Data protection in the Baltics – all businesses need to be aware

FRANZISKA BABILON,
Attorney at Law, Klauberg BALTICS Attorneys-at-Law (Riga, Tallinn, Vilnius)

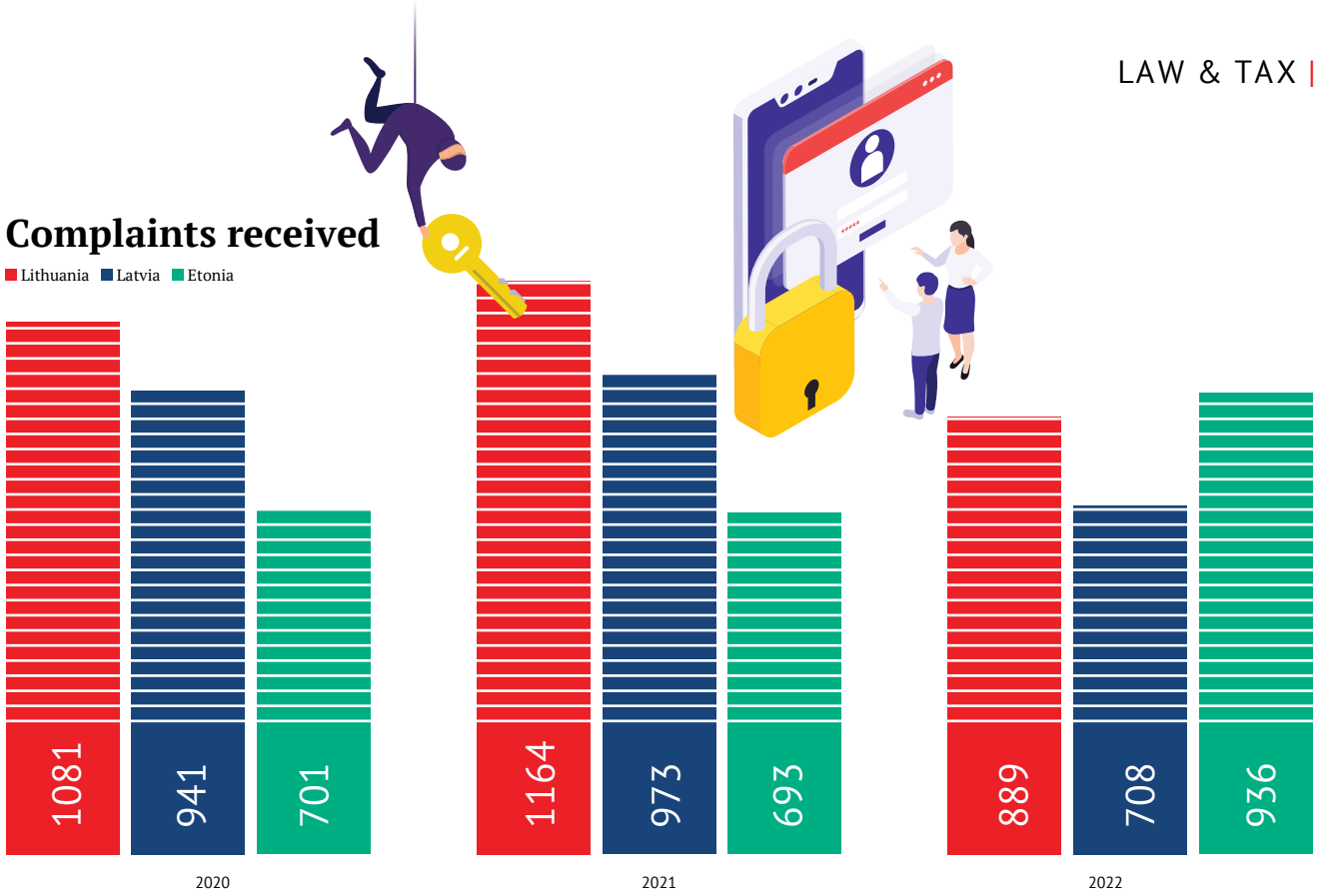
The protection of personal data is becoming increasingly important in today's digitalized world, especially in the Baltic States, a region with a thriving digital economy. As members of the European Union, Estonia, Latvia, and Lithuania are subject to EU data protection regulations, including the General Data Protection Regulation (GDPR).

It is crucial for companies to have a thorough knowledge of the applicable data protection regulations to avoid possible sanctions. The regulations apply to all companies that process personal data of customers or employees. Personal data is any information relating to an identified or identifiable natural person and is processed when such data is collected, used, or stored in, or intended to be part of, a filing system. Any natural person falls within the scope of protection of the provisions, and accordingly, the provisions also apply in relation to employment relationships. Employees, as natural persons, are thus to be considered as data suspects. Furthermore, the definition clarifies the scope of the data protection provisions for almost all companies, since payroll accounting, for example, constitutes the processing of personal data. Through the respective data protection laws in the Baltic countries, the GDPR is implemented at a national level to strengthen data protection. It is important to note that the national data protection laws refer to the GDPR, which is the most important basis for data protection in the Baltic States.

The need for lawful processing

In Latvia, data protection is regulated by the Law "Fizisko personu datu apstrādes likums", which has been in force since 5 July 2018. This law sets out the principles for data processing and the protection of individual privacy. Similarly, data protection in Lithuania is regulated by the "Asmens duomenų teisinės apsaugos įstatymas", which has been in force since 16 July 2018 and sets out clear rules for data processing. Slightly later than the other two Baltic states, Estonia's data protection law "Isikuandmete kaitse seadus", only entered into force on 15 January 2019. However, the later entry into force does not mean that less importance is attached to data protection in Estonia. The Act, like the other two, lays down strict provisions for data protection. Further national regulations on data protection in employment relationships may also arise from the respective labor laws and other legal acts.

All three data protection laws emphasize the need for lawful processing of personal data, with controllers, which include employers, having to ensure that data is only used for its intended purposes and that employees, as data suspects, are informed about the processing of their data. Before personal data can be processed in the employment relationship, workers' consent is often required. To ensure the security of data, employers in the Baltic States are obliged to take appropriate technical and organizational measures to prevent unauthorized access, loss, or misuse of personal data. Employees have the right to access and verify their data and to correct inaccurate information. The processing of sensitive personal data, such as health data, information on ethnic origin, and trade union membership, is subject to special safeguards. Such processing is only permitted with the explicit



consent of the data subject or if there is a clear legal basis. Also applies to external service providers

The transfer of employee data to a third party by the employer, e.g. by outsourcing tasks to service providers outside the company, also falls under this protection of the laws. For such a transfer to occur in Estonia, Latvia, and Lithuania, it is necessary for the employees concerned to be expressly informed that their data will be transferred to a third party and for what purpose. Employee consent is usually required unless there is a legal basis for the disclosure, such as compliance with legal obligations or the company's legitimate interest. In addition, companies must ensure that third parties who gain access to employee data implement appropriate security measures to ensure the confidentiality and integrity of the data.

In case of non-compliance with data protection rules, employers may face sanctions. The Baltic data protection authorities monitor compliance with data protection laws in the respective country and can take appropriate measures such as fines and criminal sanctions in case of violations. In 2022, the Estonian data protection authority "Andmekaitse Inspektsioon" recorded an increase in data protection complaints to 936, while Latvia with 708, and Lithuania with 889 recorded a slight decrease. Nevertheless, the Lithuanian DAP "Valstybinė duomenų apsaugos inspekcija" received the most complaints in 2020 (1081) and 2021 (1164) compared to the other Baltic countries. In the Latvian DAP "Datu valsts inspekcija", the number of complaints remained constant in 2020 and 2021, namely 941 and 973 complaints respectively. Despite the slight decrease in complaints, it is important that companies continue to increase their efforts to comply with data protection regulations and ensure the protection of personal data. To achieve this, it is advisable to familiarise oneself comprehensively with the regulations of the individual countries. The seven basic principles of data processing are a valuable support in this regard:

1. principle "lawfulness, fair processing, transparency"
2. Principle "purpose limitation"
3. Principle "data minimization"
4. Principle "accuracy"
5. Principle "limitation of storage"
6. Principle "integrity and confidentiality"
7. Principle "accountability"

By adhering to these principles, companies can ensure responsible handling of personal data and thus further strengthen data protection in the Baltic States.

Stay updated on the latest developments in Data Protection by following our Legal Newsletter (register at www.klauberg.legal), where we regularly publish news and updates about data protection regulations and practices.