17 October 2022 TPD(2021)8rev4

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Draft guidelines on data protection for the processing of personal data for Anti-Money Laundering/Countering Financing of Terrorism purposes

Section I. Data protection rules and principles

1. Introduction

1.1. Background

Money Laundering and Financing of Terrorism (ML/FT) are criminal phenomena frequently involving cross-border schemes and the abuse of financial and non-financial institutions and entities across multiple jurisdictions. Data sharing between state and non-state actors is crucial in order to effectively combat ML/FT. The anti-money laundering/countering financing of terrorism (AML/CFT) framework[1] aims at preventing, investigating, and prosecuting ML/TF crimes through a system of measures implemented by multiple stakeholders, notably obliged entities (OE) and their customers, financial intelligence units (FIUs), supervisory and law enforcement authorities (LEAs), prosecution authorities, judicial systems, customs agencies and policy makers at various levels in the government.

These operations must be considered both by states Parties and possibly by others in the light of applicable data protection frameworks such as Convention 108+ as illustrated in the following sections.

Processing of personal data for such purposes may constitute an interference with the data subject's right to respect for private life, as protected by international human rights instruments (such as Article 12 of the UNDHR, Article 17 of the IPPCR and Article 8 of the ECHR). According to Article 11 of the modernised Convention 108 lawful exceptions and restrictions with this right can only be carried out for a legitimate purpose of a public interest if they (i) are provided for by law, (ii) respect the essence of the fundamental rights and freedoms and (iii) are necessary and proportionate in a democratic society to achieve the legitimate purpose.

The AML/CFT regime provides for several contexts of processing of personal data, which are essentially based on public interest, setting out detailed obligations on data controllers. This extends to processing of personal data by government authorities which are entrusted by law with the mandate to combat AML/CFT and are granted specific powers in this area. Nevertheless, the same does not extend to private sector institutions, which are OEs, lacking the same legal status and mandate. As a result, data processing by private sector entities should be considered with caution on the legal basis of public interest and can only be envisaged if a clear legal basis exists authorising such processing, notably in the context of data pooling emerging initiatives which entail data sharing between private sector entities (which are outside of the same financial group). In any event, public interest needs to be specifically defined and limited to the circumstances where measures benefit and increase the effectiveness of the AML/CFT regime. This entails, for instance, that excessive collection and processing of personal data should be prevented first, because it would not be in line with core data protection principles and also because over data collection may not always serve operational objectives and the purposes defined by law and could also generate additional legal and technical challenges (data quality/ update, data security, etc) for key stakeholders, including LEAs.

Since data protection is fundamental to ensuring the right to respect for one's private life, family life, correspondence and home (Article 8 ECHR), regard must be given to data protection rules and principles when acting in AML/CFT interests, in compliance with Member States' commitments and obligations under international law. Under these laws, the existence of a legitimate purpose, a valid legal basis and appropriate safeguards for the processing of personal data is a prerequisite, for which the underlying rationale should be carefully analysed and articulated by international stakeholders from the AML/CFT, data protection and human rights field. Considering that data processing and sharing are crucial in combatting ML/TF, these guidelines aim to emphasize the requirements needed for compliance with data

[1] Global AML/CFT Standards: the FATF Standards; CoE Standards: The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198).). For the purposes of this paper, the following Articles of CETS No. 198 are of particular relevance: Art. 7, 17, 18, 19, 20, 43, 46, 47.

protection obligations included in Convention 108+ by controllers and processors, while complying with the AML/CFT framework.

1.2 Scope

These guidelines will cover data processing and sharing for AML/CFT purposes by public and private entities in state Parties to Convention 108+, including while cooperating with non-state-Parties (within the meaning of Article 14), and could inform such activities in non-state Parties to the Convention as well.

The purpose of these guidelines is to provide orientation on how to integrate international data protection rules and standards in the area of AML/CFT in order to provide for an appropriate level of protection while facilitating transborder data flows, and to point to some blind spots in AML/CFT related issues where data protection safeguards should be put in place or strengthened.

Considering the additional obligations imposed by Articles 6, 7, 9, 10 and 14 of Convention 108+, these guidelines also aim at providing governments and policy makers in state Parties with basic recommendations that could be considered when designing policies and regulatory instruments that comply with international data protection and privacy standards as provided by Convention 108+.

2. Terminology and context used for the purpose of the Guidelines

The definitions included in this section are understood to be necessary for proper contextualization when addressing AML/CFT issues. Notwithstanding this, specific definitions of terms applied in the latter field are also included in foot notes and in specific sections of the document.

Personal data and data subject – Article 2 (a) of the Convention defines personal data as any information relating to an identified or identifiable individual (data subject). A person is considered to be identifiable if additional information can be obtained without unreasonable time and effort which could in fine allow the identification of the data subject directly or indirectly. An individual's private life shall be interpreted in a large sense including information pertaining both to his/her private sphere as well as professional or public life. In the AML/CFT context, customers, beneficial owners (BOs)[2], parties to wire transfers, or individuals whose identifiable information is contained in data transfers, are to be considered as data subjects. They are the primary subjects of the Customer Due Diligence (CDD) measures[3], including identification and verification of identity. While Convention 108+ protects primarily personal data of natural persons, the Parties may extend the protection in their domestic law to data relating to legal persons in order to protect their legitimate interests[4], although corporate data shall not be considered as personal data, unless it relates to an individual (i.e. one-person-owned corporations or customer related data).

Data processing – All operations performed on personal data for AML/CFT purposes, either automated or manual, can be defined as data processing – including collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, use, destruction of, and the carrying out of logical and/or arithmetical operations on such data (Article 2(b) and (c) of the Convention). The aforementioned operations shall only be performed when controllers

[2] According to the FATF definition, a beneficial owner is the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
[3] Customer Due Diligence (CDD) is a process in which relevant information of an obliged entity´s customer is collected and evaluated from a ML/TF perspective. Obliged entities must have in place procedures to identify and eventually report ML/TF risks associated with a business relationship or an occasional transaction. FATF Recommendations 10, 11, 12, 15 and 17 detail the basic and additional CDD measures to be adopted by financial institutions. Recommendation 22 extend these measures to designated non-financial businesses and professions (DNFBP).
[4] Explanatory Report of Modernised Convention 108, para. 30.

and, where applicable, processors take all appropriate (and demonstrable) measures to comply with the provisions of the Convention 108+ (Article 10(1)).

Data controllers (in AML/CFT) – A natural or legal person, public authority, service, agency or any other entity which, alone or jointly with others, has the decision-making power with respect to data processing, the purpose and means of the processing, as well as data categories to be processed and access to the data (Article 2 (d) of Convention 108+). The decision-making power can derive from a legal designation or from factual circumstances that are to be assessed on a case-by-case basis (ER 22). Controllers are bound to ensure the legitimacy of data processing (Article 5 of the Convention).

From an AML/CFT standpoint, obliged entities (OE) are controllers alone or jointly. ~~However, joint controllership is rare in the AML/CFT regime~~. The OE include financial institutions[5] (FI), designated non-financial businesses and professions[6] (DNFBPs), virtual asset and service providers (VASPs). Recipients of the information such as FIUs, law enforcement authorities, and authorities holding public registers of information on basic and beneficial owners are to be considered also data controllers for the processing of personal data they perform.

The AML/CFT framework provides for different situations of information sharing, including between OEs; between legal persons and controllers of beneficial ownership registers; between OEs and FIUs or OE and other competent authority ("public-private partnerships/PPP); between the FIU of different countries; and between the FIUs and other competent authorities. In this scenario, if different controllers have the power to decide on the relevant aspect(s) of the processing operations relating to the same (set of) personal data, such as ~~shared~~ the ~~same~~ purpose for which the personal data is processed, they should be considered to be joint controllers[7]. Joint controllership leads to joint responsibility for a processing activity. For the purpose of catering for increasingly complex data processing realities, the joint controllership may take different forms and the participation of different controllers may be unequal. Therefore, joint controllers must determine their respective responsibilities for compliance with the obligations under the regulation of a specific agreement.. ~~However, joint controllership is rare in the AML/CFT regime.~~

Data processors in AML/CFT – A processor is the natural or legal person who processes personal data on behalf of a controller. The activities entrusted to a processor may be limited to a very specific task or may, on the contrary, be quite general. Legal or natural persons applying CDD measures on behalf of FIs and other DNFBPs are deemed to be data processors only in the case where they only follow instructions given by controllers. The main differentiation from data controllers relates to having decision-making power with respect to the data processing at issue (in AML/CFT, to comply with the CDD measures). However, processors could also become controllers whenever the data processing is done for their own purposes or whenever the conditions for data processing as prescribed by the controllers are breached.

[5] The term Financial Institution (FI) in the AM/CFT field as used throughout these Guidelines include both credit and financial institutions.
[6] Such as casinos, real estate agents, dealers in precious metals and precious stones, lawyers, notaries, other independent legal professionals and accountants, trust and company service providers.
[7] According to Paragraph 22 of the Explanatory Report of Convention 108+ (jointly responsible for a processing and possibly responsible for different aspects of that processing).

Special categories of personal data (sensitive data) – Under ~~the framework of Convention 108+~~ (Article 6~~)~~, there are special categories of personal data whose processing may intrinsically pose a greater risk to data subjects therefore their processing requires additional guarantees complementing those already put in place for "normal" categories of data. The following categories of personal data considered as sensitive are those: (i) revealing racial or ethnic origins, (ii) revealing political opinions, religious or other beliefs, including philosophical beliefs, (iii) revealing trade union membership, (iv) genetic data, (v) ~~and~~ biometric data processed for the purpose of uniquely identifying a person, (vi) concerning health, sexual life or sexual orientation, ~~Personal data~~(vii) ~~relating~~ to offences, criminal proceedings, convictions and related security measures ~~in the list of special categories of data are dealt with under Art. 6(1) of the Convention 108+.~~

3. Basic principles for the protection of personal data

3.1 The principle of purpose limitation

General principle

- The processing of personal data must be done for a specific, well-defined purpose and only for additional purposes that are compatible with the original one (Article 5(4)(c) of the Convention 108+). Further processing of data may not, therefore, be done in way that is unexpected, inappropriate or objectionable for the data subject.

- To assess whether the further processing is to be considered compatible, the controller should take into account, *inter alia*, for instance, the nature of personal data, the consequences of the intended further processing for data subjects, the context in which the personal data have been collected in particular concerning the reasonable expectations of data subjects based on the relationship with the controller on its further use, and/or the existence of appropriate safeguards in both the original and intended further processing operations[8].

- If the purpose of further processing is deemed by the controller to be incompatible with the original purpose, the controller shall be required to inform data subjects in order to either obtain consent, if requirements for a valid consent are met in relation to the additional purpose or to inform him/her on the justification of the processing on other applicable legal basis.

AML/CFT contextualisation[9]

- Personal data on the customer or transactional data that may be collected by OEs for CDD purposes, may, under certain conditions provided by the law, be shared with other obliged entities belonging to the same group, for fulfilling ~~additional~~ further compatible purposes (e.g. inform an OE belonging to the same group of a common customer that may have been subjected to reporting to the FIU). For example, in correspondent banking relationships, the correspondent bank may need to require additional information in relation to a client of the respondent bank, which would have been collected by that bank from its client in a different context.

- As an element of context, it is important to differentiate between the sharing of data by FIUs to other national law enforcement agencies and to foreign FIUs for the purpose of international cooperation as different rules may apply and the purpose limitation principle should be closely followed.

[8] Explanatory Report of Modernised Convention 108, para. 49.
[9] Relevant FATF Recommendations: Rec. 13, 20, 29, 31, 40

- There could be instances where data collected and processed for a defined purpose (e.g. customer due diligence information or suspicious transaction information) may have to be shared with third parties. For example, an FIU analysing a suspicion transaction report (STR), finding international links that require that STR information (including personal information) to be shared with another competent authority or a foreign FIU in the context of a request of additional information.

- On occasion, the OE may need to file a suspicious transaction report to the FIU, and the processing of personal data by the FIU constitutes an additional purpose, which is considered compatible with the original purpose of processing. The FIU may further need to report a suspected criminal activity to a competent authority. The purpose of processing of the competent investigating and prosecuting authorities are normally governed by other laws.

Recommendations

- The purpose limitation principle should be respected, both when data processing is carried out for several different purposes, or when the processing is carried out for a compatible purpose. The concept of compatible use should not hamper the transparency, legal certainty, predictability or the fairness of the processing[10].

- OEs belonging to a group should have clear policies and procedures based on law to define what type of personal data (client, BO, transactional, account, suspicion transaction report –or STR-) that could be shared among them, the legal basis and the purpose. This could be achieved using binding corporate rules (BCRs, SCCs, ad-hoc clauses).

- The FIUs processing suspicious transaction reports should have clear rules and procedures based on law, concerning the purposes for which personal data relating to STRs may be shared with other competent authorities.

- In relation to cross-border correspondent banking and other similar relationships ~~(FATF Recommendation 13)~~[11], there should be clear and detailed provisions based on law between the correspondent and the respondent bank regulating the sharing by the respondent of personal data concerning its customers, beneficial owners and transactions. The provision should detail the type of data that the respondent bank will have to provide upon the request of the correspondent bank. Guidance in this regard should be provided by data protection authorities.

- The purpose limitation principle shall also be implemented in line with Article 5(4)(c) of the Convention 108+ also in the context of data sharing/transfers by FIUs to other national law enforcement agencies ~~(FATF Recommendations 29 and 31)~~[12] but also to foreign FIUs ~~(FATF Recommendation 40)~~[13]. In this case, internal standard operating procedures should be developed to ensure that data is shared for a specified and limited purpose documented in the transfer trail and that the essentially equivalent protection is ensured during the transfer and by the receiving authorities.

[10] Explanatory Report of Modernised Convention 108, para. 49.
[11] FATF Recommendation 13
[12] FATF Recommendations 29 and 31
[13] FATF Recommendation 40

3.2 The lawfulness of processing – legal basis

General principle

- Based on obligations set forth by Art. 5 (2)-(3) of the Convention 108+ personal data shall be processed lawfully: which requires that the data processing should either be based on the data subject's consent or a legitimate basis provided for by law.

- The required elements for a valid consent are: (i) freely given, (ii) specific, (iii) informed, (iv) unambiguous which are further explicited in the Explanatory Report[14].

- The notion of "legitimate basis laid down by law" encompasses, *inter alia*, data processings that are necessary (i) for the fulfilment of a contract to which the data subject is party, (ii) data processing necessary for the protection of the vital interests of the data subject or of another person; (iii) for compliance with a legal obligation to which the controller is subject; (iv) on the basis of grounds of public interest or (v) for overriding legitimate interests of the controller or of a third party,.

- Irrespective of the legal basis for data processing, which is relied upon by the controller, additional safeguards ~~provided~~ in particular for special categories of data as foreseen by Article 6 of the Convention 108+shall be ensured such as an explicit consent.

AML/CFT contextualisation[15]

- Data processing in the AML/CFT context shall be based on a clear and detailed legal basis and shall be necessary and proportionate to the legitimate aim pursued.

- Consent as a legal basis for personal data processing must be freely given, informed, specific and expressed in an unambiguous manner, by a clear affirmative agreement to processing. However, this legal basis could very unlikely to be used for AML/CFT purposes as data subject has no real choice. An alternative legal basis must be found because even if consent is obtained it is unlike to be valid (potentially rendering the processing unlawful). More precisely, the AML/CFT framework which often involve specific investigations into suspicions of or actual ML/TF activities provides for situations where the customer is not or not completely informed of the data processing, particularly in relation to enhanced due diligence measures and suspicious transaction reporting by the OE, where prior information to the customer would contravene to AML/CFT prohibitions, in particular to tipping-off.

- Processing of personal data by public authorities shall be based on the lawful ground of public interest, given they are entrusted with the mandate to combat AML/CFT and are granted sovereign powers in this specific area. Checks and balances as well as oversight are also implemented. Nevertheless, the same does not extend to private sector institutions which are obliged entities and do not benefit from the same legal status and mandate.

- Processing of personal data by OEs should be based on legal obligations to which the controllers are subject[16].. Failure by OE to comply with those obligations would entail risks of measures taken by ~~financial~~ supervisory authorities, including administrative and criminal sanctions. Failure by customers to provide the requested data could, in turn, result in that the customer relationship is either not concluded or in the restriction of services.

[14] Modernised Convention 108, Art. 5(2); Explanatory Report of Modernised Convention 108, paras. 42-45.
[15] Relevant FATF Recommendations: Rec. 24
[16] Explanatory Report of the Modernised Convention, para. 46.

- Data processing by OEs could also be based on the overriding legitimate interest of the controller or a third person provided that the rights and interest of the data subjects have been duly balanced against the rights and interest of the controller or a third person and that appropriate guarantees have been put in place. It should however be noted that the latter case would not apply to special categories of data (including data relating to offences, criminal proceedings, convictions and related measures).

- Data processing is required to prevent the misuse of legal persons for ML or TF by ensuring that there is adequate, accurate and up-to-date information on beneficial ownership and control of legal persons ~~(FATF Recommendation 24)~~[17]. Beneficial Ownership Information could be obtained by the company and available at a specific location in their country or can be also determined in a timely manner by a competent authority. In determining the beneficial owners, countries are required to ensure that companies co-operate with competent authorities to the fullest extent possible by (i) requiring one or more natural persons resident in the country, authorised by the country and accountable to competent authorities to provide all available beneficial ownership information, (ii) requiring that a DNFBP in the country is authorised by the company and accountable to competent authorities for providing all available BO information or taking other comparable measures.

- Information sharing initiatives through Public-Private Partnerships (PPPs)

Commented [A1]: MONEYVAL - Seeking to further develop the point on information sharing initiatives through PPPs d to mirror the 4th recommendation.

Recommendation

- Data processing in the context of AML/CFT should be carried out exclusively on the basis of a clear and detailed legal basis

- Public interest as a legal basis for data processing emerging initiatives by private sector entities subject to AML/CFT obligations should be considered with caution, given the often lack of appropriate legal basis which would determine their legal status and mandate with which public authorities are entrusted and can be held accountable for non-compliance with their legal obligations.

- Data processing by a private entity could be based on its legal obligations or the overriding legitimate interest of the controller or a third person provided that the rights and interest of the data subjects have been duly balanced against the rights and interest of the controller or a third person and that appropriate guarantees have been put in place.

- Clear and detailed provisions that take into account all rights and interests concerned shall be established in relation to PPPs created for the sharing of operational information on intelligence on suspects preventing OE participating in PPPs from integrating ~~information~~ personal data shared by law enforcement authorities in their own databases.

- Regarding central beneficial ownership registries, information should only be available in the situations or to the extent provided by law, and in compliance with international data protection standards and regulations.

[17] FATF Recommendation 24

3.3 The fairness and transparency of processing principles

General principle

- In addition to lawful processing, personal data shall be processed in a fair manner by both the controller and the processor (Article 5(4) of the Convention). This principle requires, so far as possible, the provision of information to the data subject regarding the processing of his/her data, including any risks which may have been identified by the controller or the processor in order to allow them to make an informed decision and to enable them to exercise their data protection rights. In addition, fairness also requires an assessment on how the processing will affect the data subject. Processing operations shall not be performed in secret.

The principle of transparency is intrinsically linked to the principle of fairness. Data processing shall be performed "in a transparent manner in relation to the data subject" (Articles 5 (4)(a) and 8 of the Convention). In this regard, data subjects must be informed before processing their data, *inter alia*, about the categories of personal data processed, the purpose of processing and about the identity and address of the controller. In case of joint controllership, controllers need to clarify the purposes of the processing, the means of exercising the rights set out in Article 9,. to provide transparency, and also a way to demonstrate compliance with the Convention (Article 10)[18]. In doing so, in the need to consider the fact that public authorities and private sector entities have different status and legal obligations, and may therefore be subject to different data protection regimes.

- Information on the data processing must be provided in clear and plain language to allow data subjects to easily understand the risks, safeguards and rights at stake (unless an exception foreseen under Article 11 applies). Moreover, the data subject should be informed about his/her rights, according to which a request can be made to the controller on whether personal data is being processed and if so, which data is subject to such processing (Article 9(1)(b) of the Convention).

AML/CFT contextualisation[19]

- Data processing for public interest should not be considered ab ovo as fair, data controllers in the public sphere need to comply with those principles unless an exception applies.

- ~~Under FATF Recommendation 10,~~ FIs are required to undertake CDD measures when (i) establishing a business relation, (ii) carrying out occasional transactions above the applicable designated threshold (USD/EUR 15 000), (iii) in some circumstances, when carrying out occasional transactions that are wire transfers, (iv) when there is a suspicion of ML/TF, or (v) when there are doubts about the veracity or adequacy of previously obtained customer data. FIs should identify the customer (a natural or a legal person or arrangement, whether permanent or occasional) and verify the customer's identity using reliable and independent sources[20]. FIs should also identify, verify the identity and the existence of authorisation for any person purporting to act on behalf of the customer, as well as for the beneficial owner. FIs, particularly banks, typically inform the customer on the purpose for which data will be processed and may be eventually shared with third parties, and they require their consent, although this is not an FATF requirement and practice may vary from country, depending on local data protection laws. In certain specific circumstances, OEs may also require their consent, particularly for the provision of certain services or on the occasion for the disclosure of customer data to third parties.

[18] European Data Protection Board: "Guidelines 07/2020 on the concept of controller and processor in the GDPR". Version 2.0. July 7th. 2021. Page
[19] Relevant FATF Recommendations: Rec. 10
[20] FATF Recommendation 10

- In some cases, besides data protection regulations, there are banking secrecy or other professional secrecy obligations that apply to some persons (e.g. lawyers).

- To facilitate access to accurate and up-to-date beneficial ownership information some States have created central registries, with information provided by legal persons. Access to that information is typically given for OEs for the purposes of CDD as well as for competent authorities, including the FIU. Access to such information is important particularly for the investigating and prosecuting authorities to trace criminal activities.

Recommendation

- When establishing business relationships with customers or when conducting transactions for occasional customers, OEs, in their role of controller, should provide information to the data subject, *inter alia,* on, the legal basis and the purposes of the intended processing, the categories of data that the FI and DNFBP (or other third parties) will be processing, the recipients or categories of recipients of the personal data, if any; the means of exercising the rights set out in Article 9 of the Convention and potential restrictions where appropriate, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data and the use made thereof in an understandable and user-friendly way.

- OEs should assess the likely impact of intended transfers and/or other data processing activities on the rights and fundamental freedoms of data subjects prior to the commencement of such processing and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

- There must be a clear legal requirement set out by law, under which customer data may be disclosed to third parties despite secrecy rules, where applicable.

- Access to central beneficial ownership registries information should only be allowed in the situations or to the extent provided by law, and in compliance with data protection regulations.

3.4 The data minimisation principle

General principle

- Data processing must be limited to what is necessary to fulfil a legitimate and limited purpose (Article 5 (4)(c)). A controller should strictly limit collection of data to such information as is directly relevant for the specific purpose pursued by the processing including in relation to the data collection and processing by a or multiple processors. ~~The same applies to the processor when it collects data on behalf of the controller.~~

- The implementation of this principle requires the controller to assess whether data processing is necessary and proportionate in accomplishing the specific purpose and to verify the existence of alternative less intrusive means. In terms of necessity, for instance, controllers shall verify whether the purpose could be attained by processing anonymous data. Regarding proportionality, the amount of data to be collected shall be carefully considered with a view to the purpose of the processing and in parallel it is advisable to avoid breaching the data minimisation principle.

AML/CFT contextualisation

- The AML/CFT laws may provide for different levels of processing of personal data (CDD data) by the OEs, including simplified, normal and enhanced customer due diligence. In principle, enhanced due diligence requires a larger amount of personal data to be processed, including verification of that data from various sources available

for the OE. Enhanced due diligence may be required on the basis of risks for certain types of customers (e.g. politically exposed persons) or for certain types of services or transfers (e.g. money transfers to high-risk countries), or even for individual customers in situations where risks or suspicious transactions have been identified. The AML/CFT laws may provide for different data retention periods for different types of personal data.

- In practice, it appears that, in many instances, private sector entities may lack clear and specific guidance needed on collecting clients' personal data as part of AML/CFT obligations. For instance, regarding specific datasets to be collected as part of KYC standards, they need to observe at the same time data protection legal obligations which may provide for contradictory approaches, notably with regard to the application of the data minimisation principle. As a result, by fear of missing an element of threat or of being fined by financial supervisory authorities, private sector entities often end up sharing larger volume of data "just in case".

- The data minimisation principle should also be applied in the context of automated data processing at data collection but also at data transfers' level.

Recommendation

- Data processing by OEs should be limited to what is directly relevant for the specific purpose pursued in view of the risks inherent to the customer relationship.

- Data should be used for the sole purpose for which it was provided and cannot be transferred to other authorities of the data-receiving countries, unless the requirements laid down in the Convention are complied with.

- With regards to data processing by the private sector, the specific data sets to be collected as part of AML/CFT obligations are not always specified by the national law whereas the principle of data minimisation is clearly provided for in national data protection law. It could therefore be recommended to facilitate collaboration between national, regional and international fora of data protection authorities and financial and other non-financial (DNFBP) supervisory authorities and international AML/CFT fora so that specific guidance could be developed to ensure a consistency between applicable legal obligations.

- In the context of automated data processing (at data collection but also at data transfers level), a privacy by design approach should be implemented (by the private sector but LEAs, including FIUs) and embed data minimisation in the architecture of the system used (e.g. limited mandatory data fields, limited free text zones etc.) as per Article 10 Convention 108+.

- In the context of PPP sharing of transaction data that implies processing of a high amount of data, the processing should be done, to the extent possible, with anonymized or pseudonymized data. Personal data identifying a person related to a transaction should be only limited when the outcome of the processing based on conditions linked to a reasonable suspicion/probable cause reveals patterns or activities that might require reporting of the transaction to the FIU as suspicious, or when it is needed to identify links to an identified terrorist.

3.5 The data accuracy principle

General principle

- The principle of data accuracy shall be implemented by the controller in all processing operations (Article 5(4)(d)). Controllers are expected to take reasonable measures to ensure that collected data is accurate and, where necessary, regularly verify it is kept

up to date, depending on the specific purpose. Inaccurate data must be erased or rectified. As such, controllers shall respond to data subject requests to correct records that contain incomplete or inaccurate information.

- When corrections of inaccurate data were needed, it could be acceptable that controllers keep record of events that happened in error, provided that those records are not misleading about the facts, and their scope is limited to the description of the event, date and cause of the correction.

- At the data collection stage, controllers shall evaluate the reliability of the source of information. In further data processing, depending on the specific purpose, the accuracy of personal data should be regularly verified in order to prevent any adverse implications for the data subject.

AML/CFT contextualisation[21]

- OEs are required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers[22].

- OEs use external providers of information for various purposes (e.g. sanction screening, identification of PEPs, family members and close associates), which can affect the accuracy of data that they process for CDD purposes, and use AI-based systems to monitor transactions in order to identify suspicious patterns and trends, and generate alerts, which, if not using accurate data and is properly calibrated may result in false positive/negative hits and/or an excessive number of alerts, that cannot be processed in an ~~accurate~~ lawful manner. While the FATF Recommendations do not explicitly refer to the requirement of accuracy, the aforementioned requirement to keep CDD data and information up to date applies even to data collected from external providers.

- OEs are allowed to rely on third parties for the performance of certain elements of the CDD process[23]The fact that CDD information will have been collected and processed by a third party over which the relying OE may not have forms of control could result in inaccuracies of the information collected for the CDD process. However, the FATF Standards are clear in that the responsibility of the fulfilment of the CDD obligation remains in the OE that is relying on the third party. This is consistent with the role of controller of OEs, as defined in Convention 108+. While the FATF Recommendations do not explicitly refer to the requirement of accuracy, the aforementioned requirement to keep CDD data and information up to date applies even to situations where third parties are relied on.

- Companies and company registers are required to maintain accurate and up-to-date information on beneficial owners[24]. In practice, AML/CFT laws typically require the same for other legal entities entered in BO registers. ~~Recommendation 24~~It is further require~~s~~d that basic data (i.e. company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, and a list of directors) ~~to be~~is made publicly available, and also envisages the possibility to require companies or company registries to obtain and hold BO information[25].

[21] Relevant FATF Recommendations: Rec. 6, 7, 10, 17, 24, 37, 40
[22] FATF Recommendation 10
[23] FATF Recommendation 17
[24] FATF Recommendation 24
[25] idem

- Countries are required to provide rapidly, constructively and effectively the widest range possible of international cooperation in relation to basic and beneficial ownership information, including exchanging information on shareholders and beneficial owners[26].

Recommendation

- OEs should be encouraged to implement procedures to ensure that they comply with the requirement of accuracy set out in Article 5(4)(d), in any CDD data processing operations, to avoid risks and harmful effects on the rights of the customer as data subject, which may result from the processing of data that is not up to date.

- When AI is used (e.g. for transaction monitoring for the purpose of detection of suspicious activity), the data subject should not be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration. This would entail that human intervention need to occur from a staff member to verify the accuracy of the results (for instance to avoid negative impact on data subjects in case of a decision based on a false positive obtained only through automated means) or of the data subject concerned so that he/she can present his/her views. In addition criterion should be calibrated in a way not to generate an excessive number of alerts, especially false positive ones, including the case of customer/BO/recipient of transaction name-searching and matching with sanction lists [27] ~~(FATF Recommendation 6 and 7)~~.

- If OEs are using ~~programs~~ automated system, including when supported by algorithmic processing or AI for risk profiling of the customers or the BOs, appropriate measures should be taken to correct data inaccuracy factors and limit the risks of errors inherent to profiling. The periodic (or trigger-based) reassessment should also include a re-evaluation of the data and of the statistical inferences including for the elimination of potential biases used for the risk profiling, to determine whether they are still accurate and relevant.

- If OEs are using external database providers for implementing customer due diligence requirements on BOs of the customers (e.g. identity verification of the customer and BO, identification of potential relations with PEPs, and family members and close associates to the PEP) they should strive to verify that the personal data used is accurate and up-to-date and to conduct a periodic evaluation of the accuracy of the data made available by the provider.

- Countries should ensure that there are policies in place requiring controllers responsible for company registries to verify the quality of personal data held by those registries, or use other appropriate means, in order to ensure that the data is accurate and up to date.

- The OE receiving data on specific customers, BOs and transactions for specific purposes is considered to be the controller of the data and should be held responsible for the lawfulness of the processing of the data as well as for its accuracy, even in the case in which the OE uses third parties for the collection and processing of such data. Those third parties might be deemed processors according to Convention 108+.

- In accordance with Article 10 of the Convention 108+ OEs shall implement measures to prevent or minimise the risk of interference with the rights and fundamental freedoms of the customers.

- OE are also invited to Also, implement the privacy by design approach to embed and automate the update review into the system used to process the data.

[26] FATF Recommendations 37 and 40
[27] FATF Recommendation 6 and 7

- To facilitate rapid, constructive and effective international cooperation, data held or obtained for the purpose of identifying beneficial ownership should be kept in a readily accessible manner.
-

3.6 The storage limitation principle

General principle

- Article 5 (4) (e) of Modernised Convention 108 requires personal data to be deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected. However, there are exceptions to this principle on the condition that (i) they are provided by law, (ii) respect the essence of fundamental rights and freedoms and (iii) are necessary and proportionate for pursuing a limited number of legitimate aims (Art. 11). These include, inter alia, preserving national security, investigating, and prosecuting criminal offences, protecting the data subject and protecting the rights and fundamental freedoms of others.

AML/CFT contextualisation[28]

- Clear requirements are set for the record keeping period of CDD information, account files, business correspondence and results of any analysis undertaken (5 years following the termination of the business relationship) and records on transactions (5 years following completion of the transaction)[29].

- Data processing is required in order to prevent the misuse of legal persons for ML or TF by ensuring that there is adequate, accurate and up-to-date information on beneficial ownership and control of legal persons[30]. In case of dissolution of a company or otherwise cessation of existence, all stakeholders and the company itself (or its administrators, liquidators or other persons involved) are required to maintain the information and records referred to for at least five years after the date on which the company is dissolved or cesses to exists or five years after the date on which the company ceases to be a customer of the professional intermediary or the FI.

- When the legislation imposes a specific retention period, controllers must adopt the necessary measures to ensure the proper protection of the data

Recommendation

- If there are no storage limitation requirements and/or those in place are not in line with FATF Recommendation ~~11~~, data should be stored in line with Article 5 (4) (e) 5for the minimum period necessary, and be deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected.

- Regarding the storage of personal data by public authorities for the purpose of combating crime, a distinction should be made depending on the nature ~~or degree of seriousness~~ of the offence or depending on whether the data subject is only a suspect.

- Cooperation at a national level between data protection authorities and other supervisory authorities should be facilitated so that specific guidance could be developed to ensure a balance between applicable legal obligations, both from an

Commented [A2]: Delegations are kindly asked to indicate specific actions that could be taken to enhance this type of cooperation? For instance, during the FATF Digitalisation Conference, one suggestion was that AML/CFT authorities could approach DPP authorities and explain in detail the rationale for each AML/CFT measure and start harmonizing from there .

[28] Relevant FATF Recommendations: Rec. 2, 11, 24, 29, 40
[29] FATF Recommendation 11
[30] FATF Recommendation 24

AML/CFT and data protection perspective, including regarding the issue of data retention.

3.7 The data security principle

General principle

- The security and confidentiality of personal data are key to preventing adverse effects for the data subject, such as unauthorized, unlawful, or accidental access, use, modification, disclosure, loss, destruction or damage (Article 7 of the Convention). The controller and, where applicable the processor, should take specific security measures that consider the specificities of the operations and the state of the art of data security methods and techniques. The appropriateness of security measures must be determined on a case-by-case basis and reviewed regularly.

- Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation measures, which do not exempt from the application of relevant data protection principles, can reduce the risks to data subjects[31].

- As data security issues may arise from many different situations (loss of integrity by cyber-attacks, loss of confidentiality by interception of data transmissions, loss of availability (data loss, black out, down times) other measures could also be envisaged here, such as anonymization, encryption, access rights and roles, etc.

AML/CFT contextualisation[32]

- There are several requirements in the FATF Recommendations addressed to public authorities that can ensure data security. The revised version of Recommendation 2 requires countries to have cooperation and coordination between competent authorities to ensure the compatibility of AML/CFT requirements with Data Protection requirements. This should also have (albeit only indirectly) an impact for OEs processing and exchanging data.

- Ensuring the confidentiality of STRs is essential to the effectiveness of the reporting regime, by avoiding tipping-off the subject of STR as well as third parties, as this can adversely impact intelligence gathering and investigative efforts and enable dissipation of assets. STR confidentiality rules are also important in terms of protecting the reputation of a person subject of an STR, as well as the safety of the person filing the report. On a more operational level, several requirements for FIUs to protect information are already proposed in particular by (i) having rules in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination and protection of, and access to information, (ii) ensuring that staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information and (iii) ensuring that there is limited access to its facilities and information, including information technology systems[33]. In addition to FATF, the Egmont Principles also set security measures for the exchange of information. Furthermore, requirements of using

[31] T-PD Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (2017) https://rm.coe.int/16806ebe7a

[32] Relevant FATF Recommendations: Rec. 2, 29, 40

[33] FATF Recommendation 29

secure channels are foreseen for information exchange, applicable to competent authorities such as investigative authorities[34].

- The data protection legislation applicable in the states Parties may provide for detailed requirements concerning data security, that may be as such applicable to OEs as controllers. At the same time, the AML/CFT or other specific legislation of countries may also provide for additional requirements to ensure data and information security that has become known to the public officials of the competent authorities. Public officials may face disciplinary, civil, administrative, and criminal liability for breach of ensuring safety of information, which related to their activities, constituting an official, banking, tax, commercial or communication secret.

Recommendation

- There should be specific requirements for OEs to implement state of the art, strict security measures for ensuring the protection of personal data, particularly in the case of special categories of data according to Article 6 of the Convention 108+ (e.g. on PEPs, which could reveal political affiliations or sexual orientation in the case, for example, of a same-sex partnership), unless the applicable data protection framework already provides for such requirements that are directly applicable and as such binding on the OEs as controllers.

- Compliance with the principle of data security requires technical and organisational measures such as (hard, end-to-end) encryption of the data and rules on the full traceability of the exchanges, especially through the implementation of access logs, also in compliance with the accountability principle of Article 10 of Convention 108+. Other safeguards should also be put in place such as pseudonymisation in order to prevent unlawful interference with individuals' privacy and right to data protection. These technical and organisational measures should be based on a risk assessment regarding the impact on data subjects' rights.

- Controllers should analyse threats and trends in the area of cybercrime and information security on both a periodical and ad-hoc basis (unexpected trigger events) in order to enhance data security and minimise the risk of breach.

4. Types of data which are subject to the processing of personal data in the context of AML/CFT obligations

General principle

- Any type of information can be personal data if it relates to an identified or identifiable person, which could be information pertaining to the private life of a person, which also includes professional activities, as well as public information about one's life (Article 2 (a) of the Convention 108+).

  There are also special categories of personal data such as genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, whose processing is, by nature, likely to pose a higher risk to the data subjects and therefore need enhanced protection. Such data is subject to additional safeguards complementing those already in place for "normal categories of data" and can only be lawfully processed under a limited number of conditions (Article 6 of the Convention108+).

[34] Recommendation 40

Formatted: French (France)

AML/CFT contextualisation[35]

- In the preventive measures' context, AML/CFT and Data Protection Authorities shall ensure that for any given data processing both AML/CFT and Data Protection requirements are satisfied.

- To mitigate ML/TF risks, the private sector is required to undertake measures focused on the prevention, detection and reporting of customers and transactions suspected of ML, associated predicate offences and TF, notably by collecting, processing and securely sharing relevant data to competent authorities (e.g. supervisors and LEAs, at a national and sometimes an international level) and within financial groups for AML/CFT purposes.

    - Identifying, assessing and understanding the nature and level of ML/TF risks and applying AML/CFT policies, internal controls, and programmes as required to adequately mitigate those risks (R.1);

    - Knowing their customers and monitoring their accounts and activities as appropriate for AML/CFT purposes (R.10) by conducting CDD measures to identify and verify the identity of a customer at the on-boarding stage, as well as by conducting ongoing due diligence over the course of the business relationship;

    - Ensuring record-keeping on CDD and other transaction information for at minimum five years (R.11), as financial crime investigations often require considerable periods of time.

    - Information sharing within the context of financial group is required both for customer due diligence purposes and ML/TF risks management[36].

    - Being able to detect and report suspicious transactions (R.20) and ensure that customers are not aware that an STR or underlying information is filed with authorities (R.21).

- Different types of data are handled in the AML/CFT field, and it is important to acknowledge their scope. To that aim, further definitions on types of data and collection from AML/CFT standpoint are included in annex 1:

    - Customer data – The FATF Standards define parameters for information sharing only within the context of a financial group[37]. Due to data protection and privacy requirements, data sharing outside of a financial group is restricted. The required CDD datasets that should be obtained from a natural person include mainly personal data, such as: the full name, residential address, contact number and e-mail addresses, place of birth, date of birth, gender, nationality, race, government-issued identification number and tax identification number, signature. For a legal person, some personal data is required as well on directors, shareholders, senior management and beneficial owners, which is generally publicly available due to legal provisions based on the public interest.

[35] Relevant FATF Recommendations: Rec. 1, 10, 11, 18, 20, 21

[36] FATF Recommendation 18

[37] Under the FATF Glossary definition, a Financial Group constitutes "a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level".

Recommendation

- Personal data relating to offences, criminal proceedings and convictions, as well as related security measures are a part of the aforementioned special categories of personal data which are also relevant to AML/CFT. Processing of such data may only be carried out when specifically allowed by law and when appropriate safeguards are in place (e.g. professional secrecy obligation; measures following a privacy impact assessment; a particular and qualified organisational or technical security measure such as data encryption and logging)[38].

- Registers holding information on criminal convictions may be restricted to the processing and use by competent authorities, or to processing under the control of those authorities. Any processing of such data is further subject to supervision by the competent ~~data protection~~ authorities.

- Internal guidelines should be developed to provide for a case-by-case assessment on whether the collection and/or transfer of sensitive data (notably regarding religion and sexual orientation) is necessary to achieve the purpose in consideration of the risks to the life and integrity of the data subjects may raise in case of a data security incident, including a data breach.

- All entities involved in AML/CFT, including private entities, FIUs and Law Enforcement Agencies should ensure training to their staff, especially in regard to dealing with special categories of data, ~~to~~e.g. concerning the extent to which processing of such data is allowed by law.

- According to article 10 of Convention 108+, it is necessary for controllers to adopt accountability measures for the processing of such data, including data protection impact assessments, privacy by design and by default measures, and the appointment of a Data Protection Officer when applicable.

5. Rights of data subjects, exceptions and restrictions in the context of AML/CFT

General principle

- Data subjects have multiple rights detailed in Article 9 of the Convention:
    - The right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;
    - The right to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;
    - The right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;
    - The right to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller

[38] See Explanatory Report to Convention 108+, para 56.

demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

- The right to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;

- The right to have a remedy under Article 12 where his or her rights under this Convention have been violated; and

- The right to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention.

- Conditions for possible restrictions of these rights are set out in Article 11 of the Convention, they must be provided by law, respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society. Restrictions to the right of access should no longer be in place once access no longer jeopardise investigations.

- Exceptions should only be established for purposes listed in Article 11, which include inter alia the protection of national security, defence, public safety and important economic and financial interests of the state and only in relation to specific rights or obligations laid down in the article.

AML/CFT contextualisation[39]

- Some of the rights expressed in the Convention can be restricted for AML/CFT purposes and usually the restrictions based on AML/CFT laws rely on general public interest (i.e. the important economic and financial interests of the State; the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties). The rights of the data subject are restricted e.g. in a situation where the OE reports a suspicious transaction to the FIU. The AML/CFT laws require that the STR is not disclosed to the person concerned, in which case the access of the data subject to personal data relating to STRs may be restricted. Further restrictions may be imposed with regard to the processing of STRs by the FIU. At the same time, there is usually no reason to restrict access to CDD data – instead, the OEs are invited to inform customers that their personal data may be used for AML/CFT purposes.

Recommendation

- Measures should be put in place by controllers to facilitate the exercise of these rights by the data subject, in principle free of charge. In case of automated decision making, the information on the decision should be available upon request of the data subject. Other example could concern the right not to be subject to only automated decision making which would be relevant where AI is used to analyse transaction data and inform a decision whether or not a transaction is suspicious and should be transmitted to LEAs. Clear rules and instructions should be provided in line with Article 11 on if and when data subjects can exercise their right, or if an exception applies and how the "tipping – off" ban[40] can be implemented in line with data protection requirements.

- In the case of the right to object, the Explanatory report (para. 80) indicates that even when this right is limited for the purpose of the investigation or prosecution of criminal offences, the data subject can challenge the lawfulness of the processing. Restrictions

[39] Relevant FATF Recommendations: Rec. 21
[40] FATF recommendations 21.2

to the exercise of rights justified by the risk to jeopardise investigation activities should be waived once such risk no longer exists.

- The effective implementation of data subjects' rights may also require additional actions, to reflect those rights in a privacy by design architecture in accordance with Article 10 Convention 108+. For instance, the right of access may require that the architecture enables the user to seamlessly identify and select across the system all sets of data concerning the data subjects and this without disclosing data of other data subjects (data segregation or structed data embedded in the architecture).

6. Exceptions and restrictions (Article 11)

General principle

- Processing personal data is one of the most important operations in an AML/CFT context, therefore anyone concerned should take into account that only a limited number of expiations can be used provided they comply with the general conditions (i.e. they are provided for by law, respect the essence of human rights and fundamental freedoms and are necessary in a democratic society) of their lawful use:
    - The obligation to process data fairly and in a transparent manner;
    - The need to ensure that data is collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes;
    - The obligation to limit the processing to adequate, relevant and not excessive data in relation to the purposes for which they are processed;
    - The obligation to ensure that data undergoing processing is accurate and, where necessary, kept up to date; and
    - The need to ensure that data is preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

AML/CFT contextualisation

- Based on such exception the AML/CFT framework could provide for situations where the customer (data subject) is not informed of the processing, particularly in relation to so-called enhanced diligence and suspicion transaction report by the OE. That would imply prior information to the customer, which would contravene to AML/CFT prohibitions, in particular to tipping-off. Further, the right of access of customers to the data processed by competent authorities, including FIUs, is typically restricted until the reason for the restriction exists. Data subjects' rights should be fully guaranteed outside of time and scope of a lawful use of exception.

Recommendation

- Where the data subject rights are restricted for AML/CFT purposes, those restrictions should be based on the AML/CFT legislation, they should respect the essence of fundamental rights and freedoms and be strictly limited to what is necessary and proportionate in a democratic society. They should not in any case be too broad or serve as a blanket authorisation and should only apply to areas covered by Article 11(1) of the modernised Convention 108.

- Restrictions to the exercise of rights justified by the risk to jeopardise investigation activities should be lifted once such risk no longer exists.

7. The role of Data Protection Authorities (DPAs) and their relationship with authorities monitoring AML/CFT

General principle

- DPAs are public bodies that are tasked and empowered to ensure compliance with applicable data protection regulations, including through enforcement action and international cooperation..
- According to Article 15 Supervisory Authorities -in the terms of the Convention- shall have powers of investigation and intervention, perform functions relating to transfers of data, have powers to issue decisions with respect to violation of the provisions of the Convention and impose sanctions, amongst others.
- Articles 16 and 17 of the Convention provide for means of cooperation and mutual assistance between data protection supervisory authorities.
- DPAs are usually cooperating with authorities monitoring AML/CFT when matters related to the processing of personal data so require.

AML/CFT contextualisation

- The activities necessary to comply with AML/CFT regulations involve the activity of multiple actors in multiple jurisdictions, and the processing of large volumes of personal data. The Convention foresees powers of the supervisory authorities apply for any processing of personal data, including AML/CFT purposes, while only specific restrictions are possible under Article 11(1) for law enforcement (and other general public interest purposes) and Article 11(3) with reference to processing activities for national security and defence purposes. Even in the latter case where more exceptions are foreseen for those specific purposes, the Convention requires that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

Recommendation

- Processing operations for AML/CFT purposes should be subject to effective and independent ex-ante authorisation and/or ex-post review based on the domestic legal framework. In addition, national legal frameworks should provide for a specific level of security clearance for DPA' staff to access the data processed by FIUs falling under the category of intelligence service.
- DPAs should engage with other national authorities that oversee AML/CFT issues for joint activities to ensure compliance with data protection standards in the AML/CFT enforcement area.
- In general, the need for dialogue and cooperation between DPAs and other supervisory authorities (at national and international levels possibly) should be emphasised in order to develop effective guidance tools for the private sector and to develop specific training modules.
- In the AML/CFT field, DPAs should have coordinated activities with the OEs in order to to suggest effective tools and modus operandi for compliance (which could, if correctly implemented, contribute also to a more effective supervision) and could also provide specific training.

8. International data transfers in the AML/CFT field

General principle

- Cross-border data flows are personal data transfers to recipients who are subject to a foreign jurisdiction[41].

- There shall be a free movement of personal data among Contracting Parties to Convention 108+. Restrictions on the free transborder movement of personal data are foreseen when (i) there is a real and serious risk that the transfer to another Party may lead to circumventing the provisions of the Convention or (ii) if a Party is bound to do so by harmonised rules of protection shared by States belonging to a regional international organisation (Art. 14(1) of the Convention).

- Personal data transfers to third countries or international organisations may only be permitted provided that an appropriate level of protection can be ensured by the law of the recipient State or international organisation or based on ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted by the persons involved in the transfer and further processing (Article 14(2) and (3) of the Convention 108+).

- For specific situations when personal data is transferred to territories lacking appropriate data protection, a number of derogations are foreseen, when: (i) the data subject has given consent; (ii) the specific interests of the data subject require such transfer in a particular case; (iii) there are prevailing legitimate interest, in particular important public interests which are provided by law and such transfer constitutes a necessary and proportionate measure in a democratic society; (iv) the transfer constitutes a necessary and proportionate measure in a democratic society for freedom of expression (Article 14(4) of the Convention).

AML/CFT contextualisation[42]

- Given the multilateral nature of mechanisms for international data transfers for AML/CFT purposes, the question of appropriate level of protection arises particularly in all cases where the exchange of personal data involves a country that does not have an (essentially) equivalent level of protection for personal data.

- There are several requirements in the FATF Recommendations addressed to public authorities regarding data security which applies when data crosses borders. The revised version of Recommendation 2 requires countries to have cooperation and coordination between competent authorities.

- Under its General Principles, the FATF[43] requires competent authorities, for all means and channels of international co-operation, to maintain appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities are required to protect exchanged information in the same manner as they would protect similar information received from domestic sources. Competent authorities should be able to refuse to provide information if the requesting competent authority cannot protect the information effectively.

- Information sharing on a client between OEs belonging to the same group (e.g. CDD data on the client, or the fact that a client has been subjected to the reporting of a suspicious transaction), less critical aspects if there are clear requirements and policies detailing what information can be shared and for what specific purpose, and

[41] Explanatory Report of Modernised Convention 108, para. 102.
[42] Relevant FATF Recommendations: Rec. 2, 40
[43] Recommendation 40

if the exchange of information occurs within OE located in the same country (subject, therefore, to the same requirements). However, there could be cases in which OEs belonging to the same group are operating from different countries, which may have different requirements (see considerations on Transborder Flows).

Recommendation

- It would be worthwhile considering the collaboration of DPAs, governments and international organizations to include data protection related rules and recommendations in international standards ailing with AML/CT matters to facilitate transborder low and a coherent implementation

- DPAs shall play an important role in line with art 15 (2) (b) of the modernised Convention 108 to ensure lawfulness of processing even in a transborder data flow context including and if relevant by referring individual cases on transborder transfers of data to national courts. DPAs shall have the power, resources and national, international institutional agreements in place to treat these issues in line with article 15 (2) (b) of the Convention 108+ and if relevant refer individual cases on transborder transfers of data to national courts.

- International data transfers shall only be allowed within the geographical limits of countries which offer an appropriate level of protection or appropriate safeguards[44], and assuming that the other requirements of the Convention for the processing of such data are met. This is applicable to any joint project or plans, such as pooling of data amongst financial institutions, particularly across national borders and with non-parties.

- Instruments that ensure an appropriate level of protection should be available in line with Article 14 (2) before sending personal data to data controllers located in countries or jurisdictions not bound by the rules of the Convention.

- States shall ensure that when exchanges take place towards a country that does not ensure an appropriate level of protection, safeguards established in applicable international data protection legislation and in particular in Convention 108+ shall be respected, including when the data transfer takes place on the basis of a bilateral/Common Reporting Standard (CRS) agreements[45].

- ~~DPAs shall have the power, resources and national, international institutional agreements in place to treat these issues in line with article 15 (2) (b) of the Convention 108+ and if relevant refer individual cases on transborder transfers of data to national courts~~.

- In the case of an OE belonging to a group where branches/subsidiaries are located in different countries, and domestic legislation does not prohibit the cross-border exchange of data, including on data protection grounds, such exchange of data should be based on ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing. provided that an appropriate level of protection is ensured during the transfer.

- FIUs from state Parties should exchange information with other competent authorities and with their foreign counterparts in compliance with the applicable requirements and limit the personal data processed to what is directly relevant to provide or obtain the requested information. In respect of personal data transfers to states not parties to the Convention, the requirements foreseen in Article 14 of the Convention should ~~be taken into account~~respected. There could be other standards applicable to the exchange of information, specifying requirements of data protection or data security, such as

[44] Art. 14 (4) of the Convention and paras. 109 to 112 of the Explanatory Report.
[45] The Common Reporting Standard (CRS) is an information standard for the Automatic Exchange Of Information (AEOI) regarding financial accounts on a global level, between tax authorities, which the Organisation for Economic Co-operation and Development (OECD) developed in 2014 with the purpose to combat tax evasion.

Egmont Group principles[46].It should be noted that the second additional Protocol to the Budapest Convention could give further guidance on applicable safeguards when it comes to international transfers between authorities and to some extent between authorities and private parties.

- State Parties should ensure that derogations from the requirement of an appropriate level of data protection are only allowed where the conditions set out in Article 14(4) are met.

- It would be worthwhile considering the inclusion of Data Protection rules and considerations directly into FATF Recommendations in order to facilitate harmonisation of their respective implementation.

[46] As approved by the Egmont Group Heads of Financial Intelligence Units in July 2013. https://egmontgroup.org/

Compilation of recommendations

Commented [A3]: This part has to be redone according to the changes made in recommendations above

For Obliged Entities

- When establishing business relationships with clients or conducting transactions for occasional customers, FIs and DNFBPs should inform the customer of his or her identity and habitual residence or establishment, the legal basis and the purposes of the intended processing, the categories of data that the FIs and DNFBPs (or other third parties) will be processing, the recipients or categories of recipients of the personal data, if any; the means of exercising the rights set out in Article 9 of the Convention and potential restrictions where appropriate, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data and the use made thereof in an understandable and user-friendly way.

- In the context of cooperation, such as PPPs, sharing of transaction data that implies processing of a high amount of data, the processing should be done, to the extent possible, with anonymized or pseudonymized data. Personal data identifying a person related to a transaction should be only limited when the outcome of the processing based on conditions linked to a reasonable suspicion/probable cause reveals patterns or activities that might require reporting of the transaction to the FIU as suspicious, or when it is needed to identify links to an identified terrorist.

- Clear and detailed provisions that take into account all rights and interests concerned shall be established in relation to PPPs created for the sharing of operational information on intelligence on suspects preventing obliged entities participating in PPPs from integrating information shared by law enforcement authorities in their own databases.

- Obliged entities belonging to a group should have clear policies and procedures to define what type of personal data (client, BO, transactional, account, suspicion transaction report –or STR-) can be shared among them on which legal basis and for what purpose.

- In the case of correspondent banking relations, there should be clear and detailed provisions between the correspondent and the respondent bank regulating the sharing by the respondent of personal data concerning its customers, BOs of the customers. The provision should detail the type of data that the respondent bank will have to provide upon the request of the correspondent bank.

- The purpose limitation principle should be clearly respected, both when automatic processing is carried out for several different purposes, or when it is based on the principle of unity of purpose.

- In the case of an OE belonging to a group where branches/subsidiaries are located in different countries, and domestic legislation does not prohibit the cross-border exchange of data, such exchange of data should occur only in countries that have AML/CFT systems consistent with the FATF recommendations, that allow for proper safeguards in the processing of the data and where the rule of law is respected. The foregoing is without prejudice to special provisions for Parties bound by harmonised rules of protection shared by states belonging to a regional international organisation in accordance with Article 14 (1) of the Convention.

- When AI is used (e.g. for transaction monitoring for the purpose of detection of suspicious activity), the criteria should be calibrated in a way not to generate an excessive number of alerts, especially false positive ones, including the case of customer/BO/recipient of transaction name-searching and matching with sanction lists.

- If obliged entities are using programs for risk profiling of the customers or the beneficial owners, appropriate measures should be taken to correct data inaccuracy factors and limit the risks of errors inherent to profiling. The periodic (or trigger-based) reassessment should also include a re-evaluation of the data and of the statistical inferences including for the elimination of potential biases used for the risk profiling, to determine whether they are still accurate and relevant.

- If OEs are using external database providers for implementing customer diligence requirements on their clients and beneficial owners (e.g. identity verification of the customer and beneficial owner, identification of potential relations with PEPs, and family members and close associates to the PEP) they should strive to verify that data is accurate and up-to-date and to conduct a periodic evaluation of the accuracy of the data made available by the provider.

- The OE receiving data on customers, beneficial owners and transactions is considered to be the controller of the data and should be held responsible for the processing of the data as well as for its accuracy, even in the case in which the obliged entity uses third parties for the collection and processing of such data. Those third parties might be deemed processors according to Convention 108+.

- If there are no storage limitation requirements and/or those in place are not in line with FATF Recommendation[47], data should be stored for the minimum period necessary, and be deleted or anonymised as soon as are no longer needed for the purposes for which they were collected.

- Compliance with the principle of data security requires technical and organisational measures such as (hard, end-to-end) encryption of the data and rules on the full traceability of the exchanges, especially through the implementation of access logs.

- Personal data relating to offences, criminal proceedings and convictions, as well as related security measures are a part of the aforementioned special categories of personal data which are also relevant to AML/CFT. Processing of such data may only be carried out when appropriate safeguards are in place (e.g. professional secrecy obligation; measures following a risk analysis; a particular and qualified organisational or technical security measure such as data encryption)[48].

- Registers holding information on criminal convictions may be subject to the control of competent supervising authorities and should respect requirements for the processing of special categories of data.

- Measures shall be put in place by controllers to facilitate the exercise of these rights by the data subject, in principle free of charge. In case of automated decision making and according to the right not to be subject to purely automated decisions without the possibility to challenge the decision (Article 9.1a), the information on the decision and the logic underpinning the processing of the data should be available upon request of the data subject. Intellectual property law should not be an excuse for data controllers to provide data subjects with the logic and training of the algorithms applied in the specific processing operation.

- In the case of the right to object, the Explanatory report (para. 80) indicates that even when this right is limited for the purpose of the investigation or prosecution of criminal offences, the data subject can challenge the lawfulness of the processing.

[47] FATF Recommendation 11
[48] See Explanatory Report to Convention 108+, para 56.

For governments

- There must be a clear regime for the classification of information and its review including procedures by through which secrecy and confidentiality – where applicable – can be waived.

- Regarding central beneficial ownership registries, information should only be available in the cases provided by law, and in compliance with data protection regulations.

- FIUs from state Parties should exchange information complying with the requirements of the data protection legislation of the data-provider and of the data-recipient countries notably with the ones foreseen in Article 14 of the Convention. [In the AML/CFT field the exchange should also be consistent with Egmont Group principles.]

- Data should be used for the sole purpose for which it was provided and cannot be transferred to other authorities of the data-receiving countries, unless the requirements laid down in the Convention are complied with.

- There should be specific requirements for OEs to implement state of the art, strict security measures for ensuring the protection of personal data, particularly in the case of special categories of data (e.g. on PEPs, which could reveal political affiliations or sexual orientation in the case, for example, of a same-sex partnership).

- All entities involved in AML/CFT, including private entities, FIUs and Law Enforcement Agencies shall ensure training to their staff, especially in regard to dealing with special categories of data.

- AML/CFT operations should be subject to effective and independent ex-ante and/or ex-post authorisation and/or review based on the domestic legal framework

- In addition, DPAs should be tasked and empowered to ensure compliance with applicable data protection regulations.

- In the AML/CFT field, DPAs shall have coordinated activities with the OEs in order to supervise the processing of data and to suggest effective tools and modus operandi for effective supervision.

- And in regard to the above, the DPA shall contribute as much as possible to the empowering of the OEs and data subjects with internal training.

- DPAs should engage with other national authorities that oversee AML/CFT issues for joint activities in the enforcement area.

- Data transfers shall only be allowed within the geographical limits of countries which offer an appropriate level of protection or appropriate safeguards (Art. 14 (4) of the Convention, and para. 109 to 112 of the Explanatory Report), and assuming that the other requirements of the Convention for the processing of such data are met. This is applicable to pooling of data amongst financial institutions, particularly across national borders and with non-parties.

- Instruments that ensure an appropriate level of protection should be available in line with Article 14 (2) before sending personal data to data controllers located in third countries or jurisdictions not bound by the rules of the Convention.

- States shall ensure that when exchanges take place towards a country that does not ensure an appropriate level of protection, safeguards established in applicable international data protection legislation shall be respected, including when the data transfer takes place on the basis of a bilateral/CRS agreements.

- Supervisory authorities shall have the power to treat these issues in line with article 15 (2) (b) of the Convention 108+ and if relevant refer individual cases on transborder transfers of data to national courts.]

CHAPTER II

Commented [A4]: Chapter II is to be developed with the support of a scientific expert

Draft guidelines on mechanisms for inter-state exchanges of data for tax purposes and Data protection

Annex 1 to Chapter I

- Collection of data regarding PEPs could reveal political affiliations or sexual orientation (in the case, for example, of a same-sex partnership). Therefore, processing of such categories of personal data could only be lawful if granted enhanced protection.

- Beneficial ownership information – According to the FATF definition, the beneficial owner is always a natural person (or more than one) ultimately owning or controlling a customer, legal person or arrangement and/ or the natural person on whose behalf a transaction is being conducted. Datasets mainly include beneficial owner identification and contact information (the full name, nationality (ies), the full date and place of birth, residential address, national identification number and document type, tax identification number or equivalent in the country of residence), real estate holdings, information on the source of funds and wealth, on the professional activity, information on whether the beneficial owner is a PEP. The relevant identification data may be obtained from a public register, from the customer or other reliable sources. In order to be considered adequate, information has to allow the identification of the natural person who is the beneficial owner and the means and mechanisms through which they exercise beneficial ownership to control. In order to be accurate, the information has to be verified using reliable, independent sources/obtained documents, data or information, to the extent needed according to the specific level of risk. The information has to be current and updated within a reasonable period following any change.

- Financial data may include account information (such as bank account details and intended purposes of the account) and transactions information (transaction records, card records and use, past credit history, IP address, ATM usage information, information on closure or account or termination of business relationship due to suspicion, analysis conducted on a transaction pattern in the context of the financial profile). This data constitutes some of the most sensitive data about individuals, revealing their financial standing, family interactions, behaviours and habits, the state of their wealth etc (page 27 Stocktake 2021).

- Statistical data – Under the FATF Recommendation 33, countries are required to maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems, which should include statistics on (i) STRs received and disseminated; (ii) ML and TF investigations, prosecutions and convictions; (iii) on property frozen, seized and confiscated and on (iv) mutual legal assistance or other international requests for cooperation. One of the main challenges

identified is the lack of international consensus and guidance on which specific types of data should be collected[49].

- Under the FATF Recommendation 24, data processing is required for "nominee shareholder or directors", which may also include personal data processing. A nominee shareholder refers to an individual or legal person acting in a certain capacity on the behalf and subject to the instructions of another individual or legal person ("the nominator[50]") regarding a legal person. A nominee director is an individual or legal entity that routinely exercises the functions of the director in the company on behalf of and subject to the direct or indirect instructions of the nominator. A Nominee (Director or Shareholder) is never the beneficial owner of a legal person.

- Under the FATF Recommendation 25, data processing, including of personal data, is required for trusts and other legal arrangements, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership. The terms "trust" and "trustee" should be understood as described in and consistent with Article 2 of the Hague Convention on the law applicable to trusts and their recognition[51]. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non- professional (e.g. a person acting without reward on behalf of family).

- Public authorities are to set the storage of data for the purpose of combating crime and for this a previous recommendation confirmed the need to draw a distinction according to the nature or degree of seriousness of the offence or depending on whether the data subject is only a suspect.

[49] FATF Guidance on AML/CFT-related data and statistics, page 10.
[50] A Nominator is an individual (or group of individuals) or legal person that issues instructions (directly or indirectly) to a nominee to act on their behalf in the capacity of a director or a shareholder, also sometimes referred to as a "shadow director" or "silent partner".