16 June 2023 T-PD(2021)8rev8FINAL

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

CONVENTION 108

Guidelines on data protection for the processing of personal data for anti-money laundering/countering financing of terrorism purposes

www.coe.int/dataprotection

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.

AML/CFT policies include relevant data processing and sharing which must be carried out in full respect of the applicable data protection frameworks, in particular the Convention for the protection of individuals with regard to the processing of personal data (ETS No. 108) as amended by the Protocol CETS No. 223 ("Convention 108+"), as illustrated in the following sections.

The 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 Article 8 of the European Convention on Human Rights (ECHR) and other international human rights instruments such as Article 12 of the Universal Declaration of Human Rights (UNDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 11.2 of the American Convention on Human Rights (ACHR), Article 4 of the African Charter on Human and People's Rights (ACHPR). According to the case-law, an individual's private life shall be interpreted in a wide sense, including information pertaining both to his/her private sphere as well as professional or public life. Article 2 (a) of the Convention 108+ also establishes that 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). According to Article 11 of the 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 ML/FT 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. At the same time, their role and concrete obligations as gatekeepers to prevent misuse of the financial system for ML/FT is to be duly recognised as well. However, 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).

[1] 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. Global AML/CFT Standards: the FATF Standards.

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, because it would not be in line with core data protection principles. Moreover, 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.

Recent developments have also highlighted the need for further guidance in important areas such as the general public's access to information on beneficial ownership[2], which was deemed to constitute a serious interference with the rights to respect for private life and to the protection of personal data[3] as it made public a large amount of personal data on beneficial owners in a country. This case shows that this area is in constant evolution and more regulation, including hard law, but also further jurisprudence in this field are expected to come in the near future.

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 State Parties' 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 fields. Considering that data processing and sharing are crucial in combatting ML/TF, these guidelines[4] aim to emphasize the requirements needed for compliance with data protection obligations included in Convention 108+ by controllers and processors, while complying with the AML/CFT framework.

1.2 Scope

The purpose of these guidelines is to provide orientation on how to integrate the requirements of Convention 108+ in the area of AML/CFT in order to provide for an appropriate level of data protection while facilitating transborder data flows, and to highlight certain areas in the AML/CFT context where data protection safeguards should be strengthened.

These guidelines also aim at providing governments and policy makers with basic recommendations that should 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.

[2] See the definition of "beneficial ownership information" under Annex I.
[3] ECJ judgement of 22nd of November 2022 in joined cases C-37/20 Luxembourg Business Registers and C-601/20 Sovim.
[4] The Guidelines have been developed taking into account contributions from several members, experts and the Secretariat of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL).

Personal data and data subject – Article 2 (a) of Convention 108+ 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. In the AML/CFT context, customers, beneficial owners (BOs)[5], 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[6], 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 and arrangements in order to protect their legitimate interests[7], 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 Convention 108+). The aforementioned operations shall only be performed when controllers 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 or arrangement[8], 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[9]. Controllers are bound to ensure the legitimacy of data processing (Article 5 of Convention 108+).

From an AML/CFT standpoint, OEs are controllers alone or jointly. The OEs include financial institutions[10] (FI), designated non-financial businesses and professions[11] (DNFBPs), virtual asset and service providers (VASPs). Recipients of the information such as FIUs, law enforcement authorities, or other entities including public authorities holding registers of basic and beneficial ownership information are to be considered also data controllers for the processing of personal data they perform.

[5] 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.

[6] 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).

[7] Explanatory Report of Convention 108+, para. 30.

[8] While Convention 108+ refers to "legal persons" in its Article 2, the FATF Standards operate a distinction between legal persons and legal arrangements. For further details, please see Appendix 1.

[9] Explanatory Report of Convention 108+, para 22.

[10] The term Financial Institution (FI) in the AM/CFT field as used throughout these Guidelines include both credit and financial institutions.

[11] Such as casinos, real estate agents, dealers in precious metals and precious stones, lawyers, notaries, other independent legal professionals and accountants (when acting as sole practitioners, partners or employed professionals within professional firms), and trust and company service providers (when providing certain services). Certain sectors are however not always appropriately captured (e.g., in-house lawyers and accountants).

The AML/CFT framework may provide for different situations of information sharing, including between OEs; between legal persons or arrangements and controllers of beneficial ownership registers; between OEs and FIUs or between OE and other competent authority ("public-private partnerships/PPP); between the FIUs, LEAs and judicial authorities 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 the purpose for which the personal data is processed, they should be considered to be joint controllers[12]. 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.

Data processors in AML/CFT – A processor is the natural or legal person or arrangement 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 difference 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.

Special categories of personal data (sensitive data) – Under 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 personal data in general. 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) biometric data processed for the purpose of uniquely identifying a person, (vi) concerning health, (vii) sexual life or sexual orientation, (viii) relating to offences, criminal proceedings, convictions and related security measures

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+). Therefore, further processing of data may not be done in a 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[13].

[12] 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).
[13] Explanatory Report of Convention 108+, para. 49.

- If the purpose of further processing is 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 have other legal basis for subsequent processing.

AML/CFT contextualisation[14]

- 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 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 customer of the respondent bank, which would have been collected by that bank from its customer in a different context. It may sometimes be necessary to share data even with third parties[15], where it is strictly necessary to carry out the CDD obligations. Such operations are to be carried out in compliance with the secrecy obligations and applicable rules on the protection of personal data.

- 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.

- There could be instances where data collected and processed for a defined purpose (e.g. customer due diligence information or suspicious transaction information) may be shared with third parties. For example, an FIU analysing a suspicion transaction report (STR), finding international links that require relevant information from the STR (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 generally governed by other laws.

- Personal 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 Convention 108+ are complied with.

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[16].

[14] Relevant FATF Recommendations: Rec. 10-12,13, 15-18, 20, 22-27, 29, 31, 40.
[15] In this context, “third parties” should be interpreted as any natural or legal person that is external to and does not form part of the obliged entity or its financial institution.
[16] Explanatory Report of Convention 108+, para. 49.

- OEs belonging to a group should have clear policies and procedures based on law to define what type of personal data (customer, BO, transactional, account, STR) that could be shared among them[17], the legal basis and the purpose. This could be achieved in line with the requirements of Article 14 of Convention 108+ including approved standardised safeguards such as binding corporate rules (BCRs) or Model Contractual Clauses (MCC) or ad-hoc clauses provided by legally binding and enforceable instruments.

- The FIUs, for the processing of personal data in STRs, should have clear rules and procedures based on law, which should also prescribe the purposes for which personal data relating to STRs may be shared with other competent authorities[18].

- When personal data are processed in a third-party[19] reliance scenario[20], both parties should have clear rules and procedures in place that regulate not only the provision of information for CDD purposes, but also adequate safeguards for the protection of personal data processed for a given purpose.

- In relation to cross-border correspondent banking and other similar relationships[21], there should be clear and detailed provisions based on law between the correspondent and the respondent institutions, including banks 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. The same may apply to relevant relationships outside the banking area (e.g., investment firms, payment institutions). 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 recipients including national law enforcement agencies[22] but also to foreign FIUs[23]. 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.

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 and revocable at any time which are further explained in the Explanatory Report[24].

[17] FATF Recommendation 18; C. 108+ arts. 5 (1), 14 (2) (3); ER para. 40, 42, 109-111.
[18] FATF Recommendation 29; C 108+ art. 10; ER para. 85
[19] In this context, the term" third parties" refers to Fis or DNFBPs that are supervised or monitored and that meet the requirements under the FATF Recommendation 17.
[20] The party being relied upon for CDD purposes will hold information and documentation on the same customer which is provided or made available to the obliged entity placing the reliance
[21] FATF Recommendation 13; C. 108+ art. 14 (2) (3); ER para. 109-111.
[22] FATF Recommendations 29 and 31.
[23] FATF Recommendation 40; also C. 108+ art. 14 (2) (3); ER para. 109-111.
[24] Convention 108+, Art. 5(2); Explanatory Report of Convention 108+, paras. 42-45.

- The notion of "legitimate basis laid down by law" encompasses, *inter alia*, data processing 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 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[25]

- 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.

- As explained before, 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. In the AML/CFT context, the question of a "freely" given consent should be carefully considered and it should be ensured that the data subject has a choice. If this is not the case, the data processing has to be based on a different and valid legal basis. The AML/CFT framework often involves specific investigations into suspicions of or actual ML/TF activities, provides for situations where the customer is not or only partially informed of the data processing, particularly in relation to suspicious transaction reporting obligations by the OE, the provision of personal data in response to requests for information by FIUs and LEAs and the application of monitoring orders. In those cases, prior information of the customer would contravene to AML/CFT prohibitions, in particular to tipping-off[26].

- Processing of personal data by public authorities can be based on the lawful ground of public interest, given they are entrusted with the mandate to combat AML/CFT and are entrusted with specific tasks in this area. Checks and balances as well as oversight are also implemented. The same does not extend necessarily to private sector institutions which are obliged entities and have a different legal status and mandate.

- Processing of personal data by OEs in the AML/CFT context should be based on a clear and detailed legal basis that provides for the principles of necessity and proportionality to which the controllers are subject[27]. Failure by OE to comply with those obligations would entail risks of measures taken by supervisory authorities, including administrative and criminal sanctions. Failure by customers to provide the requested data could, in turn, result in that the transaction or customer relationship is not being concluded or in the restriction of services.

- For example, data processing is required to prevent the misuse of legal persons and arrangements for ML or TF by ensuring that there is adequate, accurate and up-to-date information on beneficial ownership and control of legal persons and arrangements [28]. Beneficial Ownership Information should be accessible in a timely manner by a competent authority through either a register of beneficial ownership or an alternative mechanism. [] At the same time, when providing access to BO information, competent authorities should duly take into account the right to the respect for privacy of the persons concerned, taking account of and impact such an access can make on her or his rights and freedoms.
- The existence of information sharing initiatives through Public-Private Partnerships (PPPs) has been noted in several jurisdictions. While the opportunities they provide in the fight against financial crime are significant, there are remaining challenges which

[25] Relevant FATF Recommendations: Rec. 24, 25.
[26] FATF Recommendation 21.
[27] Explanatory Report of the Convention 108+, para. 46.
[28] FATF Recommendation 24.

are also of a legislative and of compliance nature (e.g., legislative amendments may be needed to ensure a proper legal basis and allow partners to achieve their objectives.

Recommendation

- Data processing in the context of AML/CFT should be carried out on the basis of a clear and detailed legal basis respecting the principles of necessity and proportionality and with appropriate safeguards.

- Due regard has to be given to the mandate with which public authorities are entrusted and can be held accountable for non-compliance with their legal obligations. Public interest as a legal basis for data processing emerging initiatives by private sector entities subject to AML/CFT obligations should be properly substantiated and carefully scrutinised.

- 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 and intelligence on suspects including with regard to personal data shared by law enforcement authorities and the clear legal basis for the subsequent processing. These rules should specify the conditions of the processing, including: the specific purposes for which data sharing and other processing are allowed; the necessary dataset to be submitted by OE ensuring that only personal data that is strictly necessary for the on-going operational analysis or investigation is disclosed and shared; the appropriate safeguards to ensure data subjects' rights; the appropriate safeguards, complementing those of the Convention for special categories of data.

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

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 Convention 108+). This principle requires 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, unless an exception applies in line with the Convention. 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 Convention 108+). 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 all purposes of joint processing, the means, procedures and modalities of exercising the rights set out in Article 9, to provide transparency[29]. In doing so, one needs 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.

[29] European Data Protection Board: "Guidelines 07/2020 on the concept of controller and processor in the GDPR". Version 2.0. July 7th. 2021.

- 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 Convention 108+).

AML/CFT contextualisation[30]

- Data processing for public interest should not be considered by definition as fair, data controllers in the public sphere need to comply with those principles unless an exception applies in accordance with Article 11 of Convention 108+.

- OEs are required[31] to undertake CDD measures when for example (i) establishing a business relationship, (ii) carrying out occasional transactions above the applicable designated threshold, (iii), when carrying out occasional transactions that are wire transfers[32], (iv) when there is a suspicion of ML/TF, or (v) when there are doubts about the veracity or adequacy of previously obtained personal data. OEs 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[33]. OEs 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. OEs, 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.

- In some cases, besides data protection regulations, there are banking secrecy[34] or other professional secrecy obligations that apply to legal professionals such as lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals. They are not required to report suspicious transactions or provide customer information to LEAs or FIUs when such information would be obtained: (a) in the course of ascertaining the legal position of their customer, or (b) in performing their task of defending or representing that customer in, or concerning judicial, administrative, arbitration or mediation proceedings[35].

- To facilitate access to accurate and up-to-date beneficial ownership information some States have created central registries, with information provided by legal persons and arrangements. 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.

[30] Relevant FATF Recommendations: Rec. 10, 22 and 23.
[31] FATF Recommendation 10 sets out these requirements as the minimum standard that countries should put in place.
[32] In the circumstances captured by FATF Recommendation 16 on wire transfers.
[33] FATF Recommendation 10.
[34] FATF Recommendation 9 mandates that financial institution secrecy laws should not inhibit the implementation of the FATF Recommendations.
[35] FATF Recommendation 23.

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 Convention 108+ 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.

- 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.

- Public access by default to personal data in central beneficial ownership registries constitutes a serious interference with the human rights, including the right to privacy and to the protection of personal data and should only be allowed in the situations or to the extent provided by law, and in compliance with data protection regulations, notably the necessity, proportionality and purpose limitation principles. Access to publicly non available data shall be carefully managed taking into account the domestic legislation, rights and interests concerned.

3.4 The data minimisation principle

General principle

- Data processing must be limited to what is necessary to fulfil a legitimate and a pre-determined 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 one or multiple processors.

- 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 giving due account to 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 is required on the basis of risks for certain types of customers (e.g. politically exposed persons (PEP[36]) or where ML/FT risks are higher) 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.

[36] According to the FATF Standards, Politically Exposed Persons (PEPs) are classified as: (i) Foreign PEPs, (ii) Domestic PEPs, and (iii) Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories. Please see Annex 1 for further detail.

- In practice, it appears that, in many instances, private sector entities may lack clear and specific guidance needed on collecting customers' personal data as part of AML/CFT obligations. For instance, regarding specific datasets to be collected as part of the CDD obligations, OEs need to observe both data protection and AML/CFT legal obligations and may struggle to understand how to achieve both goals in a consistent and compatible way, notably with regard to the application of the data minimisation principle. As a result, by fear of exposing themselves to reputational and other risks caused by (i) the unintended processing of proceeds of crime or (ii) the possibility of being subject to administrative fines or action by competent supervisors of both financial institutions and DNFBPs, private sector entities may end up sharing larger volume of data "just in case". In that sense, the proper implementation of a risk-based approach from an AML/CFT perspective would also allow for alignment with the proportionality requirement envisaged under data protection requirements. An effective application of a risk-based approach requires a clear and practical guidance and training by supervisory authorities, investment in resources and expertise by OEs, and a proportionate application and enforcement of AML/CFT national laws.

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.

- 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, notably with respect to the risk-based approach which necessitates a certain degree of flexibility whereas the principle of data minimisation is clearly provided for in national data protection law. It is 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 by LEAs as well, 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 this respect, controllers, and, where applicable, processors, should ensure that data protection requirements are integrated ideally at the stage of architecture and system design, in data processing operations through technical and organisational measures.

- In the context of PPP, sharing of transaction data that implies processing of a high amount of data, the processing should be done, where appropriate, with anonymised or pseudonymised data. The identification of 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, modus operandi or concrete 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. For instance, when data processing is conducted for identifying trends, patterns and typologies, there is no necessity to use personal data.

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

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 factually misleading, 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[37]

- OEs are required to ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records, and conducting ongoing monitoring, which should happen at a regular frequency for higher risk categories of customers[38].

- OEs may use external providers of information for various purposes (e.g., sanction screening, identification of PEPs, family members and close associates), which, if supplied with inaccurate or outdated personal data, can yield inaccurate outcomes for CDD or other AML/CFT purposes (e.g. reporting). They might 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 not properly calibrated may result in false positive hits/undetected cases and/or an excessive number of alerts, that cannot be processed in a lawful manner. While the FATF Recommendations do refer to the requirement of ensuring accuracy of the information, concrete implications of verifying the accuracy of all personal data is yet to be determined as 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[39]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+. Therefore, and also based on the FATF Recommendations implying to verify all personal data, the aforementioned requirement to keep CDD data and information up to date applies even to situations where third parties are relied on.

[37] Relevant FATF Recommendations: Rec. 6, 7, 10, 17, 24, 37, 40.
[38] FATF Recommendation 10.
[39] FATF Recommendation 17.

- Countries are required to have mechanisms in place to ensure that beneficial ownerships information is obtained by the company or otherwise available in a timely manner[40] In practice, AML/CFT laws typically require the same for other legal entities entered in BO registers. It is further required 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) is made publicly available in a company registry, and also envisages the possibility to require companies or company registries to obtain and hold BO information[41].

- 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[42].

Recommendation

- OEs should 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), it is important that it is carried out strictly in compliance with the rules on data protection and in particular, with the obligations set out Article 10(3) for controllers, and, where applicable, processors to implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing. Furthermore, 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 unless the data processing is authorised by law to which the controller is subject to and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. This would entail that, based on the data subject's request a human intervention needs to occur from the staff of the entity collecting the information 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 one obtained only through automated means). The data subject concerned should be given the opportunity to present his/her views unless the data processing is authorised by law to which the controller is subject to and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. Such safeguards could include a requirement to: a) provide the necessary additional information to data subjects, b) ensure fair and transparent processing, c) highlighting the use of solely automated processing as well as its purpose and potential impact on the data subject in line with Article 8(1), and Article 9(1)(b). In addition, the criterion for the processing 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[43].

- If OEs are using 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. When it comes to the processing of personal data by new processing techniques and technologies, OEs are invited to follow Recommendation

[40] FATF Recommendation 24.
[41] Ib idem.
[42] FATF Recommendations 37 and 40.
[43] FATF Recommendation 6 and 7; Convention 108+ Articles 9 (a), 10 (1); Explanatory report para. 71-73, 75 and 85.

CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling[44] and the Guidelines on artificial intelligence and data protection[45].

- 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 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 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 implement the privacy by design when setting up the system for the processing of personal data, including during the phase of embedding and automating the update review.

- Without prejudice to data protection and security standards, 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 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.

[44] Result details (coe.int)
[45] https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

AML/CFT contextualisation[46]

- Clear requirements are set for the record keeping period of CDD information, account files, business correspondence and results of any analysis undertaken (currently set as at least for 5 years following the termination of the business relationship or after the occasional transaction) and records on domestic and international transactions (at least 5 years following completion of the transaction)[47].

- Data processing is required in order to prevent the misuse of legal persons and arrangements for ML or TF by ensuring that there is adequate, accurate and up-to-date information on beneficial ownership and control of legal persons and arrangements[48]. 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 in its dissolution) 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 ceases to exist 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

- Personal data should, in principle be stored, in line with Article 5 (4) (e) of Convention 108+ for 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. It is generally recommended that storage limitation requirements are periodically reviewed.

- Regarding the storage of personal data by public authorities for the purpose of combating crime, a distinction should be made in terms of length of time of storage depending on the nature of the offence or depending on whether the data subject is only a suspect in accordance with the requirement that personal data may only be processed as long as it is necessary for the specific purpose.

- Cooperation at a national level between data protection authorities and other supervisory authorities[49] should be facilitated so that specific guidance could be developed to ensure a balance between applicable legal obligations, both from an AML/CFT and data protection perspective, including regarding the issue of data retention. This type of cooperation could be enhanced, for instance, by: (i) holding joint meetings between DPAs and other supervisory authorities on AML/CFT and Data Protection, (ii) issuing joint guidelines on linked aspects, such as the technology needed (e.g. the level of encryption or multiparty computation), the necessary datasets required for processing to achieve AML/CFT goals, or how data subjects should be able to exercise their rights vis-à-vis data controllers (iii) organising consultations with the DPAs[50] in the context of drafting standards, guidelines and recommendations as well as the possibility with dialogue with other supervisory authorities; (iv) DPAs could

[46] Relevant FATF Recommendations: Rec. 2, 11, 24, 25, 29, 40
[47] FATF Recommendation 11.
[48] FATF Recommendations 24 and 25.
[49] This notwithstanding that the data protection legislation implementing Convention 108+, particularly Article 15, provides for the tasks and powers of the DPAs. Any Recommendation concerning cooperation between DPAs and other supervisory authorities (AML/CFT authorities) should be in line with the tasks and powers of the DPAs, and particularly the independent supervisory role of DPAs.
[50] The DPAs are also regularly consulted on legislative proposals, including in the context of public consultation. The possibility of consultation is also used at the EU level: EDPB letters to the European institutions on the protection of personal data in the AML-CFT legislative proposals | European Data Protection Board (europa.eu)).

also be invited to participate in informal PPP meetings, where also private sector entities have the possibility to attend in addition to the competent authorities, (v) involving DPAs in the review of different guidance documents explaining how FIs/DNFBPs should comply with each of their AML/CFT obligations, in order to ensure that these documents provide sufficient detail and guidance on DPP requirements and how OEs can meet both sets of requirements. This could also help identify areas where there is any policy incompatibility – which could then be addressed by a different forum (e.g., through legislation).

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 Convention 108+). 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[51].

- 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[52]

- 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 will have (albeit only indirectly) an impact for the security of data when processed and exchanged by OEs.

- Ensuring the confidentiality of STRs is essential to the effectiveness of the reporting regime, by avoiding tipping-off the subject of the STR as well as third parties, as this can adversely impact intelligence gathering and is likely to prejudice investigative efforts, including enable relocation 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 in effect 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

[51] 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.
[52] Relevant FATF Recommendations 2, 21,29, 40.

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[53]. In addition to FATF, the Egmont Principles also set security measures for the exchange of information. Furthermore, requirements of using secure channels are foreseen for information exchange, applicable to competent authorities such as investigative authorities[54].

- 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, data which could reveal political affiliations or data on 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, where applicable, 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

As mentioned above, all information can be personal data provided that it allows or permit the identification of a natural person. The identification does not have to be direct, information that could possibly lead to the identification of an individual together with other information, even if only remotely accessible, would also amount to personal data.

[53] FATF Recommendation 29.
[54] FATF Recommendation 40.

In parallel, there are special categories of personal data defined by Article 6 of Convention 108+ which requires that appropriate safeguards are enshrined by law, complementing those of the Convention. Those data are: 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. This includes data where such information can only be derived or inferred from. Such data are subject to additional safeguards complementing those already in place for "personal data in general" and can only be lawfully processed under a limited number of conditions.

AML/CFT contextualisation[55]

- To mitigate ML/TF risks, the private sector is required to undertake measures focused on collecting, processing and securely sharing relevant data to competent authorities (e.g. supervisors and LEAs, at a national and sometimes an international level usually through their national FIUs) and within financial groups for AML/CFT purpose for the prevention, detection and reporting of customers and transactions suspected of ML, associated predicate offences and TF:
    - information sharing within the context of financial group is required both for customer due diligence purposes and ML/TF risks management[56];
    - 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[57];
    - knowing their customers and monitoring their accounts and activities as appropriate for AML/CFT purposes[58] 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 least five years[59], as financial crime investigations often require considerable periods of time;
    - being able to detect and report suspicious transactions[60] and ensure that customers are not aware that an STR or underlying information is filed with authorities[61]. It is also to be acknowledged that certain special categories of data, notably those which relate to contributions to ideological/political organisations, payments of fines etc. are still currently being processed regardless of any extra AML/CFT checks stemming from legal obligations set out by other international crime-preventing frameworks.
    - AML/CFT purposes may lead to the processing of special categories of data which deserve a strengthened protection according to Article 6 of Convention 108+, but currently, sensitive data is rarely requested for AML/CFT purposes. For instance, in instances where customers may have to identify themselves as part of a same-sex relationship, the OE only needs to know that the customer falls within the definition of a family member or close associate of a PEP, without necessarily needing the know the nature of the relationship.

[55] Relevant FATF Recommendations: Rec. 1, 10, 11, 18, 20, 21
[56] FATF Recommendation 18.
[57] FAFT Recommendation 1.
[58] FAFT Recommendation 10.
[59] FAFT Recommendation 11.
[60] FAFT Recommendation 20.
[61] FAFT Recommendation 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.

Recommendation

- AML/CFT and Data Protection Authorities, within their respective competences shall ensure that for any given data processing both AML/CFT and Data Protection requirements are satisfied.

- OEs should not process special categories of data which are not directly linked to the purpose pursued which shall be determined following a thorough assessment on the necessity and proportionality of the processing of each category of sensitive data[62].

- 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)[63].

- Registers holding information on criminal convictions should be restricted to the competent authorities, or to processing under the control of those 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 other types of sensitive data) is necessary and proportionate 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.

- Guidelines should be provided by supervisory authorities for the processing of special categories of personal data including on the appropriate and complementary measures to safeguard the rights and freedoms of individuals concerned and that decisions by OE and competent authorities should not be based solely on these categories of personal data.

- 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, 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.

[62] Special categories of data according to Article 6 of Convention 108+: 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.
[63] See Explanatory Report to Convention 108+, para 56.

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 Convention 108+:

    - 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 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 Convention 108+, 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[64]

- Some of the rights expressed in Convention 108+ can be restricted for AML/CFT purposes and usually the restrictions based on AML/CFT laws rely on general public interest (i.e., the integrity of the financial system; 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 – and OEs in line with Article 8 of Convention 108+ are to inform customers that their personal data may be used for AML/CFT purposes including during further analysis, facilitating the exercise of data subject rights.

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, if no exception applies, the information on the decision should be available upon request of the data subject. The right not to be subject to only automated decision making should also apply even if AI is used with respect also to the analysis of transaction data and to the decision whether or not a transaction is suspicious and will be transmitted to the FIU. Clear rules and instructions should be provided, in line with Article 11, regarding if and when data subjects can exercise their right, or if an exception apply and how the "tipping – off" requirement[65] 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 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 structured data embedded in the architecture).

6. Exceptions and restrictions (Article 11)

General principle

- Only exceptions to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9 of Convention 108+ can be made, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society.

[64] Relevant FATF Recommendation 21.
[65] FATF Recommendation 21.(b)

The use of these exception may in no way derogate from the obligation to ensure that data processing is carried out by lawful means, on an appropriate legal basis and in a way that is proportionate to the aim pursued, taking into account the interests at stake and the impact on individual rights and freedoms.

It can be of relevance to note with reference to processing activities for national security and defence purposes that in addition to the exceptions specified above exceptions can be made to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d. provided they are set forth by law and that they constitute a necessary and proportionate measure in a democratic society to fulfil the aim of the processing.

This is without prejudice to the requirement 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.

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 enhanced due 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 requirements. Furthermore, any exception to the right of access of customers should be used by competent authorities, to the extent that, and for long as such a measure comply with the conditions laid down in Article 11 of Convention 108+ (i.e. provided for by law, respect the essence of fundamental rights and constitutes a necessary and proportionate measure in a democratic society.)

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 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 AML/CFT authorities

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 Convention 108+ provide for means of cooperation and mutual assistance between data protection supervisory authorities.

AML/CFT contextualisation

- The activities necessary to comply with AML/CFT regulations involve the activity of multiple actors in different, sometimes multiple jurisdictions, and the processing of large volumes of personal data. Convention 108+ foresees that the powers of the supervisory authorities notably with regard to investigation, intervention, authorising, blocking transborder flow of personal data apply for data processing for AML/CFT purposes. While no restrictions can be made to the use of these powers when the data is processed for law enforcement (and other general public interest) purposes, Article 11(3) foresees that with reference to the processing for national security and defence purposes some of these powers can be restricted (Article 11 (3)) provided that such restriction is set forth by law, respect the essence of fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society. Even in the latter case Convention 108+ 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, coherent and independent ex-ante authorisation and/or ex-post review based on the domestic legal framework in accordance Art 11(3) of Convention 108+. This can include that national legal frameworks provide for a specific level of security clearance for designated 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 competent AML/CFT authorities (at national and international levels possibly) should be emphasised in order to suggest effective tools and modus operandi for compliance by developing practical guidance for both public and the private sector and to ensure, where relevant specific trainings.

8. International data transfers in the AML/CFT field

General principle

- Transborder data flows occur when personal data is disclosed or made available to a recipient who is subject to the jurisdiction of another State or international organisation[66].

- 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 (Article 14(1) of Convention 108+).

[66] Explanatory Report of Convention 108+, para. 102.

- 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 provided they respect the principles of necessity and proportionality, 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 Convention 108+).

AML/CFT contextualisation[67]

- 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. For instance, under FAFT Recommendation 2, countries are required to have cooperation and coordination between Data Protection Authorities (DPAs) and AML/CFT authorities to ensure that data protection principles, rules and considerations are appropriately integrated into AML/CFT obligations.

- The FATF[68] 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 customer between OEs belonging to the same group (e.g. CDD data on the customer, or the fact that a customer has been subjected to the reporting of a suspicious transaction), is usually considered as less critical if there are clear requirements and policies detailing what information can be shared and for what specific purpose, and 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).

[67] Relevant FATF Recommendations: Rec. 2,18, 40.
[68] Recommendation 18.

Recommendation

- OEs should, in line with Article 14 of Convention 108+ 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. If no exception according to Article 14.4 applies, such assessment of the country or organisation of destination should aim to ensure that the level of protection afforded by Convention 108+ is guaranteed by the recipients and that the data subject is able to defend his or her interests where there is non-compliance. OEs should also take into account the enforceability of data subjects' rights and the provision of effective administrative and judicial redress for the data subjects whose personal data are being transferred.

- It would be necessary to ensure the collaboration of DPAs, governments and international organisations to include data protection related rules and recommendations in international standards dealing with AML/CT matters to facilitate transborder data flow and a coherent implementation.

- DPAs shall play an important role in line with Article 15 (2) (b) of 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 the above-mentioned article and possible exceptions provided for by Article 11.

- DPAs should be provided with resources necessary for the effective performance of their functions and exercise of their powers, including in respect of the implementation of the rules on transborder flows of personal data.

- International data transfers shall only be allowed within the geographical limits of countries which offer an appropriate level of protection or appropriate safeguards which are in place in relation to the transfer at stake and are binding on the receiving entity[69], and assuming that the other requirements of Convention 108+ 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.

  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, notably by instruments that ensure an appropriate level of in line with Article 14 (2) or meet the requirements of Article 14(4).

- In the case of an OE belonging to a group which is composed of different legal entities /subsidiaries located in different countries, and domestic legislation does not prohibit the transborder transfer of data, including on data protection grounds, such transfer of data should be based on ad hoc or approved standardised safeguards. The transfer must not undermine the appropriate level of protection of personal data.

[69] Article 14 (4) of Convention 108+ and paras. 109 to 112 of the Explanatory Report.

- 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 Convention 108+, the requirements foreseen in Article 14 of Convention 108+ should be respected. There could be additional standards applicable to the exchange of information, specifying requirements of data protection or data security[70].It should be noted that the second additional Protocol to the Budapest Convention (ETS No. 185) and its Protocols 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.

- The cooperation between data protection authorities and other AML/CFT competent authorities is to be recommended both internally with respect of data exports and at multilateral level to facilitate personal data transfers with an appropriate level of protection.

[70] Such as the Egmont Group Principles.

Annex 1

- Customer data – The FATF Standards define parameters for information sharing only within the context of a financial group[71]. 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, government-issued identification number and tax identification number, signature. For a legal person and arrangements, 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[72].

- 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.

- Politically Exposed Persons (PEPs) – are classified, according to the FATF Standards, in three main categories as described below. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories. Moreover, 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.

    - *Foreign PEPs*, which are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

    - *Domestic PEPs*, which are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

    - *Persons who are or have been entrusted with a prominent function by an international organisation* refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

[71] 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, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level".
[72] FATF requirements however only require the list of directors to be publicly available. The rest needs to only be available to competent authorities.

- 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.[73] (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[74].

- 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[75]") 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[76]. 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.

- Legal persons – covers, according to the FATF Glossary, any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies, corporate, foundations, install, partnerships, or associations and other relevantly similar entities.

- Legal arrangements – covers, according to the FATF Glossary, express trusts and other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) may include but are not limited to fiducie, certain types of Treuhand and Fideicomiso and Waqf.

---

[73] FATF Report, Stocktake on data pooling, collaborative analytics, and data protection, July 2021, page 27.

[74] FATF Guidance on AML/CFT-related data and statistics, page 10.

[75] 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".