3 November 2021 T-PD(2021)8

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

CONVENTION 108

Draft guidelines on

the implications for data protection of mechanisms for inter-state exchanges of data for Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes

Section I. Data protection rules and principles

1. Introduction

Money Laundering and Financing of Terrorism (ML/FT) involves cross-border schemes and multiple institutions through which criminal proceeds are laundered. Data sharing is crucial for combatting ML/FT which becomes increasingly complex to tackle. The Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) framework entails complex processing and exchanges of data between customers, obliged entities, financial intelligence units (FIUs) and law enforcement authorities (LEAs).

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

In the AML/CFT area, the public interest is the main element regulating data protection issues. This extends to processing of personal data by government authorities and by private sector institutions. At the same time, public interest needs to be specifically defined and limited to the circumstances where measures benefit and increase the effectiveness of the AML/CFT regime. Excessive collection and processing of personal data should be avoided and the improvement of the general effectiveness of the AML/CFT regime should not be considered as sufficient grounds to articulate specific public interest(s).

Since data protection and privacy (DPP) are considered human rights, regard must be given to DPP rules and principles when acting in AML/CFT interests, in compliance with Member States' commitments and obligations under international law. Under these laws, the existence of a 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, DPP and human rights field.

This led the Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108, hereafter "Convention 108") to draft these Guidelines, which provide orientation on how to integrate international data protection rules and standards in the area of AML/CFT in order to provide for an appropriate level of protection while facilitating transborder data flows. They also aim to highlight grey areas in AML/CFT related issues where DPP safeguards should be put in place or strengthened and to tackle prospective issues such as cooperation between AML/CFT authorities and Data Protection authorities.

Similar considerations apply to the field of tax evasion and tax fraud, which will also be analysed in the next sections.

These Guidelines have been drafted on the basis of the principles and safeguards of the modernised Convention 108 (more commonly referred to as "Convention 108+). They are primarily addressed to rule-makers, controllers and processors (please see the Terminology and context section).

1.1 Scope

1.1.1 The guidelines will cover data processing and sharing for AML/CFT purposes by public and private entities in state Parties to Convention 108+ and in countries that wish to apply its rules, principles and provisions.

1.1.2 Taking into account that data processing and sharing has a crucial role in combatting ML/TF, these guidelines will emphasize the fulfilment of data protection obligations included in Convention 108+ by controllers and processors, while complying with the AML/CFT framework.

1.1.3 These guidelines will also cover aspects related to data processing and sharing for purposes related to combating tax fraud/tax evasion.

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

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

Personal data and data subject – Article 2 (a) of the Convention defines personal data as any information relating to an identified or identifiable individual (data subject). In the AML/CFT context, customers, beneficial owners[1], 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[2], including identification and verification of identity. While the Convention 108+ protects primarily personal data of natural persons, the Parties may extend the protection in their domestic law to data relating to legal persons in order to protect their legitimate interests[3], although corporate data is not 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, either automated or manual, can be defined as data processing – including collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, use, destruction of, and the carrying out of logical and/or arithmetical operations on such data (Article 2(b) and (c) of the Convention). The aforementioned operations shall only be performed when controllers and, where applicable, processors take all appropriate measures to comply with the provisions of the Convention 108+ (Article 10(1)).

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

From an AML/CFT standpoint, obliged entities (OE) are controllers, and in some cases, only in relation to certain operations performed. Financial institutions (FI) and other designated non-financial businesses and professions (DNFBP) such as casinos, real estate agents, dealers in precious metals and precious stones, lawyers, notaries, other independent legal professionals and accountants, trust and company service providers are data controllers. Recipients of the

[1] 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.

[2] 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).

[3] Explanatory Report of Modernised Convention 108, para. 30.

information such as Financial Intelligence Units (FIU), law enforcement authorities, and public registers of information on basic and beneficial owners are to be considered also data controllers for the processing of personal data they perform.

The AML/CFT framework provides for examples of public-private partnerships (PPP), to collaborate for strategic and/or tactical information sharing. In this scenario, when the different participants of a PPP share the same purpose and there is personal data involved, they should be considered to be joint-controllers[4]. 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[5]. Therefore, joint controllers must determine their respective responsibilities for compliance with the obligations under the regulation of a specific agreement.

Tax authorities are to be regarded as controllers. Providers of professional services such as accountants, auditors and lawyers also qualify as controllers, though their role regarding tax evasion/tax fraud purposes is limited to the exchange of information with authorities on grounds of public interest provided by law (article 5 (4)(b) of the Convention and para 47 of the Explanatory Report).

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

3. Basic principles for the protection of personal data

3.1 The fairness and transparency of processing principles

General principle

- According to Article 5(4) of the Convention, personal data shall be processed in a fair manner. This principle governs primarily the relationship between the controller and the data subject and requires the information of the data subject by the controller of any risks attached to the processing in order for unforeseeable negative effects to be avoided. Articles 5 (4)(a) and 8 of the Convention 108+ require data processing to be performed "in a transparent manner in relation to the data subject". In this regard, controllers must inform data subjects before processing their data, inter alia, about the purpose of processing and about the identity and address of the controller. 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. Moreover, the data subject also has a right of access, 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 (Articles 8 and 9(1)(b) of the Convention)).

[4] 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).

[5] Article 29 Working Party (2010), Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Brussels, 16 February 2010, p. 19.

AML/CFT contextualization

- Obliged entities collect personal information from their clients, primarily at the stage of onboarding the client and, in the case of occasional clients, before executing transactions or providing services not in the context of an established business relationship. FIs, particularly banks, typically inform the customer on the purpose for which data will be processed and may be eventually shared with third parties, and they require their consent, although this is not an FATF requirement and practice may vary from country, depending on local laws about data protection.

Recommendation

- When establishing business relationships with clients or conducting transactions for occasional customers, FIs and DNFBPs should inform the customer of the types of data that the institution (or other third parties) will be processing and the use made thereof in an understandable and user-friendly way.

3.2 The principle of purpose limitation

General principle

- According to Article 5(4)(c), 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. Further processing of data may not, therefore, be done in way that is unexpected, inappropriate or objectionable for the data subject. To assess whether the further processing is to be considered compatible, the controller should take into account, inter alia, for instance, the nature of personal data, the consequences of the intended further processing for data subjects, the context in which the personal data have been collected in particular concerning the reasonable expectations of data subjects based on the relationship with the controller on its further use, and/or the existence of appropriate safeguards in both the original and intended further processing operations[6].
- Enhanced measures should be put in place when AI is used in the processing operations.

AML/CFT contextualization

- Personal data on the client or transactional data that may be collected by OEs for customer due diligence purposes, may, at a later stage, be shared with other counterparts, for fulfilling additional purposes (e.g. inform an OE belonging to the same group of a common client that may have been subjected to reporting to the FIU). In correspondent banking relations, the correspondent bank may need to require additional information in relation to a client of the respondent bank, which would have been collected by that bank from its client in a different context.

Tax field contextualization

- Purpose limitation is a major point of concern in the field of exchange of data for tax purposes, as often competent authorities would like to use available information for other purposes as well, if they consider it useful. There are still cases where the purposes for which personal data are exchanged are not always clearly specified, leaving room for exchanges of data that would not be in line with the data protection requirements.

Recommendation

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

[6] Explanatory Report of Modernised Convention 108, para. 49.

- In the case of correspondent banking relations, there should be clear and detailed provisions between the correspondent and the respondent bank regulating the sharing by the respondent of personal data concerning its customers, 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 purpose limitation principle should be clearly respected, both when automatic processing is carried out for several different purposes, or when it is based on the principle of unity of purpose.

3.3 The data minimization principle

General principle

- According to Article 5 (4)(c), data processing must be limited to what is necessary to fulfil a legitimate purpose. A controller should strictly limit collection of data to such information as is directly relevant for the specific purpose pursued by the processing.

AML/CFT contextualization

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

- The aforementioned case of OEs belonging to the same group, which may need to share information on a client (e.g. CDD data on the client, or the fact that a client has been subjected to the reporting of a suspicious transaction) is also relevant here. While this scenario presents less critical aspects 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), 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).

Tax field contextualization

- It needs to be assessed how data minimisation principle can be respected in cases when the exchanged information that is "foreseeably relevant", in accordance with Article 26 of the OECD Model Tax Convention, for the purpose for which the data are exchanged.

Recommendation

- FIUs from state Parties should exchange information consistently with Egmont Group principles and complying with the requirements of the data protection legislation of the data-provider and of the data-recipient countries notably with the ones foreseen in Article 14 of the Convention. Data should be used for the sole purpose for which it was provided and cannot be transferred to other authorities of the data-receiving countries, unless the requirements laid down in the Convention are complied with.

- In the case of an obliged entity belonging to a group where branches/subsidiaries are located in different countries, and domestic legislation does not prohibit the cross-border exchange of data, such exchange of data should occur only in countries that have AML/CFT systems consistent with the FATF recommendations, that allow for proper safeguards in the processing of the data and where the rule of law is respected.

- State Parties shall ensure that the data minimisation is respected and that the competent tax authorities will assess the compliance with this principle in view of the amount and intrusiveness of data requested to be exchanged with the purposes that need to be achieved.

3.4 The data accuracy principle

General principle

- According to Article 5(4)(d), the principle of data accuracy must be implemented by the controller in all processing operations. Inaccurate data must be erased or rectified. Data may need to be checked regularly and kept up to date to secure accuracy.

AML/CFT contextualization

- OEs use external providers for various purposes (e.g. sanction screening, identification of PEPs, family members and close associates), which can affect the accuracy of data that they process for CDD purposes, and use AI-based systems to monitor transactions in order to identify suspicious patterns and trends, and generate alerts, which, if not properly calibrated may result in an excessive number of alerts, that cannot be processed in an accurate manner.

- FATF allows OEs to rely on third parties for the performance of certain elements of the CDD process. 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, it is important that the FATF clarifies 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 processor of such third parties, as defined in Convention 108+.

- FATF Recommendation 24 requires basic data (i.e. company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, and a list of directors) to be publicly available, and also envisages the possibility to require companies or company registries to obtain and hold BO information. In all of these cases FATF requires that the information should be accurate and up to date.

Recommendation

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

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

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

- Countries should adopt policies requiring the verification of data held by company registries, in order to ensure that the data is accurate and up to date.

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

3.5 The storage limitation principle

General principle

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

AML/CFT contextualization

- FATF Recommendation 11 sets clear requirements for record keeping of CDD information, account files, business correspondence and results of any analysis undertaken (5 years following the termination of the business relationship) and records on transactions (5 years following completion of the transaction).

Recommendation

- If there are no storage limitation requirements and/or those in place are not in line with FATF Recommendation 11, data should be stored for the minimum period necessary to enable them to comply with information requests from competent authorities.

3.6 The data security principle

General principle

- According to Article 7, 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. 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.

AML/CFT contextualization

- There are several requirements in the FATF Recommendations addressed to public authorities that can ensure data security. The revised version of Recommendation 2 requires countries to have cooperation and coordination between competent authorities to ensure the compatibility of AML/CFT requirements with Data Protection requirements. This should also have (albeit only indirectly) an impact for OEs processing and exchanging data. On a more operational level, FATF Recommendation 29 has several requirements for FIUs to protect information and to ensure its operational independence. In addition to FATF, the Egmont Principles also set security measures for the exchange of information.

- At the same time, the 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 sensitive data (e.g. on PEPs, which could reveal political affiliations or sexual orientation in the case, for example, of a same-sex partnership).

- 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.

4. The lawfulness of processing – legal basis

General principle

- To be lawful, data processing shall be carried out on a legal basis: the consent of the data subject or other legitimate basis laid down by law (Article 5(2) of the Convention). Irrespective of the legal basis for data processing, which is relied upon by the controller, adequate safeguards provided will need to be ensured.

AML/CFT contextualization

- For AML/CFT purposes, consent could not be used as a legal basis, since this would imply prior information to the customer, which would contravene to AML/CFT prohibitions, in particular to tipping-off. Data processing in the AML/CFT context could be based either on the lawful ground of public interest or the overriding legitimate interest of the controller or a third person provided that the rights and interest of the data subjects have been duly taken into account.

- There could be issues of proportionality in the processing of data in the context of public-private partnerships (PPPs) where processing of a high amount of data transactions and underlying personal information on the parties of the transactions is needed to identify potential suspicious patterns or to determine links between terrorists and potential networks.

Recommendation

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

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

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

- 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.

- Customer due diligence data that should be obtained from a natural person is mainly personal data: the full name, residential address, contact number and e-mail addresses, place of birth, date of birth, gender, nationality, race, government-issued identification number and tax identification number, signature. For a legal person, some personal data is required as well on directors, shareholders, senior management and beneficial owners, but this personal data is generally publicly available.

- There are also special categories of personal data whose processing is, by nature, likely to pose a higher risk to the data subjects and therefore need enhanced protection. Such data is subject to additional safeguards complementing those already in place for "normal categories of data" and can only be lawfully processed under a limited number of conditions (Article 6 of the Convention).

- 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 under the control of an official competent authority or when appropriate safeguards are in place. Registers holding information on criminal convictions may also be subject to the control of official competent authorities.

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

6. Rights of data subjects (Article 9)

- Data subjects have multiple rights detailed in Article 9 of the Convention. Some of these rights can be restricted due to AML/CFT purposes. Restrictions will most likely rely on general public interest (i.e. the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties) and must be determined by law, respect the essence of human rights and fundamental freedoms and be necessary in a democratic society.

- Measures shall be put in place by controllers to facilitate the exercise of these rights by the data subject, in principle free of charge. In case of automated decision making, the information on the decision and the logic underpinning the processing of the data should be available upon request of the data subject. Intellectual property law should not be an excuse for data controllers to provide data subjects with the logic and training of the algorithms applied in the specific processing operation.

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

7. Exceptions and restrictions (Article 11)

- In the case of both AML/CFT and tax fields, interstate exchange of personal data is one of the most important data processing operations, and only a limited number of expiations can be used provided they comply with the general conditions (i.e. they are provided for by law, respect the essence of human rights and fundamental freedoms and are necessary in a democratic society) of their lawful use:

    - The obligation to process data fairly and in a transparent manner;
    - The need to ensure that data is collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes;
    - The obligation to limit the processing to adequate, relevant and not excessive data in relation to the purposes for which they are processed;

- The obligation to ensure that data undergoing processing is accurate and, where necessary, kept up to date; and
- The need to ensure that data is preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

8. Transborder flows of personal data (Article 14)

General

- Given the multilateral nature of mechanisms for inter-state exchanges of personal data for tax and AML/CFT purposes, the question of appropriate level of protection arises 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.

AML/CFT contextualization

- 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

Tax fields

- Data subjects are not always informed about the transferring of their data for tax purposes.

- Exchanged data may be used for different tax purposes than the ones they were collected for.

Recommendation

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

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

- Instruments, tools should be available in line with Article 14.2 to send personal data to data controllers in a country or jurisdiction which does not provide by its legal framework the appropriate level of protection for individuals

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

- State Parties to Convention 108+ shall ensure the consistency of their international commitments including by reviewing the compatibility of their bilateral agreements that facilitate the exchange of personal data for tax purposes with provisions of Convention 108+.

9. Effective independent supervision and oversight (Article 15)

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

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

- In the AML/CFT and tax fields, DPAs shall have coordinated activities with the OEs in order to supervise the processing of data and to suggest effective tools and modus operandi for effective supervision.
- And in regard to the above, the DPA shall reinforce the OEs and data subjects with internal training.

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

10. Cooperation and mutual assistance (Article 16 and 17)

- According to articles 16 and 17 of the Convention the DPAs shall engage in and improve mutual cooperation between parties.

Section II. Grey areas in AML/CFT related issues where DP requirements should be enhanced

- Private-to-private data sharing outside the same financial group – AML/CFT and Data Protection implications

- Ensure adequate safeguards from a data protection and privacy standpoint in relation to new and emerging privacy enhancing technologies

- Rapidly evolving AI technologies and digital initiatives allow competent authorities and obliged entities to have wider access to multiple internal and external databases. AI-based technologies and tools also allow to process larger volumes of up-to-date, real time and comprehensive data. However, competent authorities should ensure that such digital tools which are used for collecting and further dissemination (where needed) of data provide certain level of security. In this regard application of such digital tools should be aligned with relevant legal framework

- Processing of publicly available personal data for AML/CFT purposes

- Access to data held by private entities by public authorities from a different jurisdiction

- Responsibility of private entities in detecting and reporting suspicious/criminal activity, in a country or, involving different jurisdiction, and to reply to LEA request (also in relation to data held in a different jurisdiction, i.e. cloud)

Section III. Prospective issues and recommendations

- Recovering the analysis of the way forward on how DPAs, oversight bodies and entities are invited to treat AML/CFT issues as they evolve

- Policy recommendations on cooperation between DPAs and between AML/CFT authorities and DPAs

- The independence of DPAs is to be emphasised and new model(s) for better enforcement are to be recommended. For instance, one important form of domestic interagency cooperation between DPAs and AML/CFT authorities would be to ensure effective data protection supervision over the private sector entities involved in data sharing.