LEXcellence Statement regarding the European Data Protection Board issues recommendations regarding compliance between the new AML-CFT framework and the GDPR

European Commission following the publication of the Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing aims to present a new legislative proposal single rulebook concerning AML and terrorist financing, most probably in the form of Regulation or a revised Directive. Obviously, the new set of rules will concern the processing of the personal data of users. Andrea Jelinek, Chair of the European Data Protection Board, wrote a letter to European Commissioner for Financial Services, financial stability, Capital Markets Union, Ms. Mairead McGuiness, and European Commissioner for Justice, Mr. Didier Reynders, listing six personal data protection principles, which should be the foundation of the emerging regulatory frameworks. What are the six mentioned principles, and why are they so important? Let us analyze them one by one.

1. Proportionality and efficient risk-based approach

The letter states that the AML-CFT framework must examine each case individually, taking into consideration differences between different cases in a proportional manner. Article 52 of the Charter of Fundamental Rights of the European Union protects one's freedom to exercise one's rights, and therefore establishes the principle of necessity: any legislation that somehow limits one's right to privacy must be justified by a specific purpose. Unnecessary, disproportionate inferences with fundamental citizen rights should not be included within the regulatory frameworks. Given that the GDPR is general and does not include rules specific to given sectors, it should be the legislator's task to outline sector-specific data protection rules that would maximally protect citizens' privacy rights.

2. Data minimization

Article 5(1) (c) of the GDPR states that entities are allowed to process only the amount of data, which is required for compliance with the AML-CFT framework. All rules regarding data processing should be specified, especially in terms of data collection, and types of data processed for court cases, for example, regarding criminal convictions and offenses. Unnecessary data processing should be avoided since it only leads to the creation of false-positive reports, which generate costs and add up to data-related workload. The principle of data minimization also states that any personal data linked to criminal convictions and offenses can be only processed when it is directly connected to AML-CFT.

3. Data accuracy

Any processed data should be accurate, reliable, and up-to-date to ensure compliance with the AML-CFT. The board's recommendation is to legally oblige companies to implement effective data protection policies, which protect citizen's rights to privacy, and yet allow businesses to process data. For greater transparency, such policies should also take into consideration the collection of personal data from third parties, which are involved in the data processing. Since many entities rely on "watchlists" provided by third parties to verify information and screen databases, it raises certain concerns with data privacy. Although providers of such "watchlists" are often controllers under the GDPR, external processing of sensitive personal information may be a threat to citizens' right to privacy. The letter argues that entities are obliged to ensure the accuracy of processed personal data, and the use of third-party database providers does not exempt them from such an obligation. In general, since the importance of "watchlists" is undeniable, the European Data Protection Board believes that they should be regulated by law, especially in terms of data processing practices and responsibilities of both "watchlists" providers and entities, which seek their assistance.

4. Storage limitation

One of the most important issues raised by the European Data Protection Board is storage limitation. According to the Board's recommendation, AML-CFT should regulate both the maximum duration of data storage and types of data, which has to be stored in the first place. Following the principle of necessity and

proportionality, entities should store data related to potentially suspicious transactions longer than regular transactions.

5. Processing of special categories of personal data and processing of personal data relating to criminal convictions and offences

In general, it is forbidden to process special categories of personal data relating to criminal convictions and offenses, unless it is one of the exceptions provided by the GDPR. Article 9(2) (g) of the GDPR allows for such data processing only if it is in the substantial public interest and is done with the respect to basic data privacy rights as much as possible. The European Data Protection Board calls for a unified legal framework regarding such exceptions across all the EU and universal safeguards that would encourage data security.

6. Independent supervisory authorities

Given that any AML-CFT frameworks must comply with the GDPR, AML-CFT supervisory authorities and data protection authorities should collaborate to ensure legal compliance. The letter states that the European Commission and the European supervisory authorities would benefit from consulting the European Data Protection Board regarding their guidelines, delegated acts, and recommendations.

All things considered, Andrea Jelinek's, Chair of the European Data Protection Board, letter emphasizes the importance of personal data protection and collaboration between authorities required to create an effective legal framework for AML regulations. Principles illustrated in the letter center around the citizens' right to privacy and aim to strike a balance between innovation and fundamental human rights.

LEXcellence
Legal | Compliance | Regulatory

LEXcellence Statement
regarding
the European Data Protection Board issues recommendations regarding compliance between the new AML-CFT framework and the GDPR