Strasbourg, 10 December / décembre 2021 T-PD(2021)8Mos2

Compilation of Comments

on the Outline of the 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

Compilation des commentaires

sur le Projet de lignes directrices sur les implications pour la protection des données des mécanismes d'échanges interétatiques de données pour la lutte contre le blanchiment d'argent et le financement du terrorisme, et à des fins fiscales

TABLE OF CONTENT / TABLE DES MATIERES

FRANCE

Document concernant les flux en matière de lutte contre le blanchiment et l'évasion fiscale

Nous rejoignons le commentaire général de l'Allemagne invitant à s'appuyer sur les textes existants en la matière (en l'occurrence les dispositions de la 4ème directive UE sur la lutte contre le blanchiment) qui nous semble tout à fait pertinent.

GERMANY / ALLEMAGNE

Draft guidelines onon mechanisms for inter-state exchanges of personal data

for Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes and Data Protection

Section I. Data protection rules and principles

1. Introduction

Money Laundering and Financing of Terrorism (ML/FT)~~ML/TF~~ often involves cross-border schemes and multiple~~s~~ institutions through which criminal proceeds are transferred and/or laundered. Data sharing is crucial for combatting ML/~~T~~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 entitie~~ss (OEs)~~, financial intelligence units (FIUs) and law enforcement authorities (LEAs).

Processing of personal data ~~may~~ constitute~~s~~ an interference with the data subject's right to respect for private life, as protected by international human rights instruments (such as A~~a~~Article 12 of the UNDHR, Article 17 of the IPPCR ~~or~~and Article 8 of the ECHR). LAccording to Article 11 of the modernised Convention 108 l~~L~~awful ~~interference~~ exceptions and restrictions with this right can only be carried out for an objective of ~~general~~ 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 ~~a~~ 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 ~~where it does not significantly improve the overall effectiveness~~ 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 ~~AML/CFT and~~ data protection and privacy (DPP) are considered ~~both significant public interests~~human rights, ~~which are neither opposed, nor inherently mutual exclusive,~~ regard must be given to ~~both AML/CFT interests and~~ DPP rules and principles~~, obligations and rights,~~ when acting in AML/CFT interests, in compliance with Member States' commitments and obligations under international law~~, including human rights 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. Taking into account that data processing and sharing has a crucial role in combatting ML/TF, these guidelines will concentrate on the fulfillment of data protection obligations included in Convention 108+ by controllers and processors, while complying with the AML/CFT framework.

Commented [A1]: The current wording is misleading as it could be construed as if the inter-state exchange has implications on the data protection regime when it should be the other way round

Commented [A2]: As a general remark:
While the text has been further developed and structured, we feel that it still needs a lot of work before it could be adopted. This concerns inter alia transparency obligations, rights of data subjects and possible exceptions according to Article 11 and the relationship with FATF

Furthermore, the Directive (EU) 2019/1153 that already tackles data protection issues in the context of AML/TF might be of some use as an orientation.

Commented [A3]: As it concerns the "inter-state exchange", reference should be made to Article 14.

Commented [A4]: The processing of personal data is always likely to constitute an interference with fundamental rights

Commented [A5]: Wording of the Convention

Commented [A6]: This seems too general. It cannot be ruled out per se that an improvement in the effectiveness of the AML/CFT regime may be a sufficient basis for formulating specific public interests.

Commented [A7]: See 1.1.2 Might fit here better than in the section defining the scope of these guidelines.

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 ~~Anti-Money Laundering/Countering Financing of Terrorism~~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 ~~requirements~~ safeguards should be put in place or ~~strengthened enhanced~~ 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 ~~new~~ 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).

~~The aim is to provide 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.~~

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

(…)

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

(…)

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

Commented [A8]: There is no "1.2" in the following.

Commented [A9]: The wording is a bit unusual.

Commented [A10]: Not part of the scope

Commented [A11]: "body" is the definition of the Convention

the purpose and means of the processing, as well as data categories to be processed and access to the data (Article 2 (d) of Convention 108+). The decision-making power can derive from a legal designation or from factual circumstances that are to be assessed on a case – by- case basis (ER 22). Controllers are bound to ensure the legitimacy of data processing (Article 5 of the Convention).

(...)

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[1]. 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[2]. Therefore, joint controllers must determine their respective responsibilities for compliance with the obligations under the regulation of a specific agreement.

(...)

3. Basic principles for the protection of personal data

3.1 The lawfulness of processing – legal basis

General principle

- To be lawful, data processing shall be carried out on a legal basis: which may be the free, specific, informed and unambiguous consent of the data subject or another 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.

Commented [A12]: See Explanatory Report 22

Commented [A13]: There are new Guidelines by the EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0 Adopted on 07 July 2021 https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

Commented [A14]: A legal basis is the prerequisite for any data processing. As such it is a basic principle and should therefore be mentioned first.

Commented [A15]: editorial

Commented [A16]: editorial

Commented [A17]: What is meant by this? Appropriate safeguards for special categories of data according to Article 6? Or Appropiate security measures against risk according to Article 7

Commented [A18]: In our view, data processing should be carried out exclusively on the basis of a clear legal basis.

Against this background, we propose the following wording:

„Data processing in the AML/CFT context shall be based on a clear and detailed legal basis that provides for the principles of necessity and proportionality."

Commented [A19]: As we understand, proportionality considerations are not directly related to the legal basis. Should this part be located elsewhere, if necessary?

[1] 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).

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

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.

3. 2.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)).

(…)

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

Commented [A20]: Is pseudonymized meant?

Commented [A21]: Unless an exception according to Article 11 applies

Commented [A22]: Art. 8 (1) of Convention 108+ requires not only information about the type of data, its use and third parties. Transparency obligations should be fully reflected.

controller on its further use, and/or the existence of appropriate safeguards in both the original and intended further processing operations[3].

- Enhanced measures should be put in place when AI is used in the processing operations.

(…)

3.3 The data minimization principle

(…)

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.

(…)

- FIUs from ~~member~~state ~~p~~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, ~~without the specific consent of the data-providing country~~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.

(…)

3.4 The data accuracy principle

(…)

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.

(…)

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

Commented [A23]: This could be specified or it could be referred to the Guidelines on AI

Commented [A24]: The abbreviation is already used above.

Commented [A25]: This should be further explained

Commented [A26]: This should be further explained.

As a EU member state we also take the Schrems-II-decision of the CJEU into account. In this context it appears doubtful, if the FATF recommendations are the relevant or sufficient guidelines in this context.

Commented [A27]: Is this really a necessary recommendation? Obliged entities have an own interest in limiting the number of generated alerts. The avoidance of false positive as well as false negative alerts is a basic aim. Furthermore: Does this affect “data accuracy”?

Commented [A28]: Since the use of AI becomes increasingly important in the field of AML/CFT, we propose to further highlight the particular risks of AI.

3.5 The storage limitation principle

(…)

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

(…)

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~~ special categories of data (e.g. on PEPs, which could reveal political affiliations or sexual orientation in the case, for example, of a same-sex partnership) according to Article 6 of the Convention 108+.
- Compliance with the principle of data security requires technical and organisational measures such as ~~the~~ (hard, end-to-end) encryption of the data and rules on the full traceability of the exchanges, especially through the implementation of access logs.

Commented [A29]: editorial

Commented [A30]: Instead of focusing specifically on "information requests":
Shouldn't more general considerations be made here? (e.g.:" to be deleted or anonymised as soon as the data are no longer needed for the purposes for which they were collected.

Commented [A31]: Cf. wording of Art. 6 of Convention 108+

Commented [A32]:

~~**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 is could be solely 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 suspicious 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.~~4. Types of data which are subject to the processing of personal data in the context of AML/CFT obligations

(…)

- Customer due diligence ~~(CDD)~~ 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 ~~as required under FATF Recommendation 24~~.

(…)

- 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 ~~only~~ be subject ~~kept under~~to the control of official competent authorities.

(…)

~~6.~~5. 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.

~~7.~~6. Exceptions and restrictions (Article 11)

- In the case of both AML/CFT and tax fields, interstate exchange of personal data ~~in~~ 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;

Commented [A33]: The fact something is publicly available has no influence on its being personal data.

Commented [A34]: What is meant by this? A competent authority is always "official"

Commented [A35]: Art. 6 para. 1 alt. 2 of Convention 108+ does not provide for such a requirement

Commented [A36]: See above

Commented [A37]: Reference to Article 11

Commented [A38]: Since Art. 11 of Convention 108+ deals in particular with the possibility of restricting the rights of data subjects:

Why is there an introductory reference to the exchange of data between countries?

Commented [A39]: Exceptions?

- 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.

~~Nevertheless, some restrictions can be established for personal data exchanged for the purposes of AML/CFT and tax evasion/fraud: (1) in the name of prevention, investigation and prosecution of crime, for instance, the notification/provision of information to the data subject; (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) of the Convention).~~

Commented [A40]: Why should there be any deviation from the data protection principles laid down in Art. 5 (4) of Convention 108+?
In the original version, it was still stated that these principles must always be upheld.

Commented [A41]: Can you please explain why this part was deleted ?

7. Transborder flows of personal data (Article 14)

(…)

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

Commented [A42]: This should be further explained

(…)

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.

Commented [A43]: editorial

(…)

- 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

Commented [A44]: Art. 14 (2) of Convention 108+ merely states that data may only be transferred if "an appropriate level of protection based on the provisions of this Convention is secured". How can this be related to "tools"?

(…)

8. Effective independent supervision and oversight (Article 15)

(…)

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

(…)

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

- According to ~~a~~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

(…)

.

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

(…)

Section III. Prospective issues and recommendations

(…)

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

(…)

Commented [A45]:
This seems already regulated by data protection rules and need no further enhancement.

Commented [A46]: Another point might be the streamlining of FATF recommendations and Data Protection rules.

The development in CAHAI as well as the draft of the EU Regulation on AI – which has an impact on many Council of Europe members- shows that a final version might also have impact on the use of AI in the context of AML/TF both by OE / private entities and competent authorities

SWEDEN / SUÈDE

Sweden would like to submit the following written comments on the document *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,* document T-PD(2021)8, as regards the last proposed recommendation in Section 8 (Tax fields):

> *'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+'.*

The recommendation is unclear when it comes to the obligation for the States Parties to Convention 108+ to ensure the consistency of their bilateral commitments. Does this mean that they are expected to take action and amend their bilateral agreements that facilitate the exchange of personal data for tax purposes in case they are found not compatible with the provisions of Convention 108+? If the answer is yes, what happens if the other State party to the agreement does not agree to change the provisions in question? Is there then an obligation to terminate a treaty or to no longer permit international transfer of personal data? Will this be followed up? There is also no time frame. To go through all bilateral agreements in the tax field would mean a considerable amount of work.