

# Data Protection in Estonia

August 2023

In the digital age, where personal data is the new currency, ensuring its protection has become an indispensable responsibility. Estonia, a Baltic nation known for its innovative technological advancements, may not be the greatest example when it comes to data protection. As the digital era continues to evolve, safeguarding personal data has become a paramount concern. In this article, we delve into the key aspects of data protection in Estonia and explore the measures taken by the country to ensure the privacy and security of its citizens' information.

## Estonia's Data Protection Regulation

At the heart of Estonia's data protection efforts lies the "Personal Data Protection Act" (PDPA), which governs the processing of personal data within the country and entered into force on the 15<sup>th</sup> of January 2019. The PDPA is aligned with the General Data Protection Regulation (GDPR) of the European Union (EU) - the gold standard in data protection - to guarantee harmonization with EU data protection principles.

The PDPA enshrines the rights of data subjects, ensuring that individuals have control over their personal data. It mandates transparency, requiring organizations to inform individuals about the processing of their data and obtain explicit consent when necessary. Furthermore, data controllers and processors are held accountable for safeguarding the data they handle.

## Key Features of Estonia's Data Protection Framework

- 1. Data Protection Inspectorate (DPI):** The Data Protection Inspectorate is Estonia's data protection authority responsible for overseeing compliance with the PDPA. The DPI ensures that data processing activities align with the principles of legality, fairness, and transparency. It also handles complaints and conducts investigations into data breaches and privacy violations.
- 2. eID and Digital Signatures:** Estonia's advanced electronic identification (eID) system has revolutionized the way citizens interact with government and private services. The eID allows secure access to digital services and transactions, enabling citizens to sign documents

digitally, minimizing the need for physical paperwork while ensuring authenticity and data integrity.

- 3. X-Road:** Estonia's X-Road is a secure data exchange platform that facilitates communication between various government and private sector databases. The X-Road ensures data confidentiality, integrity, and interoperability while maintaining strict access controls, reducing the risk of unauthorized data access.
- 4. Blockchain Technology:** Estonia is one of the pioneers in implementing blockchain technology for data protection. The technology is used to secure critical records, such as those in the healthcare and legal sectors. Blockchain ensures data immutability, reducing the risk of data tampering and unauthorized alterations.
- 5. Cybersecurity Measures:** Estonia's focus on cybersecurity is essential for safeguarding data from cyber threats and attacks. The country has invested heavily in developing robust cybersecurity infrastructure and regularly conducts national-level cybersecurity exercises.

## Impact on Digital Services

The implementation of secure and user-friendly e-services has streamlined administrative processes, reduced bureaucracy, and enhanced service accessibility. From e-voting to e-residency, Estonia has leveraged digital solutions to provide efficient and transparent services but there are certain risks when talking about data breaches. For example, in the summer of 2021 a hacker was able to download 286,438 personal identification document photos from the State Information System's Authority (RIA). The head of RIA said that the attack was made possible by a vulnerability in the database, but the Estonian Data Protection Inspectorate commented that no fines can be issued against a state authority and the affected persons could not claim compensation. The focus on data protection has become more important during this year which is also evident by the fact that the Data Protection Inspectorate and the Labour Inspectorate signed an agreement to work together regarding data protection issues in 2023 during May.



## Data Breaches and Fines in Estonia

According to reports Estonia has the lowest fines connected to data breaches in the Baltics. This is mostly because the process of applying fines is done only in misdemeanour proceedings. The Estonian Data Protection Inspectorate may also apply non-compliance levies as an administrative measure if an entity under investigation does not comply with an administrative precept. It was stated that until the end of 2022 there was about a total of 560 data breaches reported in Estonia. In total the Estonian Data Protection Inspectorate has issued fines in amount of approximately EUR 35,000 until the end of 2022, which is the smallest amount in the Baltic states. According to the GDPR data protection authorities are able to apply fines up to 4% of the total worldwide turnover of an undertaking in the preceding financial year or up to EUR 20 million, whichever is higher. Starting from the 1st of November 2023 the Data Protection Inspectorate in Estonia will be able to apply fines in accordance with the amounts set in the GDPR.

## Challenges and Future Outlook

Despite Estonia's successes in technological advancements, challenges remain. Ensuring compliance with data protection regulations for all entities, including private enterprises and government bodies, requires continuous monitoring and enforcement. The country must also stay ahead of emerging technological threats and maintain its cyber defence capabilities.

Although fines connected to data breaches are the lowest in the Baltics and the focus of the government has not really been on data protection then it is still a very important topic in Estonia due to the focus on secure and user-friendly digital services. Since the Estonian Data Protection Inspectorate will be able to fine entities according to the amounts set in the GDPR starting from the 1<sup>st</sup> of November 2023, companies will have to be more careful than ever when processing people's personal data. The colossal differences between the fines that were issued before and can be issued since the 1st of November 2023 will force companies to take a serious look at their data processing practices and cybersecurity measures.