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

Purpose: *These guidelines aim at providing orientation on how to integrate international data protection rules and standards in the area of Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes in order to provide for an appropriate level of protection while facilitating the free flow of information, including by highlighting grey areas in AML/CFT related issues, where DPP requirements should be enhanced.* Data sharing is crucial for combatting ML/TF, which involves oftentimes cross-border schemes and multiples institutions through which criminal proceeds are laundered. AML/CFT are both significant public interests, which are neither opposed, nor inherently mutual exclusive (quote the FATF report on Data pooling). Therefore, regard must be given to both AML/CFT interests and DPP principles, obligations and rights, in compliance with Member States' obligations under international law, including human rights law. Under these laws, the existence of a valid legal basis 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.

Scope: The guidelines will cover data processing by public and private entities

Definitions (personal data, data processing, data subject, data controller, data processor, and recipient) applied to AML/CFT. More precisely, explain the most difficult part: who would be considered data subject, controller/processor from an AML/CFT standpoint.

* Interstate exchanges of data in (a) AML/CFT and (b) taxation field
* Interplay between data protection and (a) AML/CFT and (b) taxation field
* Reference to the 2014 Opinion

2. Basic principles for the protection of personal data

(i) Fairness and transparency

(ii) Purpose limitation

- Legislators shall be urged to define concretely the purposes for which the exchange of information is required, in order to avoid exchanges of data for other purposes which may well be legitimate, but are too broad or not compatible at all with the initial ones

(a) AML/CFT

- Clear and detailed provisions 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.

(iii) Proportionality

- Especially when AI is used, respect to fundamental rights shall be foreseen (a reference to Guidelines on AI: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8)
- Intellectual Property law might hinder the disclosure of important information about the logic and training of algorithms: how to mitigate?

4. Legal basis (Article 5)

(i) Challenges related to the application of Article 5(2) CoE Convention 108+

(a) AML/CFT

(ii) Data processing/exchange of data shall only be allowed based on a valid legal basis: this consideration might be relevant to all entities (legislator, FIUs, private entities and LEAs)

b) Taxation

(iii) Data minimization

- The entities sending the data must be able to justify, in each case of sharing of personal data, why the specific data were needed for the specific purpose. The legislation, wherever possible, shall be as concrete as possible regarding the data that can be collected by an entity and the data that can be shared for specific purposes.

(a) taxation field

- States shall ensure that the data minimisation is respected and that the competent tax authorities will be balancing the public interest underlying the requested data to be exchanged with rights and interest of data subjects and where applicable service providers that need to be achieved.

(iv) Data quality, Accuracy

a) AML/CFT

- Obliged entity receives or verifies customer client information via external sources. Obliged entities shall ensure the accuracy and quality of the data they obtain from external sources
- There is need for harmonization of the regulatory framework on the exchanges of information between the FIUs of contracting parties and other third countries.
- Recommendation on the importance of the completeness and quality of the input, as this is important for the accuracy of the output, especially when AI is used: “In the case of Machine Learning software, the accuracy of its outputs depends

significantly on the completeness and quality of the input, that is, on the data used to assess a prospective customer or a transaction. In addition to the data, the accuracy of the output also depends on how the software has been trained and what kind of patterns and correlations it has detected: if the software presents biases or inaccurate correlations, the predictions it makes might not be reliable" (from the report). Have a reference to the CM recommendation on profiling https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00

(v) Storage limitation

- It is crucial in order for the storage limitation principle to be respected that the legislation clearly mentions the retention periods during which data shall be retained after their exchange. The determination of the retention period shall respect the proportionality and purpose limitation principle.
- To include a section with guidelines for the period/situation where there is no such legislation

- Data security (Article 7)
  Compliance with the principle of data security requires technical and organisational measures such as the encryption of the data and rules on the full traceability of the exchanges, especially through the implementation of access logs

3. Key stakeholders

- Enhanced focus on the private sector, both for private-to-public data sharing, and also the grey area which is private-to-private data sharing
- Clarify who would be a controller/ a processor and who would bear ultimate responsibility
- Explain the difficulty in identifying the person of interest vs beneficial owners
- Suggest categorization of data subjects (suspect, victim, witness, etc.) and explain which data protection regime (exception regime based on art 11 or normal regime) to use in which part of the procedure (beginning, after founded suspicion/probable cause has been established, during, after the investigation, etc.)
- Avoid one-size-fits-all model and identify actors on a case-by-case basis
- Importance to identify beneficial owners to correctly identify the data subjects in the exchange of data
- Clarification of the role of third parties to whom obliged entities outsource the performance of the CDD measures
- Clarification of roles in PPPs for AML/CFT already when they are established

5. Types of data (focus on sensitive data) - Article 6

- Transactional and financial data (including metadata and other non-conventional type of personal data such as geolocation data)
- Sensitive data
  - When processing of personal data relating to criminal proceedings and convictions is allowed for AML/CFT purposes, legislators and policy makers

shall make sure that such processing is only allowed when appropriate safeguards complementing those already in place are established in law.
    - All entities involved in AML/CFT, including private parties, FIUs and law enforcement authorities shall train their staff, especially when they deal with sensitive personal data.
    - Corrective measures, including penalties, shall be established for the effective application of the safeguards
    -

6. Transparency

Art 8 of Convention 108+ and ER

including

- notification is required in the context of automated analysis (of traffic and location data, in that given case) "the competent national authority is obliged to publish information of a general nature relating to that analysis without having to notify the persons concerned individually. However, if the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning him or her, it is necessary to notify that person individually. That notification must, however, occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible" [Will modify into a recommendation based on the LQDN judgment]

7. Rights of data subjects (Article 9)

- To develop how each of the rights in art 9 could/should be exercised in the context of the guidelines possibly with specific recommendations?
- notification requirement:
    - For instance, the notification/provision of information to the data subject. Data subjects shall be notified when the notification does not jeopardize anymore the investigations. Supervisory authorities shall have the power to examine whether the notification of the data subjects is actually realised.
- Careful consideration when restrictions are applicable
  (a) AML/CFT

- Restrictions will most likely rely on "general public interest"

8. Exceptions and restrictions (Article 11)

- Relevant restrictions can be established for personal data exchanged for the purposes of AML/CFT
  (1) in the name of prevention, investigation and prosecution of crime
    - For instance, the notification/provision of information to the data subject
    - Make recommendation
  (2) in the name of national security, as interpreted in the case law of the ECtHR or

(3) in the name of other important objectives of general public interest. This latter category can cover AML/CFT objectives (Art. 11(1)(a) CoE 108+

9. Transborder flows of personal data (Article 14)

- 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
- 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
- Contracting states shall review international agreements that involve transborder transfers of personal data to make sure that the principles and requirements of Convention 108+ are respected.

(a) AML/CFT

- Make a recommendation on FIUs exchanging data to a foreign counterpart established in a country not having an adequate level of protection. (existing reflections to solve this within the CoE: https://rm.coe.int/2nd-additional-protocol-budapest-convention-en/1680a2219c (art 14) and https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee (Point 3.4)
- National supervisory authorities shall assist authorities in signatory parties in ensuring compliance with Convention 108+.
- 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) Convention 108+, para. 109 to 112 of the Explanatory Report). Without this, pooling of data amongst financial institutions, particularly across national borders and with non-parties raises a number of concerns.
- CoE law allows for data transfers to territories that do not have an appropriate level of data protection based on ad-hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by all actors involved in the transfer and further processing.

10. Effective independent supervision and oversight (Article 15)

- To recommend that the DPA is competent for supervising data processing in those areas
- Suggest effective tools and modus operrandi for effective supervision

11. Cooperation and mutual assistance (Articles 16 and 17)

- To recommend making use of the potential of international cooperation and where relevant enforcement

Section II.

Grey areas in AML/CFT related issues where DP requirements should be enhanced such as:

- Private-to-private data sharing related issues requiring careful analysis of both the AML/CFT and DPP implications. (link to the FATF report on data pooling, collaborative analysis and data protection)
- New and emerging privacy enhancing technologies related issues for private-to-private data sharing, and the need to ensure and enhance both data protection and privacy (link to the FATF report on data pooling, collaborative analysis and data protection)

Section III.

Prospective issues and recommendations

- Recovering the analysis of the way forward on how DPAs are invited to treat AML/CFT issues as they evolve
- Policy recommendations on cooperation 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.