by **GABIJA PANOMARIOVAITĖ** –
Junior Associate & Assistant Director of Platforms at Klauberg BALTICS attorneys-at-law (Lithuania)

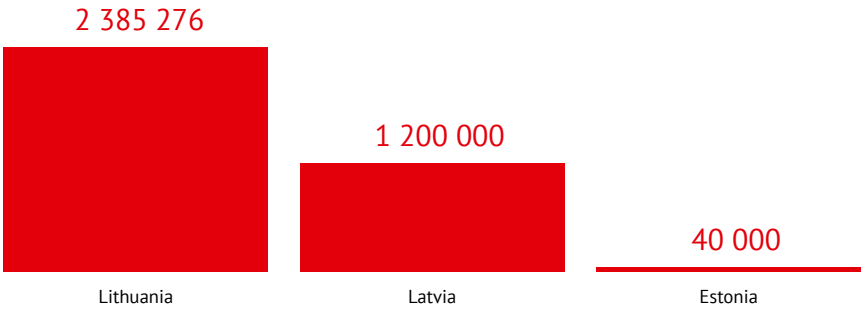
by **KĀRLIS ROMANOVS** –
Paralegal at Klauberg BALTICS attorneys-at-law (Latvia)

by **KENNETH TOMINGAS** –
Associate at Klauberg BALTICS attorneys-at-law (Estonia)

Photos: publicity photos

Overview of Data Protection in the Baltic States

Highest fine imposed 2024 Statistics on fines imposed in the Baltic States
EURO



The Baltic States – Estonia, Latvia, and Lithuania – have implemented the General Data Protection Regulation (GDPR), providing a common framework for personal data protection. Personal data is defined as any information related to an identified or identifiable natural person. The GDPR applies to all instances of personal data processing, except when the data is processed for personal or household purposes. Despite the shared regulatory structure of all Baltic countries, each country faces unique challenges in enforcing data protection laws and managing data breaches.

Regulatory Authorities and Oversight

In all three Baltic countries, specific authorities are responsible for overseeing data protection compliance:
Estonia: The Data Protection Inspectorate (DPI) is tasked with ensuring adherence to the GDPR and national laws. It issues precepts and supervises compliance, although the use of misdemeanour procedures for fines limits the effectiveness of enforcement.
Latvia: The Data State Inspectorate (DSI) supervises data protection laws and GDPR compliance. It has a broad range of responsibilities, including promoting data protection, overseeing certification procedures, verifying the qualification of data protection officers, conducting inspections to ensure that data processing complies with laws and regulations, and filing legal actions for violations.
Lithuania: The State Data Protection Inspectorate (SDPI) monitors data processing activities and resolves reports of data security breaches. Its role also includes ensuring that businesses and individuals comply with the GDPR's requirements.

All three countries have aligned their data protection laws with the GDPR,

which applies to the processing of personal data that can identify a natural person. This includes not just direct identifiers like names and ID numbers, but also indirect identifiers that could be combined to identify individuals. The GDPR lays down strict rules for data collection, storage and transfer, and gives individuals the right to access, correct, or erase their data.

Data Breaches and Common Causes

In the Baltic States, data breaches are a pressing concern, often due to human error or cyberattacks:
Human Error: The majority (52%) of data breaches reported in Lithuania, for example, were attributed to mistakes like misdirected emails or improperly anonymized documents. Such breaches are often unintentional and cannot always be prevented through technical measures alone.
Cyberattacks: Cyberattacks, including ransomware and phishing, are a growing issue in the region. In Lithuania, 33% of reported breaches in 2024 were linked to cyberattacks. According to the Information System Authority (RIA), Estonia experienced 6,515 impactful cyber incidents in 2024, nearly twice as many as in 2023. A total of 68 data breaches were recorded in Estonia in 2024, with the most significant involving the theft of data from nearly 700,000 customers of Apotheka, Apotheka Beauty, and Pet City.
Malicious acts: In 2024, the Latvian Data State Inspectorate (DSI) carried out 991 inspections. In 203 cases, the Inspectorate opened an in-depth inspection case, finding 178, of which corrective measures (reprimands) were applied in 49 cases. In 20 cases, subjects were fined for data breaches. Most of the complaints came from individuals about illegal video surveillance in the workplace or data processing rules in social networks.
Fines and Penalties for Data Breaches
Estonia: Estonia was known for imposing the lowest fines among the Baltic States due to the fact that fines are applied in misdemeanour proceedings. One of the issues was that the maximum fine for misdemeanours was up to €400,000. However, this was subject to change with the enactment of amendments to the Penal Code on 1 November 2023. These amendments expand the DPI's regulatory scope, enabling it to impose fines of up to €20 million or 4% of a company's global annual turnover. Additionally, the amendments introduced new provisions that make it possible to hold legal persons liable for violations pertaining to the GDPR.
Latvia: The DSI can impose administrative fines under both national law and the GDPR. Fines can be substantial, ranging from €1,000 for minor violations to up to €20 million or 4% of a company's global turnover for more serious breaches. For example, in 2024, the telecommunications company "Tet" was fined €1.2 million for security violations. The DSI also considers factors like the severity of the breach and the cooperation of the offending party when determining fines.
Lithuania: Lithuania enforces data protection fines in accordance with the GDPR, with penalties reaching up to €20 million or 4% of a company's global annual turnover. In 2024, the Lithuanian Data Protection Inspectorate imposed 13 fines, totalling €2.42 million, with the largest fine amounting to €2.39 million. Unlike Estonia, Lithuania has introduced specific regulations for the public sector, capping fines at 0.5–1% of an institution's annual budget, but not exceeding €30,000–€60,000. In Latvia, a public institution cannot be fined for data breaches. The only penalties to be imposed are a written apology and the correction of the data breach. Liability applies not only to organizations but also to employees in certain cases. If an employee, upon gaining access to personal data, processes or discloses it unlawfully in their own name rather than on behalf of the organization, they may be considered an independent data controller and held personally accountable. However, it should be noted that on 18 February 2025, the Lithuanian Data Protection Inspectorate issued a decision contradicting the existing practice by holding only the institution liable, without applying penalties to the employee who exceeded their authority. The country emphasizes transparency, requiring clear communication with affected data subjects regarding their rights and necessary actions.

Rights of Data Subjects and Accountability

Under the GDPR, data subjects in all three countries have a wide range of rights to protect their personal data. These include the right to access, correct, delete, or restrict the processing of their data. Additionally, they can file complaints with the relevant supervisory authority if they believe their data has been improperly processed.
Lithuania: The SDPI highlights the importance of informing individuals about what actions they can take in response to data breaches, such as blocking credit cards or contacting responsible parties. it also emphasizes clear, accessible communication to ensure that individuals fully understand their rights.
Estonia and Latvia: Both countries similarly grant individuals the right to be informed about data processing, and they require organizations to act transparently when a breach occurs. Latvia's DSI, for example, takes into account whether an organization has implemented corrective measures or cooperated with the authorities when determining fines.