edpb
European Data Protection Board

Letters

Ms Mairead McGuiness
European Commissioner for Financial services,
financail stability and Capital Markets Union

Mr Didier Reynders
European Commissioner for Justice
by e-mail only

Brussels, 19 May 2021
Ref: OUT2021-0088

Dear Commissioner McGuinness,
Dear Commissioner Reynders,

This letter follows the adoption by the EDPB, on 15 December 2020, of a Statement on the protection of personal data processed in relation with the prevention of the use of the financial system for the purposes of money laundering and terrorist financing[1], as well the adoption by the European Commission of an Action Plan[2] for a comprehensive Union policy on preventing money laundering and terrorist financing and the launch of a public consultation[3] in May 2020.

The Commission aims to present new legislative proposals in 2021, *inter alia*, establishing a single rulebook on these topics (i.e. a Regulation or a more detailed revised Directive), ensuring EU level supervision (either by granting new powers to an existing EU Agency or by establishing a new dedicated body), and creating a support and coordination mechanism for Financial Intelligence Units.

The core purpose and function of the AML Directives and their subsequent transposition into EU member state domestic laws are for…. *"the prevention of the use of the financial system for the purposes of money laundering or terrorist financing"*. It is important to keep this statement in mind when considering the data protection implications of AML laws, because the key method for monitoring AML is to follow the monetary transactions in order to detect suspicious money flows.

[1] Statement on the protection of personal data processed in relation with the prevention of the use of the financial system for the purposes of money laundering and terrorist financing, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf.
[2] Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 7 May 2020, available at https://ec.europa.eu/info/publications/200507-anti-money-laundering-terrorism-financing-action-plan_en.
[3] The consultation can be accessed at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12176-Action-Plan-on-anti-money-laundering/public-consultation.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Considering that the EDPB, and before it the Article 29 Working Party, has repeatedly noted the privacy and data protection challenges related to the AML-CFT framework[4], the EDPB wish to advise the Commission on this subject matter before the presentation of the legislative proposals, pursuant to Article 70 GDPR. Indeed, a fair balance has to be struck between the interest to prevent money laundering and terrorist financing, on the one hand, and the interests underlying the fundamental rights to data protection and privacy, on the other.

Furthermore, the EDPB recommends the Commission to include specific provisions in the upcoming legislative proposals in order to specify the application of the GDPR in the context of the AML-CFT legal framework, pursuant to Article 6 (3) of the GDPR. The EDPB notes that the current AML-CFT legislation already contains a provision on the purpose limitation principle[5], which effectivity is crucial and should be carefully assessed by authorities. To promote compliance and create more legal certainty for obliged entities, the EDPB recommends that the new AML-CFT instruments contain specific provisions with regard to the general conditions governing the lawfulness of processing by obliged entities and the personal data that is provided by third parties (see section 3 below); the types of data which are subject to the processing of personal data in the context of AML-CFT obligations; the data subjects concerned; the entities to, and the purposes for which the personal data may be disclosed; the specifications of storage periods, and processing operations and processing procedures, including measures to ensure lawful and fair processing.

Moreover, the EDPB recommends the inclusion in the legislative proposals of appropriate safeguards to ensure the respect of the data protection by design and by default obligations in the AML-CFT framework pursuant to Article 25 GDPR, including through techniques such as data avoidance (i.e. to avoid processing personal data altogether when this is possible for the relevant purpose), separation (i.e. to separate the processing of personal data as much as possible), abstraction (i.e. to limit as much as possible the detail in which personal data are processed) and security measures such as access restriction, obfuscation (i.e. to make data incomprehensible), encryption or dissociation of personal data (i.e. to break the link and the correlation between events, persons and data)[6].

Additionally, the EDPB recalls that the following personal data protection principles are of utmost, and equal, importance in the AML-CFT context. They should be taken into account, at each stage, to ensure that the anti-money laundering measures are compatible with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

1. Proportionality and efficient risk-based approach

[4] See for instance Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf.

[5] See Article 41(2) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[6] See EDPB Guidelines4/2019 on Article 25 Data Protection by Design and by Default, available at : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf. See also Jaap-Henk Hoepman, *Privacy design strategies*, January 27, 2020. pds-booklet.pdf (ru.nl)

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

The EDPB recalls that, pursuant to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union as interpreted by the case law of the European Union, the AML-CFT framework shall respect the principles of necessity and proportionality. It implies that different cases should be treated differently, proportionately to their relevant differences.

Pursuant to Article 52 of the Charter, any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others[7]. This means that legislative measures that limit the right to privacy and data protection have to be specific in order to correspond to objectives of general interest pursued and should not constitute disproportionate and unreasonable interference undermining the substance of those rights.[8]

The EDPB highlights that the GDPR is the general data protection framework, and does not contain sector specific data protection rules; therefore, for specific areas, it is important that the legislator lays down these specific data protection rules in the law in accordance with Article 6(3) of the GDPR.

Under the AML-CFT legislation, obliged entities must identify and report suspicious transactions, that is, the situations where the financial system could be used to launder the proceeds of crimes or to fund terrorist activity. This has proven difficult to do, as the standard for ensuring that the transaction is legitimate is based on a reasonable risk-based approach[9], which is a standard that is not clearly enough quantified or defined in legislation or through guidance from regulatory bodies. Consequently, the monitoring of financial transactions produces a large quantity of false positive alarms, where the transaction is not associated with money laundering or terrorist financing and therefore it is not reported to the FIU.

The Board therefore recommends that the specifics as to what the obliged entities should be monitoring should be clearly defined and guidance provided as to what exactly is required from a reasonable risk-based approach.

Furthermore, the EDPB recommends that the trigger events as to when further investigation should occur, should be distinct and clear so as, to avoid any disproportionate and therefore unlawful processing of personal data of any individual**.**

Moreover, the processing operations carried out by the AML officers of obliged entities, when suspicious financial or monetary transactions are detected and require further investigation as to the individuals concerned, should be accompanied by rigorous safeguards from a data protection perspective. It is important to state that it should not be a "*one size fits all*" approach as the scrutiny of an individual's financial movements should only really happen where there is suspicious transactions or activity occurring. Otherwise, if such close individual scrutiny occurred on all

[7] See also Article 23 GDPR and the EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR.
[8] See ECJ judgement of 13 April 2000, Case C-292/87, para. 45.
[9] See Article 18(2) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

individuals in the customer databases of obliged entities, there could be unnecessary and disproportionate processing of their personal data and probably not proportionate under data protection laws and possibly ultra vires to the legal requirements under AML-CFT.

Moreover, concerning Enhanced Due Diligence (EDD), it is important that obliged entities establish clear and transparent criteria of the individuals following into such category. Indeed, the EDD involves inter alia, the request and review by the obliged entity of extensive information about the individual falling within this process, as well as multiple person access to the data (i.e. before establishing a business relationship, approval from the obliged entity's senior manager is required in line with Article 19 of the AML D4). The Board therefore recommends that the parameters as to when EDD occurs are strict so as to avoid disproportionate and therefore excessive processing of personal data.

2. Data minimisation

Pursuant to the data minimization principle provided by Article 5(1) (c) of the GDPR, obliged entities must process only the personal data that are necessary to comply with the AML-CFT framework.

The EDPB therefore recommends that the AML-CFT legislation specify what is necessary and proportionate to comply with its obligations. From a data protection perspective, it is crucial to insert language in every AML obligation that clarifies whether the personal data necessary to comply with a specific obligation should (only) be collected from the data subject or whether other sources (e.g. third party) can/must be used (public / non-public). It is also necessary to specify whether or not and, if yes, which types of special categories of personal data and/or personal data relating to criminal convictions and offences can/must be processed to comply with that specific obligation.

Additionally, defensive behaviour of obliged entities – which leads them to send large quantities of non-material suspicions, generating a high number of false positive reports – should be avoided. The EDPB recommends that the new AML-CFT legislation explicitly contain requirements that only accurate and relevant data can be used for reports. These requirements should also specifically prohibit the inclusion of personal data relating to criminal convictions and offenses that are not connected to AML-CFT.

3. Data accuracy

The accuracy and reliability of data is an important aspect, not only from a data protection perspective as enshrined in Article 5(1) (d) of the GDPR, but also for the effectiveness of AML-CFT obligations. Therefore, the EDPB recommends that the AML-CFT legislation states that personal data processed by obliged entities shall be accurate, reliable, and up to date in order to comply with the AML-CFT obligations.

The EDPB observes that the applicable AML-CFT measures include very broad and far-reaching obligations on financial services providers and other obliged entities to identify and know their

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

customers, to monitor transactions undertaken using their services, and to report any suspicious transactions[10].

The Board therefore recommends to include a legal obligation in the coming legislative proposals for obliged entities to implement appropriate data protection policies with regard to the processing of personal data for AML-CFT purposes, within the meaning of Article 24(2) of the GDPR, as this would be appropriate and proportionate in relation to the processing activities that take place in this context, considering their nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The Board also recommends to specify that these policies shall include the collection of personal data from third parties whose services are used or the processing by third parties to whom certain processing activities are outsourced.

More specifically, obliged entities are increasingly dependent on external sources known as "watchlists", which are provided by third parties. These "watchlists" are commonly used by obliged entities to screen their databases and verify relevant information about their clients, in order to fulfil their legal obligations, and notably to assess the risk of the business relationship. The providers of these "watchlists" are in general controllers under the GDPR and do not fall under the current AML-CFT legislation. Nevertheless, the data processing performed in the context of these watchlists raise serious concerns, considering the quantity and sensitive nature of personal data they process which could lead to serious damage to the rights and freedoms of data subjects. Moreover, the fact that obliged entities make use of these databases provided by third parties does not exempt them from ensuring the accuracy of personal data that they process.

The EDPB therefore recommends to seize to create a specific legal framework for "watchlists" and, in particular, to clarify the responsibilities between obliged entities and the watchlists providers regarding GDPR obligations, to provide guarantees especially regarding the compilation of sensitive data, as well as to regulate the consultation of those lists by obliged entities and specify how data subject rights are respected in this context. .

4. Storage limitation

Pursuant to Article 5(1) (e) of the GDPR, all personal data processed for AML-CFT purposes must not be retained unnecessarily and indiscriminately. The EDPB therefore recommends that the AML-CFT legislation specify which personal data has to be retained and for how long, taking into account the necessity[11] and proportionality[12] principles. For instance, a distinction in the applicable storage period could be made between, on the one hand, data related to executed or intended transactions which

[10] See Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing, adopted on 15/12/2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf.

[11] See EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017.

[12] See EDPS, Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

have been deemed suspicious and reported to the financial intelligence unit and, on the other hand, data related to unsuspicious transactions.

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

Processing of special categories of personal data, within the meaning of Article 9 of the GDPR, and processing of personal data relating to criminal convictions and offenses, are prohibited except if one of the exceptions provided by the GDPR applies, or, in the case of personal data regarding criminal convictions and offences, the processing shall be laid down in specific legal provisions. In the AML-CFT context, the only applicable derogation to the processing of special categories of personal data is the one provided by Article 9(2) (g) of the GDPR, which allows such processing if it is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Similarly, Article 10 of the GDPR required that processing of personal data relating to criminal conviction and offences by obliged entities should be authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects

The EDPB noticed that there are currently wide differences between Member States laws regarding the provision of such derogations and safeguards. Therefore, the EDPB considers that there is a need for harmonization to enhance both the legal certainty and the EU citizens' right to data protection.

In addition, according to Articles 9(2) (g) any law allowing the processing of the special categories of personal data shall contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. According to Article 10 of the GDPR, personal data regarding criminal convictions and offenses, shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Therefore, the GDPR requires that the legislator specifies the general data protections principles of the GDPR into these new AML-CFT instruments. Indeed, appropriate and specific safeguards are necessary to comply with the GPDR. For instance, regarding the processing of personal data relating to criminal convictions and offenses, it could be provided that obliged entities should only be allowed to process criminal convictions and offences related to money laundering and terrorist financing handed down in countries where the rule of law, and especially the presumption of innocence, the right of defence and right of a fair trial are respected. Another appropriate safeguard could be to ensure the training and expertise of staff that deal with sensitive personal data in the context of AML-CFT obligations. All safeguards should be accompanied by serious corrective measures, including penalties, for the controller (obliged entity or FIU as the case may be) in case of non-compliance.

6. Independent supervisory authorities

To ensure the application of the data protection principles in the AML-CFT context, a cooperation between AML-CFT supervisory authorities and data protection authorities should be laid down in the texts. The EDPB therefore recommends to specify in the AML-CFT framework that the European Commission and the European supervisory authorities should consult the EDPB prior enacting

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

delegated act, guidelines or recommendations involving additional processing of personal data or affecting the right to data protection. Similarly, in those cases, the Member States AML-CFT competent authorities should consult the national data protection authorities.

Conclusion

To conclude, the EDPB urges the European Commission to propose specific provisions in the future AML-CFT legal framework in order to adapt the application of rules of the GDPR for obliged entities . If the AML-CFT legislation is not designed in a balanced and proportionate manner, that respects every individuals' fundamental rights to data protection, legal uncertainties for obliged entities will continue to exist and the AML-CFT framework would be vulnerable. Data Protection Authorities will be forced to use their powers in order to bring the activities of the obliged entities in accordance with the GDPR through corrective measures. European citizens will also likely exercise their right to an effective remedy before a tribunal, enshrined in the Article 47 of the Charter of Fundamental Rights of the European Union.

Thus, the EDPB deems crucial to correctly articulate the interplay between the two legal frameworks, since such articulation is necessary to ensure the compatibility between personal data protection and the prevention of money laundering and terrorist financing. When properly addressed, the data protection principles could, moreover, lead to more efficiency of the AML-CFT framework, excluding inaccurate personal data from processing operations.

Yours sincerely,

Andrea Jelinek

CC: Ms Raluca PRUNA, Head of Unit, Unit D.2, DG FISMA

Mr Olivier MICOL, Head of Unit, Unit C.3, DG JUST

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels