI tools and systems, introducing transparent business policies, and promoting targeted cybersecurity training.

## Risk management in the IT and cyber services supply chain

LAW COMMENTARY


**Paola Finetto**
Partner
✉ paola.finetto@it.andersen.com

**Luca Rigotti**
Partner
✉ luca.rigotti@it.andersen.com


In today's highly interconnected marketplace, a company's resilience is closely tied to the reliability of its suppliers. Managing risks across the supply chain has become a cornerstone of corporate compliance, as any unethical or negligent behaviour by suppliers or subcontractors can lead to severe legal, reputational, and financial consequences. A Third-Party Risk Assessment aims to mitigate these threats. It has also become essential regarding IT and cyber service providers, which are crucial to the proper functioning of business operations. Auditing ICT and cybersecurity practices, roles and responsibilities, data subject rights, continuity plans, and security incidents helps build a transparent and reliable supply network. In a historical context where responsibility extends to the entire value chain, the creation of structured and continuous processes for evaluating and monitoring suppliers not only safeguards the business but also becomes a real source of competitive advantage.

> Third-Party Risk Assessment + essential regarding IT and cyber service providers."

# Poland

**Andersen in Poland**
Member Firm of Andersen Global

**Kamil Kozioł**
Senior Manager
✉ kamil.koziol@pl.andersen.com

**Alicja Dziegciarz**
Associate
✉ alicja.dziegciarz@pl.andersen.com

## Implementation of the NIS2 Directive Submitted to the President

REGULATORY UPDATES

The Polish government's draft law implementing the NIS2 Directive, is currently awaiting the President's signature. This marks a significant step towards strengthening national cybersecurity resilience, and aligning Poland with Europe's updated cybersecurity framework.

It is expected, that the law will take effect in February 2026, following the termination of the legislative process. Under the new regulations, "important" and "essential" entities will be required to fulfil their obligations within 12 months from the date the law becomes effective. According to the latest amendments approved during the legislative process, penalties and fines for non-compliance may only be imposed starting 24 months after the provisions enter into force, providing organizations with an extended two-year grace period to fully implement the required cybersecurity measures without immediate risk of sanctions.

> It is expected, that the law will take effect in February 2026, following the termination of the legislative process. Under the new regulations, "important" and "essential" entities will be required to fulfil their obligations within 12 months from the date the law becomes effective".

According to preliminary estimates, the new conditions will affect approximately 10,000 economic entities operating in Poland, spanning sectors such as energy, transport, healthcare, finance, and digital infrastructure. The forthcoming legislation is therefore anticipated to have an impact on both public and private sector organisations, forcing them to improve risk management, incident response, and supply chain security in line with the European standards.

The coming months will be crucial for organisations preparing for NIS2 compliance, because the scope of the new requirements is significantly broader than previously anticipated.

## Strengthened Board Responsibility under the NIS2 Implementation

LAW COMMENTARY

The implementation of the NIS2 Directive significantly strengthens the responsibility of the management board regarding cybersecurity. It gives an obligation on the board to approve and supervise risk management measures, provide training for board members, and ensure adequate resources.

Board members bear personal responsibility for any negligence, which may result in sanctions such as fines, legal proceedings, or even temporary bans from holding manager positions. This responsibility is collective (shared by all board members unless a specific person is designated) and cannot be delegated to lower management levels, even if duties are assigned elsewhere.

> Board members, bear personal responsibility for any negligence, which may result in sanctions such as fines, legal proceedings, or even temporary bans from holding manager positions."

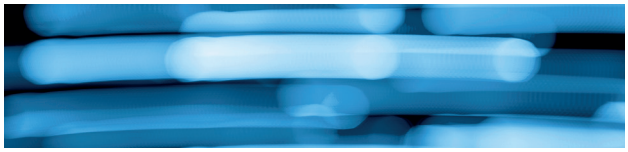
This framework aims to ensure effective oversight and accountability at the highest level of organisational management in matters of cybersecurity.

## Hidden Video Surveillance and Data Security Failures at Medical Centre

CASE LAW

The President of the Personal Data Protection Office in Poland (UODO) imposed two fines on Medical Centre Ujastek for installing image-recording devices in two neonatal ward rooms without complying with legal regulations and for failing to apply adequate technical and organisational measures to protect the data stored on the memory cards of these devices.

From 1 July to 23 July 2023, the monitoring system recorded images of newborns and their mothers during intimate activities such as feeding and care. Neither patients nor staff were informed about this recording, making the surveillance covert and in violation of data protection laws.



Additionally, the medical centre reported the loss or theft of memory cards containing all recordings. An investigation revealed that the devices were not configured to meet the facility's security requirements and the risk assessment failed to identify the causes of the incident or implement preventive security measures.

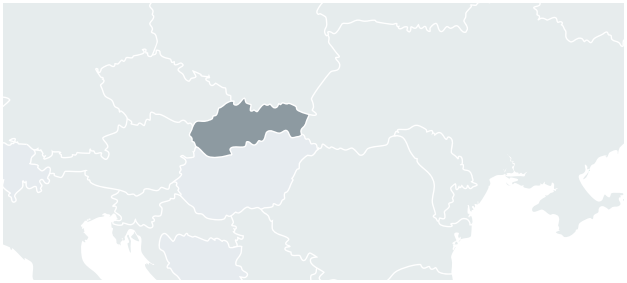
Following these violations of data protection regulations, the President of UODO imposed two sanctions on the centre due to illegal monitoring practices and inadequate data protection measures.

> Monitoring system recorded images of newborns and their mothers during intimate activities such as feeding and care. Neither patients nor staff were informed about this recording, making the surveillance covert and in violation of data protection laws."

# Slovakia

**CLS Čavojský & Partners, S.R.O.**
Collaborating firm of Andersen Global

**Jakub Kováčik**
Senior Associate
✉ kovacik@clscp.sk



## Report on the State of Personal Data Protection for 2024

REGULATORY UPDATE

The Office for Personal Data Protection of the Slovak Republic released its Report on the State of Personal Data Protection for 2024, providing an overview of how privacy regulations were applied nationwide. More than half of all inspections focused on camera surveillance systems, mainly those installed by private individuals around homes or by municipalities in public spaces.

According to the Office, surveillance has dominated its inspection agenda since 2021. The most frequent violations involved unlawful data processing, insufficient information provided to monitored individuals, and missing data protection impact assessments. In several cases, cameras recorded broader areas than necessary, including public roads and neighbouring properties.

The section Selected Cases from the Supervisory Activities of the Office highlights examples from practice. Inspectors reviewed camera systems in social care homes, addressing privacy concerns of residents, as well as unlawful processing of traffic accident data and unauthorized use of personal data for marketing purposes.

The report concludes that in 2024, the Office focused not only on penalties but also on education and prevention, encouraging organizations and individuals to handle data responsibly and to strengthen a culture of privacy protection across both the public and private sectors.

> In 2024, the Slovak Data Protection Office concentrated on camera surveillance systems—especially those run by individuals and municipalities—revealing frequent breaches of legality, transparency, and data minimization principles."

## Data protection in the field of telecommunication services – non-pecuniary damages

CASE LAW

The decision of the Supreme Court of the Slovak Republic (5Cdo/137/2024 dated 31.7.2025) relates to the protection of personality and compensation for non-pecuniary damage in connection with the violation of personal data protection under the GDPR in the field of telecommunications services.

The case concerned a security incident during the destruction of documents of a telecommunications operator. The intermediary in charge of document destruction failed to exercise due diligence in handling customers' sensitive personal data, which included name, address, birth number, ID card number and signature. This misconduct constituted a breach of obligations under the GDPR.

> Supreme Court ruling confirms telecommunications operators' liability for GDPR violations, awarding compensation for potential data breach risks involving customers' sensitive personal information."

The Slovak Data Protection Authority imposed a fine of €5,000 for the data breach. The injured party subsequently sought compensation for non-pecuniary damage in civil proceedings for the protection of personality.

The court awarded compensation for non-pecuniary damage in the amount of EUR 110. In determining the amount of compensation, it considered several factors: there was a potential threat to rights rather than a proven interference with them, there had been no disclosure or misuse of personal data, and the responsible party had apologized for the incident.

# Malta

**Chetcuti Cauchi Advocates**
Collaborating firm of Andersen Global

**Danielle Mercieca**
Senior Associate
✉ danielle.mercieca@ccmalta.com

## Online Platforms Under Pressure

LAW COMMENTARY

The EU Digital Services Act (DSA) introduces new legal obligations for online platforms operating in Malta and across the EU. By placing strict obligations on platforms to detect, prevent, and remove illegal or fraudulent content. As online advertising becomes increasingly sophisticated, so too do the risks posed by misleading promotions, impersonation schemes, and manipulative design. The DSA directly targets these harms through enhanced transparency duties, mandatory risk assessments, and stronger mechanisms for user reporting and redress.

Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) now face heightened scrutiny, including independent audits and the requirement to demonstrate robust content moderation processes. Enforcement actions by the European Commission show that compliance is no longer optional: platforms must proactively address systemic risks or face significant penalties.

For businesses, the DSA introduces greater clarity and a more trustworthy digital environment, while consumers benefit from stronger safeguards against deceptive practices. The regulation seeks to rebalance online power dynamics by ensuring that digital services operate responsibly, fairly, and transparently across the EU.

The Digital Services Act reframes online accountability by making transparency, safety, and fairness core obligations—not optional aspirations—for every major platform."

## Tech & Innovation Incentives Launched

JURISDICTIONAL UPDATES


**Danielle Mercieca**
Senior Associate
✉ danielle.mercieca@ccmalta.com

**Susanna Grech Deguara**
Senior Associate
✉ sdeguara@ccmalta.com


The Malta Budget 2026 places strong emphasis on accelerating the country's technological and innovation capacity through a suite of ambitious fiscal incentives. Central to these measures is a 175% super deduction for eligible research and innovation (R&I) expenditure, enabling businesses to significantly reduce taxable income while investing in high value development projects. Complementing this is a 60% tax credit on qualifying capital investments in machinery, software, automation tools, and other productivity enhancing technologies, claimable over four years and aimed at boosting enterprise modernisation and competitiveness.

> Malta's 2026 Budget transforms innovation from aspiration into actionable investment, rewarding businesses that modernise, digitise, and lead the next wave of technological progress."

Digital transformation remains a national priority. The enhanced MicroInvest Scheme now offers tax credits up to €65.000 for Malta based SMEs and €85.000 for Gozo enterprises, with digitalisation expressly recognised as an eligible investment category. To support talent retention in knowledge intensive industries, the government will also finance 65% of salary increases for long serving employees (or 80% in Gozo), easing wage pressures while strengthening workforce stability.

These measures, coupled with Malta's robust economic projections, reinforce the country's strategic ambition to position itself as a competitive, digitally enabled innovation hub within the EU.