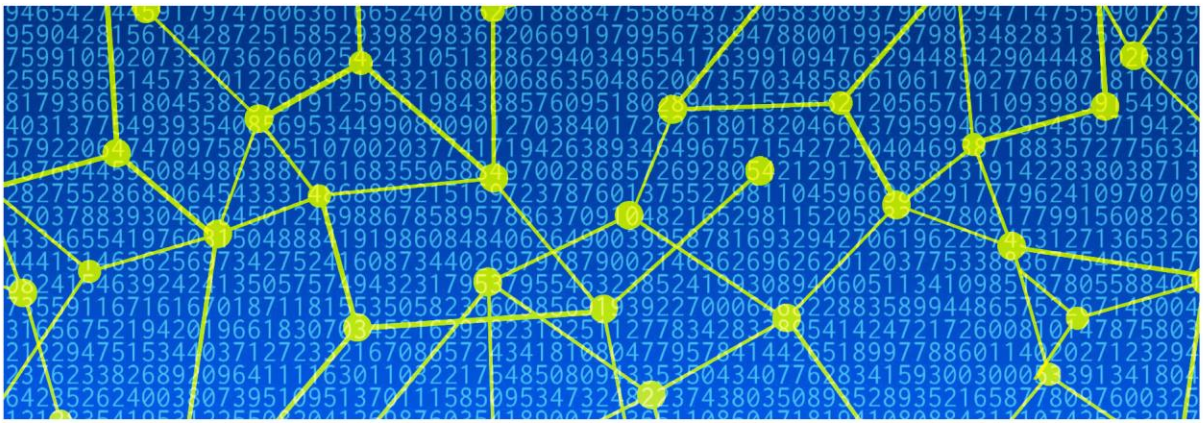

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2020

on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing

EDPS

23 July 2020

The European Data Protection Supervisor (EDPS) is an independent EU authority, its responsibilities are outlined under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 58(3)(c) of Regulation 2018/1725, the EDPS shall have the power 'to issue on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data'.

Wojciech Wiewiorówski was appointed as Supervisor on 5 December 2019 for a term of five years.

Executive Summary

On 7 May 2020, the Commission issued a Communication on an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (C(2020)2800 final) which sets a route map for the achievement of its objectives on this area. This Opinion assesses the data protection implications of the initiatives laid out in the Commission's Action Plan.

While the EDPS acknowledges the importance of the fight against money laundering and terrorism financing as an objective of general interest, we call for the legislation to strike a balance between the interference with the fundamental rights of privacy and personal data protection and the measures that are necessary to effectively achieve the general interest goals on AML/CFT (the principle of proportionality).

The EDPS recommends that the Commission monitors the effective implementation of the existing AML/CFT framework while ensuring that the GDPR and the data protection framework are respected and complied with. This is particularly relevant for the works on the interconnection of central bank account mechanisms and beneficial ownership registers that should be largely inspired by the principles of data minimisation, accuracy and privacy-by-design and by default.

The EDPS welcomes the envisaged harmonisation of the AML/CFT framework, as this will result in a more consistent application of the main rules by Member States as well as a uniform interpretation by the Court of Justice of the European Union. The EDPS invites the Commission to follow the risk-based approach when deciding on the new measures of the reinforced rulebook, since this approach is also in line with the data protection principles.

The EDPS recommends the Commission to foresee in its proposal bringing about the EU-Level AML/CFT supervisor a specific legal basis for it to process personal data as well as the necessary data protection safeguards in line with the GDPR and Regulation 2018/1725, particularly regarding information sharing and international transfers of data.

The EDPS welcomes the initiative of the Commission to boost the development of FIU.net and to find a suitable solution for its management that is in line with the GDPR and the data protection framework. Furthermore, we recommend that the proposal establishing the mechanism for the support and coordination of FIUs clarifies the conditions for access to and sharing of information on financial transactions by FIUs.

The EDPS supports the development of PPPs for the research and analysis of typologies and trends in AML/CFT, within the respect of the boundaries of the GDPR. To the contrary, and whether the EDPS does not wish to express any merit judgement on the policy purposes behind the initiative, we consider that PPPs for the sharing of operational information on intelligence suspects by law enforcement authorities to obliged entities, would result in a high risk for the rights to privacy and data protection. Furthermore, processing operations concerning information on possible offences arising from financial transactions should remain within the boundaries of competent authorities and not be shared with private entities.

The EDPS welcomes the Commission's efforts to play a stronger role within the Financial Action Task Force and to speak with one voice. He encourages the Commission to strive to make the data protection principles part and parcel of the AML/CFT processes, when setting up international standards in this area.

Finally, the EDPS expects to be consulted, in accordance with Article 42 of Regulation 2018/1725, following the adoption of proposals for legislative acts where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data. This may include, *inter alia,* the future proposals for a Regulation on AML/CFT measures, establishing a support and coordination mechanism for FIUs and setting up the EU-Level supervisor.

TABLE OF CONTENTS

1 Contents

1. INTRODUCTION AND BACKGROUND 6
2. GENERAL COMMENTS 7
   2.1. The principle of proportionality. Striking a balance between the protection of personal data and the fight against money laundering and terrorist financing 7
3. COMMENTS AND RECOMMENDATIONS 8
   3.1. First pillar: ensuring effective implementation of the existing eu aml/cft framework 8
   3.2. Second pillar: delivering a reinforced rulebook 9
   3.3. Third pillar: bringing about eu-level supervision 11
   3.4. Fourth pillar: establishing a coordination and support mechanism for fius 12
   3.5. Fifth pillar: enforcement of eu criminal law provisions and information exchange 13
   3.6. Sixth pillar strengthening the eu-s global role 15
4. CONCLUSIONS 16

Notes 16

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1],

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data[2], and in particular Article 58(3)(c) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. On 7 May 2020, the European Commission adopted its Communication on an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (C(2020)2800 final) (the "Action Plan"). The Action Plan is an initiative foreseen in the policy objective no 21 of the Commission Work Programme 2020 "Completing the Banking Union".
2. The Action Plan consist of six pillars, namely (1) ensuring the effective implementation of the existing EU framework for anti-money laundering and countering the financing of terrorism ("AML/CFT"), (2) establishing an EU single rule book on AML/CFT; (3) bringing about EU level AML/CFT supervision, (4) establishing a support and cooperation mechanism for FIUs, (5) enforcing Union-level criminal law provisions and information exchange and (6) strengthening the international dimension of the EU AML/CFT framework. To gather the views of citizens and stakeholders on these measures, on 7 May, the Commission launched a public consultation[3] in parallel with the adoption of the Action Plan until 29 July 2020.
3. The Action Plan concretises the pillars into a number of specific measures, including various legislative proposals concerning the EU AML/CFT single rulebook, establishing an EU level AML/CFT supervisor and developping a support and coordination mechanism for Financial Intelligence Units ("FIUs"). This Opinion follows the six pillars' structure and expresses the views of the EDPS on selected measures of the Action Plan, and in particular, on their potential interference with the right to privacy and to data protection of individuals as guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. This Opinion is without prejudice to the obligation of the Commission to consult the EDPS, in accordance with Article 42 of Regulation 2018/1725, on any legislative proposals that may be proposed within the framework of the Action Plan where there is an impact on the protection of individuals' right to the protection of personal data.

2. GENERAL COMMENTS

2.1. The principle of proportionality. Striking a balance between the protection of personal data and the fight against money laundering and terrorist financing

4. The EDPS recognises the importance of establishing a strong framework and putting in place suitable and effective structures that are endowed with the necessary technological means to develop their tasks relating to the fight against money laundering and terrorism financing. However, the achievement of these legitimate and important goals should not be at the expense of the protection of the privacy and personal data rights of individuals, which remain fully applicable. Indeed, data protection requirements should be perceived as a basic requirement which should be complied with in the context of anti-money laundering obligations.

5. The case law of the European Court of Justice has confirmed that the fight against serious crime constitutes an objective of general interest[4] which may justify interference with the fundamental rights to privacy and data protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. At the same time, the EU legislature's discretion is reduced, and the legislation must strike a balance between the interference that is really necessary, and the right to privacy and personal data of individuals (**proportionality**). For more guidance on the principle of proportionality in the context of data protection, we draw attention to the **EDPS Necessity Toolkit**[5], as well as our **Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data**[6]**.**

6. Concerning the EU legislative framework for AML/CFT, it has rapidly evolved and expanded during the last years. Major steps were introduced by the 4th and the 5th Anti-Money Laundering Directives (hereafter, the "**AML D4**" and the "**AML D5**" respectively), and will continue with the transposition of the 6th Anti-Money Laundering Directive[7] (the "**AML D6**") by 2021[8]. The EDPS welcomes key changes of the AML D6 that are in line with the right to privacy and the protection of personal data, such as the obligation of investigating or prosecuting authorities to use targeted investigative tools, to follow a risk-based approach[9] (i.e. less risky situations justify less intrusive procedures) and to take into account the principle of proportionality and the nature and seriousness of the offences under investigation[10].

7. The EDPS has provided advice during these legislative developments and issued specific recommendations in our opinions of 2013[11] and 2017[12] (hereafter "**2013 Opinion on the draft AML D4**" and "**Opinion 1/2017**" respectively), aimed at ensuring that data protection safeguards were duly considered in the proposals for the AML D4 and the AML D5.

8. In particular, in our 2013 Opinion on the draft AML D4, we insisted on the need to respect **data protection safeguards,** especially in the context of **customer due diligence** (CDD) processes. We recalled that the sole purpose of the processing of data under the AML Directives must be the prevention of money laundering and terrorist financing, and that **data must not be further processed for other incompatible purposes** by obliged entities (e.g. commercial or marketing purposes), as well as by public authorities.

9. Moreover, we insisted on the need to respect the **necessity and proportionality principles** when limiting data subjects´ rights and when making administrative sanctions publicly available, and recommended evaluating alternative and less intrusive options to the general **publication** obligation. Lastly, we insisted on the need to issue **rules listing specifically which of the beneficial owners' identification data** should be processed by the central

beneficiary ownership registers. In this respect , Article 30(5) AML D4 now specifies that these registers process personal data including at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner, as well as the nature and extent of the beneficial interest held.

10. In the Opinion 1/2017, we expressed a number of concerns relating to the respect of the **principles of purpose limitation and proportionality** by the amendments introduced by the AML D5. In particular, we pointed at deficiencies in the proposed legislation in connection with the insufficient safeguards to avoid that personal data collected for the purpose of AML/CFT are used for other purposes, such as countering **tax evasion** or enhancing corporate transparency. Moreover, we recommended to ensure a proper assessment of the **proportionality of the policy measures proposed in relation to the purposes sought**, particularly with regard to the application of the risk-based approach, the broader access to information on financial transactions by FIUs, and the broadening of the access to beneficial ownership information to both competent authorities and the public. For the latter, we recommended to design a limited access only for the entities in charge of enforcing the law.

3. COMMENTS AND RECOMMENDATIONS

3.1. First Pillar: Ensuring effective implementation of the existing EU AML/CFT framework

11. The EDPS agrees with the Action Plan that, among the Commission's initiatives to fight money laundering and financing of terrorism, the first priority should be to ensure rigorous and effective **implementation** of the existing EU AML/CFT rules by Member States. This also includes full compliance with the data protection framework in the implementation of such AML/CFT measures.

12. Among the envisaged measures, **the setting up of central bank account mechanisms and beneficial ownership registers** have special relevance from a data protection perspective, since they aim for the the interconnection of databases with a high amount of personal data (e.g. name, date of birth, nationality, country of residence, bank account number, etc.). Therefore, the EDPS welcomes the Commission's commitment to closely monitor the setting up of these central registers to ensure that they are populated with high-quality data[13] and the most up-to-date possible, as this is in line with the principle of accuracy set by Article 5(1)(d) of the GDPR.

13. Pursuant to the AML D5, the central bank account mechanisms must be set up by 10 September 2020[14]. These are **centralised automated mechanisms**, such as central registries or central electronic data retrieval systems, which allow the identification of natural or legal persons holding or controlling payment accounts and bank accounts, and safe-deposit boxes held by a credit institution[15].

14. The Commission's report to the European Parliament and the Council on the interconnection of national centralised automated mechanisms of the Member States on bank accounts[16] concluded that the **interconnection of these mechanisms** is possible. The EDPS welcomes that in this report, which assesses various IT solutions at EU level which may serve as models for the interconnection of these centralised mechanisms, the Commission takes into account the data protection principles and highlights the need to restrict the scope of the information accessible through the interconnection platform to the minimum required (**data minimization**) and to keep the proportionality between the scope of access to personal data

and what is necessary to comply with the objectives of the AML Directive (**proportionality principle**).[17]

15. Moreover, the Action Plan notes that there is ongoing work on the interconnection of **central registers of beneficial ownership** for corporate and other legal entities, which shall be interconnected via the European Central Platform[18] by 10 March 2021[19]. The EDPS recalls that these registers, which are accessible to obliged entities within the framework of CDD processes, process the personal data of beneficial owners, including at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner, as well as the nature and extent of the beneficial interest held[20]. Therefore, it is of particular importance that these registers are kept up to date and that every reasonable step is taken to ensure that any inaccurate personal data are erased or rectified without delay, in line with Article 5(1)(d) of the GDPR. This has also been emphasised by the Parliament in its recent resolution on the Action Plan (2020/2686(RSP) which calls on the Commission to address the lack of sufficient and accurate data in the national registers of beneficial ownership, and demands that verification mechanisms related to data accuracy are put in place to ensure that the registers function properly and provide public access to high-quality data[21].

16. While works are still ongoing on the interconnection of both national centralised automated mechanisms and the central registers of beneficial ownership, the EDPS welcomes that the Action Plan highlights the importance of **following the data protection principles in relation to the interconnection of these mechanisms.** Indeed, since this interconnection will provide access to centralised registries to public authorities of different nature, both law enforcement authorities and FIUs, it is important that the interconnection works strive to embed in the mechanisms the principles of data protection by design and data protection by default in accordance with Article 25 of the GDPR, and that strong data protection safeguards are established, particularly concerning access rights and the accuracy of data. On this point, the EDPS draws attention to Opinion 5/2018 on privacy by design[22], which provides examples of **methodologies to identify privacy and data protection requirements and integrate them into privacy engineering processes** in view of implementing appropriate technological and organisational safeguards. Moreover, we suggest that the interconnection works consider the recommendations provided in our Opinion on the Proposal for a Directive of the European Parliament and of the Council amending Directives 89/666/EEC, 2005/56/EC and 2009/101/EC on the interconnection of central, commercial and companies' registers[23]. In particular, we draw attention to our earlier recommendations relating to the **governance of the network, the roles, competences, and responsibilities** of the stakeholders involved, as well as those concerning the data protection safeguards for **the transfers of personal data to third countries.** Finally, precise guidance for the establishment of a solid IT governance and IT management of these interconnected databases is provided in the EDPS Guidelines on the protection of personal data in IT governance and IT management of EU institutions[24].

3.2. Second Pillar: Delivering a reinforced rulebook

17. The EDPS agrees that the fight against money laundering would significantly benefit from the harmonisation of AML/CFT rules, through the adoption of a Regulation that ensures direct application of the main rules, as well as their uniform interpretation by the Court of Justice of the European Union. We would therefore welcome further harmonisation of these rules at EU level which would have a beneficial impact not only for the fight against money laundering and countering terrorism, but also to enhance and streamline data protection safeguards at European level in this area.

18. To this end, the Action Plan suggests a number of important topics that may be covered by a future Regulation, such as the list of obliged entities, customer due diligence requirements, internal controls, reporting obligations, provisions on beneficial ownership registers and central bank account mechanisms. As mentioned before, these are areas with a significant impact on the right to data protection and privacy because they involve the processing of a substantial amount of personal data.

19. The EDPS welcomes that the Commission intends to follow a **risk -based approach to the new measures of the reinforced rulebook,** consisting on applying less intrusive procedures to less risky situations. This approach is in line with the data protection principles and in particular, with the need to assess the necessity and the proportionality of the legislative measures, in view of the impact of such measures on the rights to privacy and personal data. For guidance on this topic, we recommend the consultation of our **Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data**[25].

20. The EDPS has already highlighted, in the past, the importance of establishing clear safeguards to guarantee compliance with the **right of information within Customer Due Diligence** (CDD) **processes**[26]. In particular, we had recommended safeguards, which were inserted in the AML D4, to guarantee that when data is collected, the customer is informed about the purpose(s) for which data is required and processed. This is important as, for instance, data necessary to establish the business relationship will be collected and used at the same time for commercial purposes (i.e. customer identity verification) and CDD purposes (i.e. AML). In this regard, Article 41(3) AML D4 requires that "*obliged entities shall provide new clients with the information required pursuant to Article 10 of Directive 95/46/EC before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of obliged entities under this Directive to process personal data for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 of this Directive*". These recommendations are still valid today under the GDPR and we encourage the Commission to take them into account, also in the context of the preparation of future provisions.

21. In our 2013 Opinion on the draft AML D4, we also recommended that the legislator clarifies the type of information that should be taken into account in normal and also in enhanced CDD (for politically exposed persons and related persons) and for the purposes of performing risk assessments in order to prevent arbitrary decisions and discriminations, as well as to ensure the respect of the **principle of data minimisation**. In this regard, CDD processes involve today, the processing of data relating to the customer's identity, beneficial ownership of legal entities, purpose and intended nature of the business relationship, and scrutiny of transactions including, when necessary, the source of funds[27]. For politically exposed persons, family members or persons known to be close associates, the enhanced CDD also requires that the business relationship is approved by senior management of the obliged entity, that adequate measures to establish the source of wealth and source of funds are taken, and the enhanced, ongoing monitoring of the business relationship[28]. Therefore, obliged entities, when collecting and processing customer's data in CDD processes, should make sure that all the personal **data requested are adequate, relevant and limited to strictly necessary** in relation to the purposes of CDD.

22. The CDD processes should also include data protection safeguards in line with the GDPR to ensure, for instance, that individuals within the Know-Your-Customer scope **are not subject to decisions based on personal data that should either not have been collected or/and are**

not necessary for the establishment of the business relationship, or that have been **re-used for other incompatible purpose**. Moreover, CDD provisions should also take into account and be aligned with the limits of the automated individual decision-making, including profiling, set by Article 22 of the GDPR, particularly when these CDD processes might result in the issuing of a Suspicions Activity Report (SAR) on the client's activity.

23. We note that with the development of the digitalisation in all spheres of life, CDD processes for customer identification and identity verification might take place online (remotely) in the future. In such a case, the EDPS highlights that **CDD digitalisation** must be accompanied by the adoption of the necessary measures to ensure the **security of personal data**, and in particular measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage (integrity and confidentiality). Moreover, the digitalisation of CDD processes should be underpinned by the **data protection-by-design principle** in a way that from the outset, such digitalisation facilitates the exercise of personal data rights. Finally, the EDPS recalls that following the entry into force of the GDPR, all entities must ensure that they are able to demonstrate compliance with data protection obligations (**accountability principle**). As a result, obliged entities, as controllers, in CDD processes must maintain a record of processing activities under their responsibility, and have such information available to the data protection supervisory authority at their request.

24. Finally, the Action Plan advocates for a broader scope of the European AML legislation to address the implications of technological innovation and developments of international standards. The EDPS welcomes the explicit reference to the need for **new technological solutions which might help improve the detection of suspicious transactions and activities in compliance with data protection rules**, and recommends that these solutions follow the principles of data protection by design and data protection by default, in line with the EDPS Opinion 5/2018 on privacy by design.

3.3. Third Pillar: Bringing about EU-Level Supervision

25. The Commission envisages, in the Action Plan, the creation of an **integrated AML/CFT supervisory system at EU level** that ensures consistent high-quality application of the AML/CFT rulebook throughout the EU and also promotes efficient cooperation between all relevant competent authorities.

26. As the Action Plan puts forward, the powers of the EU-Level AML/CFT supervisor, either in exclusive or joint responsibility with national supervisors, may imply its ability to review the documentation on transactions and customers, in order to ensure the proper implementation of internal policies by supervised entities[29]. The EDPS insists on the importance that the future legislative proposal setting up the EU-Level AML/CFT supervisor includes a clear **legal basis concerning the processing of personal data and** stating the purposes and the limits of such processing, in line with Article 5(1) of Regulation 2018/1725.

27. This supervision will also likely involve cooperation at two levels: on the one hand, a **multi-Member State** cooperation involving cross-border information sharing; on the other hand, **different authorities** of the same or various Member States, including financial and prudential supervision authorities at an early stage, and investigative and law enforcement authorities later on. **The EDPS recommends that the legal instrument** creating the EU-Level AML/CFT supervisor **already foresees specific rules on information sharing and dissemination that take into account the necessary data protection safeguards.**

28. When the functions and powers of the future EU-Level AML/CFT supervisor foresee the possible cooperation of the new authority with third countries or international organisations, the founding act should also introduce **specific provisions on the conditions for international transfers of operational personal data**, and in particular on the transfers by way of appropriate safeguards and derogations for specific situations[30]. The EDPS recalls that these provisions must respect the conditions of Articles 46 to 51 and Article 94 of Regulation 2018/1725, and be subject to appropriate data protection safeguards.

3.4. Fourth Pillar: Establishing a coordination and support mechanism for FIUs

29. A **strong and effective coordination mechanism between FIUs**, which are considered the "hubs of financial intelligence"[31], is a crucial element of the fight against money laundering, since illicit activities usually involve cross-border and/or cross-institution transactions. However, joint analysis of those activities and relevant factors by Member States' FIUs and other public authorities remains limited. As a result, in practice there may be legislative and operational loopholes, of which malicious actors may take advantage of to commit illicit acts relating to money laundering and financing of terrorism.

30. Cross-border coordination requires the use of **tailored and effective tools and procedures** that facilitate the information sharing and data matching, but at the same time are fully compliant with data protection requirements. In this respect, as pointed out earlier, data protection needs to be understood as part and parcel of the complex analytical process for the prevention and detection of money laundering and other illicit activities, and not as an obstacle to it.

FIU.net

31. For nearly 20 years, the cooperation between FIUs in the European Union has been facilitated by a network for information exchange (the so-called **FIU.net**[32]). In its Communication "*Towards better implementation of the EU/s anti-money laundering and countering the financing of terrorism framework*", the Commission acknowledges that there are, still today, recurrent technical difficulties in the functioning of the FIU.net tool, which have made it more cumbersome for FIUs to share information and thus, have resulted in lesser information exchange and data matching between them[33]. Moreover, the report points out the lack of regulation on exchanges of information between Member States' FIUs and FIUs of third countries which has led to a non-harmonised approach to such exchanges. These legal and practical obstacles inevitably have an impact on the accuracy and up-to-date information of FIU.net and thus constitute a risk for the protection of the rights to privacy and personal data.

32. In order to mitigate these problems, the Action Plan echoes the urgent need to invest in the development of FIU.net, as well as finding a suitable solution for its management.

33. Concerning the future of FIU.net[34], the Commission has pointed to the future EU-Level AML/CFT supervisor as the potential **host entity of the network**, together with other possible solutions, for example, **strengthening the mandate** of Europol to provide them with a legal basis for hosting the network[35]. In case a solution is not in place by the end of 2020, the Commission has expressed its intention to provisionally take over the management of the FIU.net, in order to ensure the continuous and uninterrupted functioning of the system.

34. Although the role of the Commission as host of FIU.net still needs to be determined from a data protection perspective (i.e. controller, joint controller, processor), the EDPS recalls that a valid legal basis is necessary to process the personal data shared through the network. In this regard, we note that Article 51 AML D4 provides that "***the Commission may lend such***

assistance *as may be needed to facilitate coordination,* ***including the exchange of information between FIUs within the Union****".* Without prejudice to further analysis, and although not explicitly referring to personal data processing, this provision would appear to provide a certain basis for the management of **FIU.net,** as the processing of personal data would normally be considered necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Commission (see Article 6 of the GDPR and Article 5 of Regulation 2018/1725).

The FIUs support and coordination mechanism

35. Regarding the support and coordination mechanism for FIUs more broadly, **the EDPS notes that FIUs in the different Member States follow different institutional models and have, as a result, heterogeneous powers.** There are, on the one hand , **administrative** FIUs that carry out the analysis of suspicious activity reports and transmit these to the law enforcement authorities for investigation when there are indicia that the reported transaction could be constitutive of an offence. On the other hand, there are **law enforcement** FIUs with embedded investigative competencies with regard to AML/CFT. And there are hybrids of both models, with different powers. As the Commission indicated in its Report assessing the framework on FIUs[36], the FIUs' different status, powers, and organisation continue to **affect their ability to access and share** relevant information. From a data protection perspective, such distortions resulting from the different nature of the FIUs pose a serious risk that the purpose limitation principle is not respected in the managing and sharing of information.
36. Furthermore, the EDPS recalls that Recital 56 of the AML D4 states that the exchange of information between FIUs relating to money laundering or terrorist financing **for analytical purposes, which is not further processed or disseminated,** should be permitted unless such exchange of information is contrary to fundamental principles of national law**.** Therefore, the EDPS recommends that the legislative proposal envisaged by the Commission, establishing a support and coordination mechanism for FIUs, already foresees provisions setting **explicit and clear conditions for access to and sharing of information on financial transactions by Member States FIUs**. Moreover, as we already indicated in our Opinion 1/2017, we consider more in line with the principles of proportionality and purpose limitation a legal configuration of the powers of FIUs as "investigation-based" rather than "intelligence-based", where FIUs' may request information to obliged entities for their own analysis and intelligence, without a prior reporting of suspicious transactions[37]. As we highlighted in the said opinion, the latter approach would be more similar to data mining than to a targeted investigation, thus impacting personal data rights.

3.5. Fifth Pillar: Enforcement of EU criminal law provisions and information exchange

37. Concerning the call for enhanced coordination in financial intelligence matters between law enforcement authorities and the Member States' FIUs in the Action Plan, and taking into account their different nature and scope of powers (administrative and criminal/law enforcement roles), the EDPS would like to highlight that **such coordination and data exchange must comply at all times with the data protection framework.** Moreover, the technological means used for the sharing of information between these authorities should include appropriate technical and organisational measures, to protect data against accidental or unlawful destruction, accidental loss, alteration or unlawful disclosure, including encryption and anonymization.

38. In the Action Plan, the Commission encourages the use of public-private partnerships (PPPs) in financial intelligence matters, essentially in two forms: (1) exchanges of information on **typologies and trends** by FIUs and law enforcement to obliged entities; and (2) sharing of **operational information on intelligence suspects** by law enforcement authorities to obliged entities for the purposes of monitoring the transactions of these suspects. This initiative is in line with the Financial Action Task Force ("**FATF**") position in the last years, advocating for a more active role of PPPs in financial intelligence for the purposes of safeguarding the integrity of the international financial system[38].

39. Concerning **the first type of PPPs**, **the EDPS welcomes and supports the idea of joint efforts between law enforcement authorities, FIUs and the private sector** for structuring policy debates, discussion forums, and for research and analysis of typologies and trends in AML/CFT. We recall that PPPs have been successfully used in similar areas such as cybersecurity, high performance computing, robotics or future internet technologies[39], where data protection requirements have shaped the exchanges of information and have been integrated into the research processes, without raising particular concerns for their implementation.

40. The EDPS welcomes the Parliament's resolution on the Action Plan[40], in which it expressly supports PPPs in the form of tripartite platform, and highlights the obligation for these type of PPPs to work within the strict respect of the limits of applicable data protection rules and fundamental rights. Moreover, the EDPS joins the Parliament's call on the Commission **to propose a clear legal framework for these platforms**, which also ensures compliance with the rules for the exchange of information and data protection.

41. With regard to the constitution of PPPs for the sharing of **operational information on intelligence suspects by law enforcement authorities to obliged entities**, and while the EDPS does not express any merit judgement on the policy purposes behind them, **we are concerned that such policy choice would lead to a high risk for the individuals' rights to privacy** and data protection.

42. The EDPS recalls that in our Opinion 1/2017, we highlighted that the AML framework reserves the investigation and enforcement of criminal activities to the competent authorities. Under no circumstances, a private subject is, either formally or informally, directly or indirectly, entrusted with an enforcement role[41]. Thus, the creation of PPPs aiming to allow private entities (i.e. the obliged entities) to monitor subjects (who are at the same time their clients) on the basis of up-to-date operational information still under investigation by law enforcement authorities, would create, in our view, a very risky precedent from a data protection perspective.

43. Pursuant to the AML framework, the role of obliged entities is limited to the reporting of suspicious activities to FIUs through the so-called suspicious activity reports. This role is unidirectional, and obliged entities receive no feedback from FIUs or law enforcement authorities on the analysis or the course of the information reported. This is, from a data protection point of view, a safeguard for the privacy of individuals, as the obliged entities are not involved in any processing operation concerning information on possible offences arising from the suspicious transactions reported, and which, due to their sensitive nature, should be limited to public authorities only, given their impact on the fundamental rights of the concerned individuals.

44. Without prejudice to evidence that might be put forward in the future, the EDPS considers that there are currently no compelling reasons to justify granting private subjects access to the sensitive personal data of individuals concerning criminal activities and offences under

investigation, as this is and should remain in the exclusive hands of the relevant public authorities. Furthermore, the EDPS recalls that, for a measure to meet the principle of proportionality as enshrined in Article 52(1) of the Charter, the advantages resulting from such measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of the fundamental rights. In this regard, we consider that a measure granting private subjects the powers of monitoring suspects would meet with great difficulty the proportionality and necessity test and that first, other options for achieving the same goal which are less intrusive should be explored[42].

45. Secondly, the sharing of sensitive data of "suspects" with the private sector which may also have those individuals as clients, raises concerns from a conflict of interest perspective. In particular, the EDPS is concerned that PPPs created for the sharing of **operational information on intelligence suspects** might not enjoy the necessary independence and autonomy, since the obliged entities would be required to monitor their own clients, towards whom they bear a duty of confidentiality within the framework of their business relationship.

46. Thirdly, the EDPS is concerned that the constitution of this type of PPPs may create issues in connection to the **principle of purpose limitation**, pursuant to which personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes. In particular, obliged entities participating in PPPs might be tempted to integrate the information shared by law enforcement authorities through this platform **in their global databases, so as to re-use it later,** as part of their customer profiles[43]. This could lead to discrimination against certain clients, for instance, those offering low profitability for the bank and presenting a significant level of risk, conceivably resulting in the financial exclusion of vulnerable individuals and communities (the so-called "de-risking" of financial entities whereby relationships with clients that may pose risks are terminated or restricted)[44].

47. Indeed, the difficult fit and the concerns arising from the involvement of PPPs in financial intelligence tasks is evidenced by the few countries in the world that have chosen this model[45], with a precedent in the EU, only in a former Member State[46]. Moreover, the few existing ones seem to be information sharing parnterships at national-level, with no cross-border exchanges on financial intelligence and a small number of participants.

3.6. Sixth Pillar Strengthening the EU's global role

48. The EDPS welcomes the ambition of the Commission to play a stronger role within the works of the FAFT and in setting international standards on AML/CFT. In this context, we encourage the Commission to strive to embed the EU data protection principles within the AML/CFT compliance processes, as a safeguard for the fundamental rights of individuals. Following the adoption of the GDPR, the EU has demonstrated its capacity to impact the legal systems of third countries and raise their data protection standards. We believe that it should continue to do so, for instance, when discussing AML/CFT international standards on CDD processes, record-keeping or suspicious activity reports, where the information rights of individuals whose data will be processed and the principles of data minimisation and accuracy are of major importance.

49. Moreover, the EDPS welcomes the new methodology on the assessment of high-risk countries (SWD (2020) 99)[47] which has been published in parallel with the Action Plan. This methodology is based on the criteria listed in Article 9 of AML D4, and its assessment of high-risk countries should be in line with the elements highlighted in this Opinion.

4. CONCLUSIONS

In light of the above, the EDPS makes the following recommendations:

- Invites the Commission, in the legislative works, to strike a balance between the measures that are necessary to effectively achieve the general interest goals on AML/CFT and their interference with the fundamental rights of privacy and personal data protection;
- Recommends that the Commission monitors the implementation of the existing AML/CFT framework while ensuring the respect of the GDPR and the data protection framework;
- Concerning the works on the interconnection of central bank account mechanisms and beneficial ownership registers, recommends that they comply, in particular, with the principles of data minimisation, accuracy and data protection-by-design and by default;
- Suggests that the Commission keeps a risk based approach to the new AML/CFT measures of the reinforced rulebook, i.e. by applying less intrusive procedures to less risky situations, as this is also in line with the data protection principles;
- Concerning Customer Due Diligence, recommends that safeguards are maintained in the proposed legislation to guarantee the right of customers to be informed when their data is collected, and about the purpose(s) for which data is required and will be processed, as well as to ensure compliance with the principles of data minimisation, purpose limitation and data protection-by-design, and the limits of the automated individual decision-making;
- Recommends the Commission to provide in its forthcoming proposal to set up an EU-Level AML/CFT Supervisor for a legal basis for the processing of personal data as well as the necessary data protection safeguards in line with the GDPR and Regulation 2018/1725, particularly regarding the information sharing and international transfers of data;
- Recommends the Commission to clarify in the proposal for the mechanism for support and coordination of FIUs, the conditions for access to and sharing of information on financial transactions by FIUs;
- Supports the development of PPPs for the research and analysis of typologies and trends in AML/CFT, within the respect of the boundaries of the GDPR;
- Encourages the Commission to integrate data protection principles, when setting up international standards at the Financial Action Task Force.

Brussels, 23 July 2020

Wojciech WIEWIÓROWSKI
(e-signed)

NOTES

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), L119 of 4.5.2016.

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, L 295, 21.11.2018.

[3]https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12176-Action-Plan-on-anti-money-laundering/public-consultation

[4] Digital Rights Ireland case (2014)

[5] https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf

[6] https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

[7] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018

on combating money laundering by criminal law

[8] Member States are required to transpose the AMLD 6 into national law by 3 December 2020, after which, firms within Member States will have to implement the relevant regulations by 3 June 2021.

[9] Recitals 22 and 33 of the AML D4 state that "*The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, risk- based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively. Underpinning the risk-based approach is the need for Member States and the Union to identify, understand and mitigate the risks of money laundering and terrorist financing that they face*" [...].

[10] See Recital 19 of AML D6

[11] https://edps.europa.eu/sites/edp/files/publication/13-07-04_money_laundering_en.pdf

[12] https://edps.europa.eu/sites/edp/files/publication/17-02-02_opinion_aml_en.pdf

[13] See Action Plan, page 4

[14] See Recital 53 AML D5

[15] See Article 1(19) of AML D5, inserting Article 32a and 32b into AML D4

[16]Available at
https://ec.europa.eu/info/sites/info/files/report_assessing_the_conditions_and_the_technical_specifications_and_procedures_for_ensuring_secure_and_efficient_interconnection_of_central_bank_account_registers_and_data_retrieval_systems.pdf

[17] See page 6 of the report

[18] Article 30(10) of AML D4, as amended by AML D5

[19] Recital 53 AML D5

[20] Article 30(5) AML D4

[21] European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments (2020/2686(RSP)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0204_EN.html

[22] See https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2011.220.01.0001.01.ENG&toc=OJ:C:2011:220:TOC

[24] https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf

[25] See endnote 6

[26] See EDPS 2013 Opinion on the draft AML D4, para 13

[27] See Article 13 of AML D4

[28] See Articles 20-23 AML D4

[29] See page 8 of Action Plan

[30] See Article 94 Regulation 2018/1725

[31] See EP report "Anti-money laundering - reinforcing the supervisory and regulatory framework".

[32] FIU.net is a decentralised and sophisticated computer network supporting the Financial Intelligence Units (FIUs) in the European Union in their fight against money laundering and the financing of terrorism. It became operational in 2002 (under Council Decision 2000/642/JHA of 17 October 2004) and was subsequently referred to Directive 2005/60/EC (AML D3) and in the current AML D4 as a tool of information exchange between FIUs. Since January 2016, FIU.net is incorporated into Europol.

[33] See Communication from the Commission to the European Parliament and the Council "Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework". COM/2019/360 final.

[34] In December 2019, the EDPS found that the embedment of FIU.Net into Europol's systems (SIENA) breached the provisions governing the processing of personal data due to the restrictions of the Europol Regulation on the categories of individuals about whom Europol can process personal data. In particular, to comply with the rules, individuals involved in suspicious transactions would have to be considered as suspects, something that could not be consistently ensured by Europol considering all types of information and personal data shared through FIU.net. In our opinion, we concluded that the technical administration of FIU.net by Europol was in breach of the Europol Regulation. However, taking into account the importance of FIU.net in the fight against money laundering and terrorism financing at EU level, we suspended the ban until 19 December 2020, in order to allow time for the smooth transition of the technical administration of FIU.net to another entity.

[35] See point 33 in the adjusted Commission´s Work Programme, available here https://ec.europa.eu/info/sites/info/files/cwp-2020-adjusted-annexes_en.pdf

[36] https://ec.europa.eu/info/sites/info/files/report_assessing_the_framework_for_financial_intelligence_units_fius_cooperation_with_third_countries_and_obstacles_and_opportunities_to_enhance_cooperation_between_financial_intelligence_units_with.pdf

[37] See EDPS Opinion 1/2017, para 52

[38] See https://www.fatf-gafi.org/publications/fatfgeneral/documents/public-private-sector-partnership.html

[39] https://ec.europa.eu/digital-single-market/en/public-private-partnerships

[40] See endnote 19.

[41] See Opinion 2017, paragraph 16

[42] See EDPS Necessity Toolkit, available https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf

[43] Tsingou, E. Global financial governance and the developing anti-money laundering regime: What lessons for International Political Economy?. Int Polit 47, 617–637 (2010). https://doi.org/10.1057/ip.2010.32

[44] See https://www.fatf-gafi.org/publications/fatfgeneral/documents/public-private-sector-partnership.html

[45] https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwwell_artingstall_web_4.2.pdf

[46] The experience of PPPs in financial intelligence in the European Union was limited to the UK's Joint Money Laundering Intelligence Taskforce (the "JMLIT"). The JMLIT has a threefold structure: (1) An operational Group for the sharing of operational-level activity information between the financial sector, law enforcement agencies and the Financial Conduct Authority; (2) various Expert Working Groups that identify and assess new and emerging money-laundering and terrorist-financing threats and provide knowledge products such as typologies and red-flag indicators; and (3) an Alerts Service for the wider dissemination of assessments and typologies, which is provided by UK Finance.

[47]https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology_en.pdf