

Unprecedented GDPR Enforcement in Lithuania: Natural Person Receives Fine

March 2024

In a landmark ruling with substantial implications for GDPR enforcement in Lithuania, the State Data Protection Inspectorate (VDAI) has issued its first-ever fine against a natural person for violations of the General Data Protection Regulation (GDPR). This groundbreaking decision underscores a new era in data protection accountability, extending beyond organizations to individual actors.

Detailed Overview of the Case

Decision Date: 11 September 2023

Nature of the Case: The case is national in scope, involving a healthcare service provider in the field of plastic surgery and an individual doctor.

Violations & Consequential Penalties:

- The healthcare provider was penalized with a €6 000 fine for the unauthorized publication of patient photos on the company's and the doctor's personal Instagram accounts without the patient's consent.
- In an unprecedented move in Lithuanian GDPR enforcement history, the doctor involved was fined €840. This decision is notable as it represents the first instance in Lithuania where a natural person has been held financially accountable for breaching GDPR.

In-depth Analysis of the Violation

The case stemmed from the publication of identifiable patient photos, which are considered sensitive personal data under GDPR. The investigation revealed that the healthcare provider and the doctor failed to obtain clear, explicit consent from the patient, thereby breaching several GDPR principles, including those of legality, fairness, transparency, and confidentiality.

Interestingly, the decision to fine the doctor individually was based on the determination that he acted as an independent data controller. This aspect of the ruling is particularly significant as it establishes that individuals within an organization,

not just the organization itself, can be held liable for GDPR violations.

Implications for Data Controllers and Processors

This ruling marks a turning point in GDPR enforcement, highlighting the importance of individual responsibility in the realm of data protection. It sends a clear message that compliance is not only a corporate responsibility but also a personal one.

Organizations, as well as individual professionals, need to understand the gravity of GDPR regulations and ensure that their practices align with the law. This includes obtaining clear, unambiguous consent for the use of personal data, especially when it pertains to sensitive information such as health data.

Recommendations for Compliance

- 1. Review and Update Consent Procedures:** Ensure that consent forms and processes are robust, clear, and in strict alignment with GDPR requirements.
- 2. Enhance Training and Awareness:** Regularly train staff and individuals involved in data processing on GDPR compliance, emphasizing personal accountability.
- 3. Implement Rigorous Data Protection Policies:** Establish and enforce stringent data protection policies that comply with GDPR standards.
- 4. Regular Audits and Assessments:** Conduct periodic audits of data processing activities to identify and mitigate any potential compliance risks.

This case serves as a critical reminder of the evolving landscape of data protection law and the importance of adhering to GDPR standards.

For assistance in understanding and implementing GDPR compliance measures, please contact our office for expert guidance and support.