Strasbourg, 05 June 2023 T-PD(2021)8rev5Comp

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

CONVENTION 108

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

***

Compilation des commentaires sur le projet de lignes directrices sur la protection des données personnelles dans le traitement de ces données en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

www.coe.int/dataprotection

Tables of contents

DENMARK / DANEMARK

(…)

3. Basic principles for the protection of personal data

3.1 The principle of purpose limitation

(…)

AML/CFT contextualisation[1]

- 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, or with third parties[2] 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~~an insurance intermediary gathering CDD data which is in turn passed on to the insurance company who would sell and issue the life insurance policy). 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.

(…)

Commented [A1]: We suggest that the deleted sentence should stay as the deleted example is more aligned with the exceptions to the prohibitions of disclosure as regulated in article 39, para 2-6 of Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

[1] Relevant FATF Recommendations: Rec. 10-12,13, 15-18, 20, 22-27, 29, 31, 40

[2] In this context, ~~"~~"third parties" should be interpreted as a~~A~~ny natural or legal person that is external to and does not form part of the obliged entity or its financial ~~group~~institution.

FINLAND / FINLANDE

(…)

4. Basic principles for the protection of personal data

3.1 The principle of purpose limitation

(…)

AML/CFT contextualisation[3]

- 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, or with third parties[4] 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~~an insurance intermediary gathering CDD data which is in turn passed on to the insurance company who would sell and issue the life insurance policy). 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.

(…)

Recommendations

(…)

- When personal data are processed ~~i~~in a third-party[5] reliance scenario[6], ~~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~~. ~~B~~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.

(…)

3.5 The data accuracy principle

(…)

Recommendation

(…)

- When AI is used (e.g., for transaction monitoring for the purpose of detection of suspicious activity), the data subject should not be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration 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

[3] Relevant FATF Recommendations: Rec. 10-12,13, 15-18, 20, 22-27, 29, 31, 40

[4] In this context, «"third parties" should be interpreted as aAny natural or legal person that is external to and does not form part of the obliged entity or its financial group.

[5] 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.

[6] 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

Commented [A2]: FI observation: First, it is important to try and define what is meant by data sharing with third parties. The AML/CFT legislation allows OEs to rely on third parties when carrying out CDD obligations. That might be close to the concept of "data processor" (on behalf of the controller), which is a situation different from that of sharing CDD/transactional data e.g. for the purpose of verifying CDD data or of analysing an individual transaction. Sharing of CDD or transactional data with third parties within that meaning is typically a difficult issue, and e.g. in the EU directives it has been restricted. It might be problematic from a data protection point of view to assimilate it with data sharing within the obliged entity/ its financial group. It is essential that data sharing with third parties is strictly limited for example to the need to verify certain CDD data from a reliable source, in which case a minimum set of data (such as identifying data) could be shared to get the necessary supplementing CDD data.

Further, where the potentially unusual or suspicious nature of an individual transaction is analysed by the obliged entity, it is important to note that transaction data (e.g. transfers from a bank account) may be highly sensitive particularly if the purpose of the payment discloses information about the private life of the customer. It may disclose for example location data or health data. Further, if the transaction relates to a potential suspicion of money laundering or terrorist financing, revealing customer data to a third party may entail risks of tipping off/ data leaks, which could run counter the purpose of the secrecy obligations relating to the submission of STRs. Apart from protecting personal data, the secrecy obligations also protect the interests of criminal investigations.

Proposal: Perhaps it would be clearer to mention data sharing with third parties in a separate sentence, and include further conditions e.g. as follows: "***It may sometimes be necessary to share data even with third*** …

Commented [A3]: FI observation: This is an important addition. See our comment above.

Commented [A4]: We support drawing attention to the increasing use of AI in the detection of suspicious transactions, including the added text. The rights of the data subject are typically restricted by the AML/CFT legislation in the case of STRs. For that reason, the possibility to request human intervention does not usually work that well as a safeguard to protect the rights of the data subject, nor the opportunity to present his/her views. Also, the possibility to challenge the STR may not exist until at a rather late stage of its processing, such as during the investigation/ hearing of a criminal suspect.

In view of the impact of STRs and the related risks for the rights of the data subject, perhaps other examples of suitable safeguards could also be given in the text, such as a requirement to provide the necessary additional information to data subjects to ensure fair and transparent processing, highlighting the use of solely automated processing as well as its purpose and potent …

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). ~~or During the process of t~~The data subject concerned ~~so that they~~should be given the opportunity to ~~can~~ present ~~their~~ 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. 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[7].

(…)

[7] FATF Recommendation 6 and 7; C 108+ art. 9 (a), 10 (1); ER para. 71-73, 75 and 85.

ITALY / ITALIE

Data protection rules and principles

(…)

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 (and demonstrable) measures to comply with the provisions of the Convention 108+ (Article 10(1)).

Commented [A5]: IT We should check the consistency of the wording (Convention/Convention108+) in the whole document

3. Basic principles for the protection of personal data

3.1 The principle of purpose limitation

General principle

(…)

- 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 inform him/her on other legal basis for subsequent processing.

Commented [A6]: IT: It is not just a question of informing the data subject but rather to **have** an appropriate legal basis

(…)

Recommendations

(…)

- When personal data are processed ~~I~~in a third-party[8] reliance scenario[9], ~~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.~~ ~~B~~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.

Commented [A7]: Not sure it is clear

(…)

3.2 The lawfulness of processing – legal basis

(…)

AML/CFT contextualisation[10]

(…)

[8] 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.
[9] 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
[10] Relevant FATF Recommendations: Rec. 24, 25.

- For example, data processing is required to prevent the misuse of legal persons for ML or TF by ensuring that there is adequate, accurate and up-to-date information on beneficial ownership and control of legal persons[11]. 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. [In determining the beneficial owners, countries are required to ensure that companies co-operate with competent authorities to the fullest extent possible by (i) requiring that one or more natural persons resident in the country is authorised by the country and accountable to competent authorities to provide all available beneficial ownership information, (ii) requiring that a DNFBP in the country is authorised by the company and accountable to competent authorities for providing all available BO information or taking other comparable measures.] 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 ~~i~~nformation 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~~raises concerns in the data protection perspective. Being the contrast of crimes including in the financial sector essentially a public task, the allocation of the said task to private parties or PPP's should be subject to strict limitations and a thorough scrutiny also by means of specific legislation providing appropriate safeguards for data subjects. ~~challenges which are also of a legislative nature (e.g. legislative amendments may be needed to ensure a proper legal basis and allow partners to achieve their objectives).~~

Recommendation

(…)

- 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~~ 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~~cover:~~ (i) who ~~participates~~can ~~to~~ ensure that the information is provided on a strictly need-to-know basis, (ii) the specific purpose of ~~use of shared~~ personal data sharing~~, undertakings~~ and other processing ~~and~~ (iii) ~~assurances~~ requirements that ~~receivers~~recipients of personal data will have in place appropriate safeguards and (iv) ~~ensuring~~guarantees that only ~~that~~ personal data that is strictly necessary for the on-going operational analysis or investigation is disclosed and shared~~,~~; and clear and precise requests as to the necessary dataset ~~to be~~are submitted by obliged entities.

- Regarding central beneficial ownership registries, personal data should only be available in the situations or to the extent provided by law in compliance with the principles of ~~the~~ Convention 108+~~,~~ and ensuring that appropriate, access criteria should be established based on an analysis of necessity, purpose and proportionality.~~,~~ ~~and in compliance with international data protection standards and regulations.~~

3.3 The fairness and transparency of processing principles

General principle

(…)

[11] FATF Recommendation 24.

Commented [A8]: IT In favour of deletion

Commented [A9]: IT We may try to reword a little bit and say: "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"

Commented [A10]: IT: not sure it is clear

Commented [A11]: ?

Formatted: Font: (Default) Arial, 10 pt, English (United Kingdom)

- The principle of transparency is intrinsically linked to the principle of fairness. Data processing shall be performed "in a transparent manner in relation to the data subject" (Articles 5 (4)(a) and 8 of the Convention). In this regard, data subjects must be informed before processing their data, *inter alia*, about the categories of personal data processed, the purpose of processing and about the identity and address of the controller. In case of joint controllership, controllers need to clarify the purposes of the processing, the means of exercising the rights set out in Article 9, to provide transparency~~, and also a way to demonstrate compliance with the Convention (Article 10)~~[12]. In doing so, in the need to consider the fact that public authorities and private sector entities have different status and legal obligations and may therefore be subject to different data protection regimes.

(…)

Recommendations

(…)

- OEs should, in line with Article 14 of the Convention assess the likely impact of intended ~~[wire/all]~~ 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, ~~S~~such assessment of the country or organisation of destination should aim to ensure that the level of protection afforded by the Convention 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.

(…)

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

General principle

- ~~Any type of information can be personal data if it relates to an identified or identifiable person, which could be information pertaining to the private life of a person, which also includes professional activities, as well as public information about one's life (Article 2 (a) of the Convention 108+).~~ As mentioned above, all information can be personal data provided that it allows or permits the identification of a natural person. The identification does not have to be direct, information that could possibly lead the identification of an individual together with other, maybe only remotely accessible information would also amount for personal data.

(…)

AML/CFT contextualisation[13]

(…)

- 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[14].

[12] European Data Protection Board: "Guidelines 07/2020 on the concept of controller and processor in the GDPR". Version 2.0. July 7th. 2021.
[13] Relevant FATF Recommendations: Rec. 1, 10, 11, 18, 20, 21
[14] FAFT Recommendation 1.

Commented [A12]: IT strange sentence: is it the case only for joint controllerhip?

Commented [A13]: To be corrected in the whole document

Commented [A14]: IT just wonder whether the recommendations on transfers should be moved to the specific section on data transfers.

Commented [A15]: IT What is the difference between "allows" and "permits"?

- Knowing their customers and monitoring their accounts and activities as appropriate for AML/CFT purposes[15] 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[16], as financial crime investigations often require considerable periods of time.

[15] FAFT Recommendation 10.
[16] FAFT Recommendation 11.

- ~~Information sharing within the context of financial group is required both for customer~~

- Being able to detect and report suspicious transactions[18] and ensure that customers are not aware that an STR or underlying information is filed with authorities[19] . It is also to be acknowledged that special categories of data, notably those which relate to ~~based on other legal obligations~~following other international crime-preventing frameworks, contributions to ideological/political organisations, payments of fines etc. ~~that all can contain special categories of data~~ are processed regardless of any extra AML/CFT checks stemming from legal obligations set out by other international crime-preventing frameworks.

(…)

Recommendation

(…)

- Special categories of data, including p~~P~~ersonal data relating to offences, criminal proceedings and convictions, as well as related security measures which are also relevant for AML/CFT, ~~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)[20].

(…)

- Registers holding information on criminal convictions should be restricted to the competent authorities, or to processing under the control of those authorities.

(…)

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

(…)

AML/CFT contextualisation[21]

- Some of the rights expressed in the Convention can be restricted for AML/CFT purposes and usually the restrictions based on AML/CFT laws rely on general public interest (i.e. the 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 – instead, the OEs are invited to inform customers that their personal data may be used for AML/CFT purposes including during ~~subsequent~~further analysis.

Recommandation

- Measures should be put in place by controllers to facilitate the exercise of ~~these~~ data subjects' rights ~~by the data subject,~~ in principle free of charge. In case of automated

Commented [A16]: IT The main sentence is missing before the list of these actions. Is it a list of obligations for OEs?

Commented [A17]: This is true for all special categories of data

Formatted: Indent: Left: 2,54 cm, No bullets or numbering

Commented [A18]: A little bit confusing: here it seems that we are referring to the transparency requirements rather than right of access

Commented [A19]: Not sure it is clear

decision making, if no exception applies, the information on the decision should be available upon request of the data subject. ~~Other example could concern t~~The right not to be subject to only automated decision making should also apply even if ~~e.g., where~~ AI is used ~~to~~ with respect also to the analysis ~~of e~~ transaction data and ~~inform a~~to the decision whether or not a transaction is suspicious and will be transmitted to the FIU. ~~In line with Article 11,~~Clear rules and instructions should be provided in line with Article 11 regarding ~~on~~ if and when data subjects can exercise their right, or if an exception apply~~es~~ and how the "tipping – off" requirement ~~ban~~[22] can be implemented in line with data protection requirements.

Commented [A20]:

(…)

6. Exceptions and restrictions (Article 11)

(…)

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. Further more, the right of access of customers should be guaranteed to the data processed by competent authorities, ~~including FIUs to the extent that, and for long as such a measure constitutes a necessary and proportionate measure in a democratic society.~~., ~~is typically restricted, but where exceptions cannot be used lawfully any more data subjects' rights should be fully guaranteed~~.

Commented [A21]: IT We suggest to delete. This wording is very ambiguous and seems to limit the right of access. The main principle on the contrary Is that – as correctly said in the recommendation -although the right of access could be limited when there is the risk of jeopardising investigations, the limitations should be lifted when there is no longer such risk.

(…)

7. The role of Data Protection Authorities (DPAs) and their relationship with AML/CFT 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 . ~~According to Article 15 of the Convention data protection authorities should have competences on the processing carried out by different controllers in the AML/CFT field.~~The Convention foresees that the powers of the supervisory authorities notably with regard to investigation, intervention, authorizing, blocking cross-border transfer 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[23] can be restricted (Article 11 (3)) provided that such restriction is set forth by law, respect the essence of fundamental rights and freedoms

Commented [A22]:

[17] ~~FATF Recommendation 18.~~
[18] FAFT Recommendation 20.
[19] FAFT Recommendation 21.
[20] See Explanatory Report to Convention 108+, para 56.
[21] Relevant FATF Recommendation 21.
[22] FATF Recommendation 21.2.
[23] ~~To request information related to the international transfer of personal data, to require to the data controller to demonstrate the lawful conditions for international transfer and its ability to intervene and to the Supervisory authority's power to investigate and intervene, functions relating to authorising/blocking international transfer, power on taking regulatory decisions and sanctions and to turn to the judiciary~~

and constitute a necessary and proportionate measure in a democratic society. Even in the latter case the Convention requires that processing activities for national security and defence purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

Recommendation

(…)

- 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 incluDing in respect of the development of possible ~~order to develop~~ effective guidance tools for both public and the private sector and ~~to developof~~ specific training modules.

- In the AML/CFT field, DPAs should work with competent AML/CFT authorities and OEs in order to suggest effective tools and modus operandi for compliance (which could, if correctly implemented, contribute also to a more effective supervision) and also by providing specific training.

Commented [A23]: Still have the feeling of some overlapping between this bullet point and the previous one

8. International data transfers in the AML/CFT field

General principle

- ~~Cross-border~~Transborder data ~~flows~~ transfers occur when~~are~~ personal data ~~transfers is disclosed or made available~~ to a recipient~~s~~ who ~~are is~~ subject to the ~~a foreign~~ jurisdiction of another State or international organisation[24].

Commented [A24]: IT To be consistent with the wording of 108+ ER

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 t

Formatted: Font: (Default) Arial, 10 pt

- o another Party may lead to circumventing the provisions of the Convention or (ii) if a Party is bound to do so by harmonised rules of protection shared by States belonging to a regional international organisation (Art. 14(1) of the Convention).

Formatted: Font: (Default) Arial, 10 pt, English (United Kingdom)

(…)

AML/CFT contextualisation[25]

(…)

- There are several requirements in the FATF Recommendations addressed to public authorities regarding data security which applies when data crosses borders. The revised version of Recommendation 2 requires countries to have cooperation and coordination between Data Protection Authorities (DPAs) and AML/CFT authorities to ensure that data protection principles, rules and considerations are appropriately integrated into AML/CFT obligations.

Commented [A25]: IT Still have some doubts on the reference to Rec 2 which refers to domestic cooperation rather than international

(…)

Recommendation

(…)

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

[24] Explanatory Report of Modernised Convention 108, para. 102.
[25] Relevant FATF Recommendations: Rec. 2, 40.

above-mentioned article and possible exceptions provided for by Article 11. ~~They~~

(…)

- States shall ensure that when exchanges take place towards a country that does not ensure an appropriate level of protection, safeguards established in applicable international data protection legislation and in particular in Convention 108+ shall be respected~~, [including when the data transfer takes place on the basis of a bilateral/Common Reporting Standard (CRS) agreements[26]]~~.

(…)

- The cooperation between data protection authorities and other AML/CFT competent authorities is to be recommended.

Commented [A26]: IT The sentence is not clear Should we say something as "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?"

Commented [A28]: IT This could be merged with the previous bullet point as it may be redundant

Commented [A29]: IT Still have the feeling that we are mixing domestic and international cooperation. We can probably delete this sentence here

NETHERLANDS / PAYS-BAS

General comment: As also mentioned in remark in the text, we noticed that all references to legitimate interest, as a ground for processing by private entities, has been removed in this version of the guidelines. It seems to us that a guideline can articulate a clear preference/recommendation for a legal basis, but cannot rule out other bases, such as legitimate interest, that are currently provided by EU law which is aligned with the Convention. We therefore suggest to not remove the paragraph on legitimate interest.

(…)

9. Basic principles for the protection of personal data

(…)

3.2 The lawfulness of processing – legal basis

(…)

AML/CFT contextualisation[27]

(…)

- Processing of personal data by OEs in the AML/CFT context should preferably be based ~~on legal obligations [/~~on a clear ~~and detailed~~ legal basis that provides for the principles of necessity and proportionality to which the controllers are subject[28]. 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.

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

(…)

Recommendation

(…)

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

(…)

3.3 The fairness and transparency of processing principles

(…)

[27] Relevant FATF Recommendations: Rec. 24, 25.
[28] Explanatory Report of the Modernised Convention, para. 46.

Commented [A30]: This guideline goes beyond current stipulations in the GDPR, that does not discern between the legal basis for a public or private controller. A guideline can articulate a clear preference/recommendation for a legal basis, but cannot rule out other bases, such as legitimate interest, that are currently provided by EU law which is aligned with the Convention. Suggest to not remove the paragraph on legitimate interest.

Commented [A31]: Again, no reason to remove this paragraph. Legitimate interest is a legal ground to process on that cannot be discarded by guidelines.

Recommendation

(…)

- Access to personal data in central beneficial ownership registries should not be freely given as it may constitute 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 ~~specification~~limitation principles. Access to publicly non available data shall be carefully managed taking into account the domestic legislation, rights and interests concerned.

(…)

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

(…)

Recommendation

(…)

- 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[29].

(…)

- Registers holding information on criminal convictions ~~may~~ should be restricted to the ~~processing and use by~~ 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.

(…)

Commented [A32]: Suggest to leave out this addition. This is a matter of margin of appreciation for the members of the convention.

Commented [A33]: Suggest to leave out or further specify, this wording contradicts with observation above that acknowledges that processing of special categories happens regardless.

Commented [A34]: Suggest may, this goes beyond scope guidelines.

[29] Special categories of data according to Article 6 of the Convention: 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.

NORWAY / NORVEGE

(…)

Data protection rules and principles

(…)

3. Basic principles for the protection of personal data

(…)

3.2 The lawfulness of processing – legal basis

(…)

AML/CFT contextualisation[30]

(…)

- For example, data processing is required to prevent the misuse of legal persons for ML or TF by ensuring that there is adequate, accurate and up-to-date information on beneficial ownership and control of legal persons[31]. 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. [In determining the beneficial owners, countries are required to ensure that companies co-operate with competent authorities to the fullest extent possible by (i) requiring that one or more natural persons resident in the country is authorised by the country and accountable to competent authorities to provide all available beneficial ownership information, (ii) requiring that a DNFBP in the country is authorised by the company and accountable to competent authorities for providing all available BO information or taking other comparable measures.] 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.

(…)

3.3 The fairness and transparency of processing principles

(…)

Recommendation

(…)

- Access to personal data in central beneficial ownership registries ~~should not be freely given as it~~ may constitute 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 ~~specification~~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

(…)

Commented [A35]: We believe this sentence is overly specific and should be removed. Methods of effective collection of beneficial ownership information may vary from State to State.

Commented [A36]: This appears to be overly prescriptive, altso taking into account the other criteria that are set out in this paragraph. Hence the suggestion of erasing "should not be freely given".

[30] Relevant FATF Recommendations: Rec. 24, 25.
[31] FATF Recommendation 24.

AML/CFT contextualisation[32]

(…)

- 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[33] 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[34].

Commented [A37]: This requirement appears too detailed. Consider removing the last two: "basic regulating powers, and a list of directors".

(…)

3.6 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 in line with Article 5 (4) (e) of the Convention 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.

Commented [A38]: We assume that R. 11 is the relevant recommendation to refer to here

(…)

[32] Relevant FATF Recommendations: Rec. 6, 7, 10, 17, 24, 37, 40.
[33] FATF Recommendation 24.
[34] Ib idem.

POLAND / POLOGNE

(…)

3. Basic principles for the protection of personal data

3.1 The principle of purpose limitation

(…)

Recommendations

(…)

- The FIUs processing suspicious transaction reports should have clear rules and procedures based on law, concerning the purposes for which personal data relating to STRs may be shared with other competent authorities[35].

(…)

3.2 The lawfulness of processing – legal basis

(…)

Recommendation

(…)

- 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

(…)

Recommendation

(…)

- 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.

(…)

3.4 The data minimisation principle

(…)

AML/CFT contextualisation

(…)

- 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 ~~"Know Your Customer" (KYC) standards~~CDD obligations, ~~they~~ 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

[35] FATF Recommendation 29; C 108+ art. 10; ER para. 85.

Commented [A39]: The item in question states that FIUs should have procedures based on law in this regard. In our opinion such issues should be strictly defined by law, not by internal procedures (legal basis, purpose, scope of data shared are required).

Commented [A40]: FYI: The Polish DPA, when giving its opinion on the draft law amending the Law on Anti-Money Laundering and Financing of Terrorism and Certain Other Laws, raised objections that concerned the provisions governing the operation of the Central Registry of Beneficial Owners. The Polish DPA noted at the time that the DPA had received many signals and concerns about the scope of personal data to be included in the Registry. The Registry is public, which means that access to it is unrestricted. Thus, anyone can have access to the personal data collected in the Registry, most importantly the PESEL (Personal identification number) or the value of the shares of the most important companies' owners. Without questioning the legitimacy of the implementation of Directive 2015/849 (AML), which required EU member states to establish a register of persons exercising direct or indirect control over a company, the so-called "beneficial owners," the Polish DPA noted that national legislation should also be in compliance with the provisions of Regulation 2016/679 and thus ensure adequate protection of personal data processed in the register. According to recital 14 of the aforementioned directive, member states should also ensure that other persons who can demonstrate a legitimate interest in information relating to money laundering, terrorist financing and related crimes - such as corruption, tax offenses and fraud - are given access to information on beneficial owners, while respecting data protection principles. The President of the Polish DPA pointed out that the introduction of legislative amendments to the AML/CFT law should be done in such a way as to comply with the EU's obligation to create an open register of beneficial owners, while at the same time ensuring appropriate tools for the protection of personal data included in the register. A change in the law that would allow access to data from the Registry only to persons with a legal or factual interest would prevent the danger of obtaining data from the Registry, in particular the PESEL, for unlawful purposes. In this connection, attention may be drawn to the above-mentioned demonstration of legal/factual interest.

Commented [A41]: It is worth adding that "resulting from the law".

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 supervisory authoritiesmissing an element of threat or of being fined by financial supervisory authorities, 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. Conversely, due to the limited information position of each individual OE, data minimalisation can be promoted by more focused and streamlined information sharing between OE's to avoid unnecessary information collection by each individual OE in every instance. 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.

Commented [A42]: Collecting data "just in case" is not permissible. The legal basis, scope, purpose should be derived from the law.

(…)

3.6 The storage limitation principle

(…)

AML/CFT contextualisation[36]

- Clear requirements are set for the record keeping period of CDD information, account files, business correspondence and results of any analysis undertaken (at least 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)[37].

Commented [A43]: In our view, the guidelines should also touch on the aspect of the upper limit of data retention . The "Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing" adopted by the EDPB on 15 December 2020, stresses that a period of five years after the end of a business relationship should be considered long.

(…)

Recommendation

- If there are no storage limitation requirements and/or those in place are not in line with FATF Recommendation, data should be stored in line with Article 5 (4) (e) of the Convention 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.

Commented [A44]: In our view, given the long data retention periods, it is important that the law set upper data retention limits based on clear criteria. It also raises the question of whether, if the FATF (Financial Action Task Force) guidelines do not recommend setting an upper data retention period, they will take precedence over the retention limitation rules under both the GDPR and Convention 108.

(…)

[36] Relevant FATF Recommendations: Rec. 2, 11, 24, 29, 40
[37] FATF Recommendation 11.

SWITZERLAND / SUISSE

General comment:

La Suisse a les remarques générales suivantes concernant le projet de lignes directrices AML susmentionné (remarques qui ont également été reprise dans le document ci-joint) :

- En ce qui concerne la traduction des recommandations du GAFI : Il y a une version française qui tient compte des modifications jusqu'à mars 2022. Elle est accessible par le lien suivant Les Recommandations du GAFI (fatf-gafi.org). La version de mars 2022 tient compte de la dernière révision de la R24 et de sa note interprétative (transparence des personnes morales). Il y a par contre eu une nouvelle révision de la R25 et de sa note interprétative (transparence des constructions juridiques [trusts] en février 2023 qui n'est actuellement disponible qu'en anglais.
- Dans la mesure où les normes de référence en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme sont les recommandations du GAFI, il serait bien que les lignes directrices reprennent, dans toute la mesure du possible, la terminologie française employée dans la version française des recommandations du GAFI (en particulier le glossaire général). Sinon cela risque de créer une certaine confusion pour le lecteur. Le problème ne se pose pas en anglais, car la version anglaise reprend en principe fidèlement la terminologie anglaise des recommandations du GAFI.
- Il y a aussi une certaine confusion du fait que tant le GAFI que la Convention 108 parlent d'autorités de contrôle (en anglais supervisory authorities), si bien que lorsque l'expression est employée, on ne sait pas si on se réfère aux autorités antiblanchiment ou aux autorités de protection des données ou aux deux. Généralement la version anglaise parle de DPA (data protection authorities) lorsqu'il s'agit de désigner les supervisory authorities en matière de protection des données. Il n'y a donc pas de confusion. Par contre, dans la version française, je ne sais pour quelle raison l'expression « autorités chargées de la protection des données » a quasiment été remplacée partout par « autorités de surveillance » ou « autorités de contrôles », créant une certaine confusion.

(…)

Projet de lignes directrices sur la protection des données ~~personnelles~~

dans le traitement des données ~~personnelles~~ à caractère personnel en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

Règles et principes de protection des données

1. Introduction

1.1. Généralités

Le blanchiment de capitaux et le financement du terrorisme (BC/FT) passent fréquemment par des activités transfrontalières et par un usage détourné d'institutions et d'entités, financières et non financières, situées sur de multiples territoires. Le partage de données entre acteurs étatiques et non étatiques est donc crucial pour lutter efficacement contre ces phénomènes criminels. Le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme

(LBC/FT[38]) poursuit à la fois des buts de prévention, d'investigation et de poursuites, à travers un système de mesures mises en œuvre par de multiples acteurs : en particulier, les entités soumises à obligation de déclaration (EO) et leurs clients, les cellules de renseignement financier (CRF), les services répressifs et de supervision, les autorités chargées des poursuites, les systèmes judiciaires, les douanes et les responsables politiques à différents niveaux.

(…)

Le traitement des données à caractère personnel pour de telles finalités peut constituer une ingérence dans le droit de la personne concernée au respect de sa vie privée, tel qu'il est protégé par l'article 8 de la Convention européenne des Droits de l'Homme (CEDH) et par d'autres ~~les~~ instruments internationaux relatifs aux droits de l'homme ~~(~~notamment l'article 12 de la Déclaration universelle des droits de l'homme (DUDH), l'article 17 du Pacte international des droits civils et politiques (PIDCP), l'article 11.2 de la Convention américaine des droits de l'homme (CADH), l'article 4 de la charte africaine des droits de l'homme et des peuples (CADHP) ~~et l'article 8 de la Convention européenne des Droits de l'Homme (CEDH)~~. La vie privée d'un individu doit être interprétée au sens large, y compris les informations relevant à la fois de sa sphère privée et de sa vie professionnelle ou publique. Tout type d'information peut être une donnée personnelle s'il se rapporte à une personne identifiée ou identifiable, qui pourrait être une information relative à la vie privée d'une personne, ce qui inclut également les activités professionnelles, ainsi que des informations publiques sur sa vie (article 2 (a) de la Convention 108+).En vertu de l'article 11 de la Convention 108 modernisée, les exceptions et restrictions à ce droit ne sont admises que si elles poursuivent un objectif légitime d'intérêt public et (i) sont prévues par la loi, (ii) respectent l'essence des droits et libertés fondamentales et (iii) constituent une mesure nécessaire et proportionnée dans une société démocratique pour atteindre ce but légitime.

Le régime de LBC/FT prévoit plusieurs contextes de traitement des données à caractère personnel, qui sont essentiellement fondés sur l'intérêt public, en définissant des obligations détaillées pour les responsables du traitement. Cela s'étend au traitement des données à caractère personnel par les autorités gouvernementales qui sont habilitées par la loi à lutter contre la LBC/FT et qui sont dotées de pouvoirs spécifiques dans ce domaine. Néanmoins, il n'en va pas de même pour les institutions du secteur privé, qui sont des ~~OE~~EO, qui n'ont pas le même statut juridique ni le même mandat. Dans le même temps, leur rôle et leurs obligations concrètes en tant que gardiens pour prévenir l'utilisation abusive du système financier à des fins de BC/FT doivent également être dûment reconnus. Cependant, le traitement des données par les entités du secteur privé sur la base légale de l'intérêt public doit être envisagé avec prudence et seulement lorsqu'une base légale claire autorisant ce traitement existe, notamment dans le contexte des nouvelles initiatives de mise en commun de données qui impliquent le partage des données entre les entités du secteur privé (qui ne font pas partie du même groupe financier).

(…)

~~L'évolution~~ Les développements récents~~e~~ dans des domaines importants tels que l'accès du grand public à l'information sur ~~la propriété effective~~les bénéficiaires effectifs[39], qui a été considéré~~e~~ comme constituant une ingérence grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel[40], car cela rend public toute donnée personnelle de chaque bénéficiaire effectif dans un pays. ~~Ce cas~~ montrent que ce domaine est en constante évolution et que de plus en plus de réglementation, y compris de droit contraignant, mais aussi d'autres jurisprudences dans ce domaine sont attendues dans un proche avenir.

[38] Normes LBC/FT ~~au niveau mondial : normes du GAFI ;~~ au niveau du CdE : Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE n° 198). Pour ce document, les articles suivant de la Convention du Conseil de l'Europe STCE No.198 sont d'importance particulière : articles 7, 17, 18, 19, 20, 43, 46, 47. Au niveau universel en matière de BC/FT : normes du GAFI.

[39] Voir la définition de « l'information sur ~~la propriété effective~~les bénéficiaires effectifs » en annexe ~~I~~1.

[40] Arrêt de la CJUE du 22 novembre 2022 dans les affaires jointes C-37/20 Luxembourg Businesses Registers et C-601/20 Sovim

Commented [A45]: CH : Nous nous permettons de soulever la question suivante : De manière générale la terminologie en anglais et en français n'est pas très claire, ni vraiment cohérente avec la terminologie du GAFI. Dans le texte anglais on a: supervisory and law enforcement authorities (LEAS), prosecution authorities. Dans le langage du GAFI : supervisory authorities ou supervisors = autorités de contrôle ; law enforcement authorities = autorités de poursuite pénale. Prosecution authorities n'est employé qu'une seule fois et est traduit par autorités judiciaires. Par contre le terme prosecution revient plusieurs fois et est systématiquement traduit par « poursuites ».

Est-ce que ce qui est visé par « services représsifs » est assez clair pour le lecteur ? En quoi ses services se distinguent-ils des autorités chargées des poursuites ? La question se pose aussi en anglais : quelle est la différence entre law enforcement authorities et prosecution authorities ?

Commented [A46]: CH : cf. la version anglaise.

Commented [A47]: CH : Cf. plus haut : entités soumises à obligation de déclaration (EO)

Commented [A48]: CH : Il semblerait utile de reprendre la terminologie bien connue du GAFI de bénéficiaires effectifs, puisque les recommandations du GAFI constituent la norme de référence. Cf. ch 1 de la note interprétative de la Recommandation 24 qui mentionne entre parenthèses les « informations sur les bénéficiaires effectifs », définies plus précisément dans la note de bas de page 47.

Commented [A49]: CH : Se réfère à l'accès => considéré

Commented [A50]: CH : La phrase n'est pas correcte, ni en français, ni en anglais. Il manque un verbe pour le sujet de la phrase.

Étant donné que la protection des données est fondamentale pour garantir le droit au respect de la vie privée, de la vie familiale, de la correspondance et du domicile (article 8 de la CEDH), il convient de tenir compte des règles et principes qui l'encadrent lorsqu'on agit dans l'intérêt de la lutte contre le blanchiment de capitaux et le financement du terrorisme, conformément aux engagements et obligations des États parties découlant du droit international. En vertu de la législation, l'existence d'un objectif légitime, d'une base juridique valable et de garanties appropriées pour le traitement des données à caractère personnel est une condition préalable, pour laquelle la logique sous-jacente doit être soigneusement analysée et énoncée par les principaux acteurs des domaines de la LBC/FT, de la protection des données et des droits de l'homme. Compte tenu du fait que le traitement et le partage des données jouent un rôle crucial dans la LBC/FT, ces lignes directrices[41] mettront l'accent sur les exigences ~~– telles que~~ prévues par la ~~convention sur la protection des personnes à l'égard du traitement des données personnelles (STE No. 108) telle qu'amendée par le Protocole STE No. 223 (« c~~Convention 108+ ~~»)~~ ~~que~~ pour les responsables du traitement et les sous-traitants ~~doivent appliquer pour respecter les obligations en matière de protection des données prévues par la Convention 108+,~~ tout en se conformant au cadre de la lutte contre le ~~L~~LBC/FT.

1.2 Champ d'application

Les lignes directrices couvriront le traitement et le partage des données à des fins de LBC/FT par des entités publiques et privées dans les États parties à la Convention 108+, y compris les exigences pour le flux ~~transfert~~ transfrontière de données à caractère personnel ~~de commande cross-b~~ lorsqu'elles coopèrent avec des États non parties (au sens de l'article 14). Elles pourraient également servir d'orientation aux Parties non étatiques à la Convention dans le contexte de la LBC/FT.

Leur objectif est de fournir des orientations sur la manière d'intégrer ~~les règles et normes internationales en matière de protection des données [y compris~~ les exigences de la Convention 108+~~]~~ dans le domaine de la LBC/FT afin d'assurer un niveau de protection approprié tout en facilitant les flux de données transfrontaliers, et de mettre en évidence certains domaines dans le contexte de la LBC/FT dans lesquels des garanties en matière de protection des données ~~devraient être mises en place [ou pourraient~~ devraient ~~avoir besoin d'~~être renforcées~~]~~.

(…)

2. Définitions et terminologie employées pour ces lignes directrices

(…)

Données ~~personnelles~~ à caractère personnel et personne concernée - L'article 2 (*a*) de la Convention définit les ~~données personnelles~~à caractère personnel comme toute information relative à une personne physique identifiée ou identifiable (personne concernée). Une personne est considérée comme identifiable lorsqu'il est possible d'obtenir, sans délais ni efforts déraisonnables, des compléments d'information qui peuvent permettre à terme d'identifier directement ou indirectement la personne concernée. ~~La notion de vie privée d'un individu est à interpréter au sens large, en englobant les informations relatives à sa sphère privée, mais aussi à sa vie professionnelle ou publique.~~ Dans le contexte de la LBC/FT, les clients, les bénéficiaires effectifs[42], les parties aux virements électroniques, ou les personnes dont les informations identifiables sont contenues dans les transferts de données, doivent être

Commented [A51]: CH : Le L se réfère déjà à la lutte. Il doit donc être supprimé. Sinon, il faut reprendre la formulation alternative suivante : « tout en se conformant au cadre de la LBC/FT »

Commented [A52]: CH : cf. chapitre III C108+ ; si l'on veut utiliser la terminologie de la C108+, il faudra aussi modifier le terme « cross-border data transfer » par « transborder flows of personal data » dans la version anglaise.

Commented [A53]: CH : cf. la définition figurant dans le Glossaire général des recommandations du GAFI , p. 132: Les Recommandations du GAFI (fatf-gafi.org)

La deuxième phrase est erronée. Il s'agit de la reprise d'une note de bas de page en lien avec la définition des autorités de contrôle, ce qui n'a rien à voir avec la définition du bénéficiaire effectif.

[41] Les lignes directrices ont été élaborées en tenant compte des contributions de plusieurs membres, d'experts et du Secrétariat du Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme (MONEYVAL).

[42] Selon la définition du GAFI, un bénéficiaire effectif est la ou les personnes physiques qui en dernier lieu possède ou contrôle ~~en dernier ressort~~ un client et/ou la personne physique pour le compte de laquelle une ~~transaction~~ opération est effectuée. ~~Ceci inclut les autorités de contrôle visées par les Principes fondamentaux qui exercent des fonctions de contrôle liées à la mise en œuvre des recommandations du GAFI.~~ Sont également comprises les personnes qui exercent en dernier lieu un contrôle effectif sur une personne morale ou une construction juridique.

considérés comme des personnes concernées. Ils sont les principaux sujets des mesures de vigilance à l'égard de la clientèle (CDD)[43], y compris l'identification et la vérification de l'identité. Alors que la Convention 108+ protège principalement les données ~~personnelles~~ à caractère personnel des personnes physiques, les Parties peuvent étendre la protection dans leur droit national aux données relatives aux personnes morales afin de protéger leurs intérêts légitimes[44], bien que les données d'entreprises ne soient pas à considérer comme des données à caractère personnel~~personnelles~~, à moins qu'elles ne concernent une personne physique (sociétés unipersonnelles ou données relatives aux clients, par exemple).

(…)

Dans le contexte de la LBC/FT, les entités soumises à obligation de déclaration (EO) sont soi~~ent~~t seules, soit co-responsables du traitement. Les EO peuvent être des institutions financières (IF[45]), des entreprises et professions non financières désignées[46] (EPNFD) ou des prestataires de services d'actifs virtuels (PSAV). Les destinataires des informations, notamment les cellules de renseignement financier (CRF), les autorités répressives ou d'autres entités y compris celles qui gèrent les registres ~~publics~~ d'informations sur les propriétaires de base et les bénéficiaires effectifs, doivent être considérés comme des responsables du traitement de données pour le traitement des données à caractère personnel qu'ils effectuent.

Le cadre de la LBC/FT peut prévoir différentes situations de partage d'informations, notamment entre les EO, entre les personnes morales et les contrôleurs des registres ~~de propriété effective~~sur les bénéficiaires effectifs, entre les EO et les cellules de renseignement financier (CRF) ou entre les EO et une autre autorité compétente (« partenariats public-privé/PPP »), entre les CRF, les services répressifs ~~et de supervision~~ et les autorités judiciaires de différents pays et entre les CRF et d'autres autorités compétentes. Dans ce scénario, lorsque les différents responsables du traitement ont le pouvoir de décider des aspects pertinents des opérations de traitement concernant les mêmes données ~~personnelles~~à caractère personnel, telles que le but dans lequel la donnée personnelle est traitée, ils doivent être considérés comme des responsables conjoints du traitement[47]. Ce statut conjoint entraîne la responsabilité conjointe d'une activité de traitement. Afin de répondre à des réalités de traitement des données de plus en plus complexes, le traitement conjoint peut prendre différentes formes et la participation des différents responsables du traitement peut être inégale. Par conséquent, ils doivent déterminer leurs responsabilités respectives en ce qui concerne le respect des obligations prévues par le règlement d'un accord spécifique.

(…)

Catégories particulières de données à caractère personnel (données sensibles) - Dans l'article 6, il existe des catégories particulières de données à caractère personnel dont le traitement est, par nature, susceptible de présenter un risque plus élevé pour les personnes concernées. Leur traitement nécessite donc d'autres garanties complétant celles déjà en place pour les catégories ~~« normales/simples »~~ de données de ~~/~~données ~~personnelles~~à caractère

Commented [A54]: CH : Concernant la note de bas de page, cf. la définition des entreprises et professions non financières désignées dans le Glossaire général des recommandations du GAFI, p. 136

Commented [A55]: CH : Ne figure pas dans la version anglaise

Commented [A56]: CH : le « telles » ne se réfère-t-il pas aux aspects, auquel cas il conviendrait de le remplacer par « tels » ?

[43] La ~~diligence raisonnable~~vigilance à l'égard de la clientèle (CDD) est un processus dans lequel les informations pertinentes sur le client d'une entité obligée sont collectées et évaluées du point de vue du ~~ML/TF~~BC/FT. Les entités soumises à l'obligation de déclaration doivent avoir mis en place des procédures pour identifier et éventuellement signaler les risques de blanchiment et de financement du terrorisme associés à une relation d'affaires ou à une transaction occasionnelle. Les recommandations 10, 11, 12, 15 et 17 du GAFI détaillent les mesures CDD de base et supplémentaires que doivent adopter les institutions financières. La recommandation 22 étend ces mesures aux entreprises et professions non financières désignées (~~DNFBP~~EPNFD).

[44] Rapport explicatif de la Convention 108 modernisée, paragraphe 30.

[45] Le terme Institution financière (IF) dans le domaine de la LBC/FT, tel qu'il est utilisé dans les présentes lignes directrices, comprend à la fois les établissements de crédit et les institutions financières.

[46] Par exemple les casinos, agents immobiliers, négociants en métaux précieux et pierres précieuses, avocats, notaires, autres professions~~nels du droit juridiques~~ indépendante~~s~~, ainsi que les comptables (lorsqu'ils agissent ~~à titre d'avocats exerçant seuls~~comme membres d'une profession libérale exerçant à titre indépendant, d'associés ou de ~~professionnels~~ salariés au sein de cabinets professionnels) et les prestataires de services aux trusts et aux sociétés ~~et fiducies~~ (pour la fourniture de certains services). Toutefois, certains secteurs ne sont pas toujours saisis de façon appropriée (p. ex., les avocats et les comptables internes).

47 Conformément au paragraphe 22 du rapport explicatif de la Convention 108+ (coresponsable d'un traitement et éventuellement responsable de différents aspects de ce traitement).

personnel en général]. Les catégories ci-après de données à caractère personnel considérées comme sensibles sont celles qui révèlent : i) des origines raciales ou ethniques, ii) des opinions politiques, des convictions religieuses ou autres, y compris les convictions philosophiques, iii) de l'appartenance syndicale, iv) des données génétiques, (v) des données biométriques traitées dans le but d'identifier une personne de manière unique, vi) de l'état de santé, (vii) la vie sexuelle ou l'orientation sexuelle, viii) des infractions, procédures pénales,et condamnations pénales et mesures de sécurité sûreté connexes.

3. Principes de base pour la protection des données à caractère personnel

3.1 Le principe de la limitation de la finalité

(…)

Dans le contexte de la LBC/FT[48]

- Les données personnelles à caractère personnel sur le client, ou les données transactionnelles qui peuvent être collectées par les EO à des fins de vigilance à l'égard de la clientèle, peuvent – dans certaines conditions prévues par la loi – être partagées avec d'autres entités obligées appartenant au même groupe, ou avec des tiers[49], afin de remplir des finalités compatibles supplémentaires (par exemple, informer une EO appartenant au même groupe au sujet d'un client commun qui peut avoir fait l'objet d'une déclaration à la CRF un intermédiaire d'assurance collectant des données CDD qui sont à leur tour transmises à la compagnie d'assurance qui vendrait et émettrait la police d'assurance-vie). Par exemple, dans les relations de correspondance bancaire, la banque correspondante peut avoir besoin d'exiger des informations supplémentaires concernant un client de la banque répondante, qui auraient été recueillies par cette banque auprès de son client dans un contexte différent.

(…)

- Parfois, des données collectées et traitées dans un but précis (par exemple, des informations sur la vigilance à l'égard de la clientèle ou des informations sur des transactions suspectes) doivent peuvent être partagées avec des tiers. Par exemple, une CRF qui analyse une déclaration d'opération suspecte (DODDOS) peut trouver des liens internationaux qui l'incitent à solliciter partager des informations complémentaires pertinentes de la DOS (notamment des renseignements à caractère personnel) auprès d'avec une autre autorité compétente ou d'une CRF étrangère dans le cadre d'une programme demande d'entraidevisant à obtenir des informations supplémentaires.

- À l'occasion, l'EO peut avoir besoin de déposerdevoir effectuer une déclaration d'opération suspecte auprès de la CRF. Le traitement des données à caractère personnel par la CRF constitue dans ce cas une finalité supplémentaire qui est considérée comme compatible avec la finalité initiale du traitement. La CRF peut en outre être amenée à signaler une suspicion d'activité criminelle à une autorité compétente. Le traitement des dossiers par les autorités compétentes en matière d'enquête et de poursuites est généralement régi par d'autres lois.

- Les données personnelles à caractère personnel doivent être utilisées aux seules fins pour lesquelles elles ont été fournies et ne peuvent être transférées à d'autres

Commented [A57]: CH : Le « have to » a été supprimé en anglais.

[48] Les recommandations pertinentes du GAFI sont : Rec. 10-12, 13, 15-18, 20, 22-25, 27, 29, 31, 40.
[49] Dans ce contexte, il convient d'interpréter par « tiers » toute personne physique ou morale extérieure à et ne faisant pas partie de l'entité ou de son groupe financier.

autorités des pays destinataires des données, à moins que les exigences énoncées dans la Convention ne soient respectées.

Recommandations

(…)

- Les EO appartenant à un groupe doivent disposer de politiques et de procédures claires, fondées sur la loi, pour définir quel type de données à caractère personnel (client, bénéficiaire effectif, transactionnel, compte, déclaration d'opération suspecte ou DOS) elles peuvent échanger entre elles[50], sur quelle base juridique et dans quel but. Cela pourrait être fait conformément à l'~~A~~article 14 de la Convention y compris des clauses contractuelles types valides ~~en utilisant~~ telles que des règles d'entreprise contraignantes, ou des clauses ad hoc venant d'instruments légalement contraignants en vigueur.

- Les CRF qui traitent les déclarations ~~de transactions~~d'opérations suspectes devraient disposer de règles et de procédures claires, fondées sur la loi, concernant les fins auxquelles les données ~~personnelles~~ à caractère personnel relatives aux déclarations peuvent être partagées avec d'autres autorités compétentes[51].

- Lorsque des données à caractère personnel sont traitées dans le cadre d'un scénario de dépendance[52] à l'égard de tiers[53], les deux parties devraient avoir mis en place des règles et des procédures claires qui régissent non seulement la fourniture d'informations à des fins de vigilance à l'égard de la clientèle, mais aussi des garanties adéquates pour la protection des données à caractère personnel traitées à des fins données.

- En ce qui concerne les relations de correspondance bancaire transfrontière et les autres relations similaires[54] , il faudra prévoir des dispositions claires et détaillées, fondées sur la loi, entre le correspondant et la banque répondante pour réglementer le partage par la banque répondante des données à caractère personnel concernant ses clients, ses bénéficiaires effectifs et ses opérations. The provision should detail the type of data that the respondent bank will have to provide upon the request of the correspondent bank. Il peut en aller de même pour des relations similaires pertinentes en dehors du secteur bancaire (par exemple, entreprises d'investissement, établissements de paiement). Des orientations à cet égard devraient être fournies par les autorités ~~chargées de la protection des données~~ de surveillance.

- Il convient aussi de mettre en œuvre, conformément à l'article 5(4)(c) de la Convention 108+ le principe de limitation de la finalité également dans le contexte du partage/transfert de données par les CRF avec d'autres destinataires y compris des services répressifs nationaux[55], mais aussi avec les CRF étrangères[56] . Dans ce cas, des procédures ~~pour la mise en œuvre des normes internationales~~internes normalisées devraient être élaborées pour garantir que les données soient partagées pour une finalité spécifique et limitée, et documentées au cours du

Commented [A58]: CH : le GAFI parle de « recours à des tiers » cf. Recommendation 17.

Commented [A59]: CH : La note de bas de page ne correspond pas au texte anglais. Elle ne fait que répéter la note de bas de page précédente.

Commented [A60]: CH : Ne correspond pas tout à fait à l'anglais tel que modifié : between the correspondent and the respondent institutions, including banks

Commented [A61]: CH : La traduction de cette phrase a été oubliée

Commented [A62]: CH : Le texte anglais mentionne les autorités de protection des données et non les autorités de surveillance. Si on parle d'autorité de surveillance ou de contrôle, on ne sait pas si on parle des autorités de surveillance/contrôle chargées de la protection des données ou des autorités de surveillance/contrôle en matière de LBC/FT. Il conviendrait donc d'être extrêmement précis pour savoir quelles autorités sont visées.

Commented [A63]: CH : L'anglais ne parle pas de mise en œuvre des normes internationales mais de « internal standard operating procedures »

[50] GAFI, recommandation 18 ; C108+ : articles 5(1), 14(2) (3) ; paragraphes 40, 42, 109-111 du Rapport explicatif.
[51] GAFI, recommandation 29 ; C108+ articles 10 ; paragraphe 85 du Rapport explicatif.
[52] Dans ce contexte, le terme « tiers » désigne les institutions financières ou les EPNFD qui sont supervisées ou surveillées et qui satisfont aux exigences de la Recommandation 17 du GAFI.
[53] ~~Dans ce contexte, le terme « tiers » désigne les institutions financières ou les EPNFD qui sont supervisées ou surveillées et qui satisfont aux exigences de la Recommandation 17 du GAFI.~~ 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.
[54] GAFI, recommandation 13 ; et C108+ article 14(2) (3) ; paragraphes .109-111 du Rapport explicatif.
[55] GAFI, recommandations 29 et 31.
[56] GAFI, recommandation 40 ; et C108+ article 14(2) (3) ; paragraphes .109-111 du Rapport explicatif.

transfert, et qu'une protection essentielle équivalente soit assurée pendant le transfert ainsi que par les autorités destinataires.

3.2 La licéité du traitement – base juridique

(…)

Dans le contexte de la LBC/FT[57]

(…)

- Comme déjà expliqué, ~~P~~pour constituer une base juridique au traitement de données à caractère personnel, le consentement doit être libre, éclairé, spécifique et non équivoque ; le consentement au traitement doit être clairement affirmé. Dans le contexte de la LBC/FT, la question d'un consentement « librement » donné devrait être examinée attentivement et il convient de veiller à ce que la personne concernée ait le choix. Si tel n'est pas le cas, le traitement des données doit être basé sur une autre base juridique. ~~Par conséquent, il est très peu probable que cette base juridique soit utilisée à des fins de LBC/FT, car elle sera probablement supplantée par d'autres bases juridiques. [Cependant, il est très peu probable que cette base légale soit utilisée à de fins de LBC/FT~~ comme à d'autres fins, ~~la personne concernée n'ayant pas vraiment le choix. Un fondement légal alternatif doit être trouvé car, même dans le cas d'un consentement, il ne sera probablement pas valable (ce qui invaliderait potentiellement la procédure). Plus précisément,]~~ ~~T~~ Le cadre LBC/FT, qui suppose souvent des investigations spécifiques sur les activités de BC/FT établies ou soupçonnées, prévoit des situations où le client n'est pas ou ~~pas entièrement~~ seulement partiellement informé du traitement des données, en particulier en ce qui concerne les obligations de déclaration des ~~transactions~~opérations suspectes par l'EO, la fourniture de données à caractère personnel en réponse aux demandes d'informations des CRF et des LEA et l'application des ordonnances de contrôle. Dans ces cas, l'information préalable du client contredirait les interdictions associées à la LBC/FT, en particulier l'interdiction d'avertir le client[58].

- Le motif licite autorisant les pouvoirs publics à traiter des données à caractère personnel peut être celui de l'intérêt public, dans la mesure où ils sont investis ~~de~~ du pouvoir de lutter contre le ~~BT~~BC/FT et de fonctions spécifiques dans ce domaine. Des mécanismes régulateurs ainsi qu'un contrôle sont également mis en œuvre. Il n'en va cependant pas de même pour les institutions du secteur privé, qui sont des entités obligées et ne bénéficient ni du même statut juridique, ni du même mandat.

(…)

- Par exemple, le traitement des données est nécessaire pour éviter l'utilisation de personnes morales à des fins de BC ou de FT, en assurant des informations satisfaisantes, exactes et à jour sur les bénéficiaires effectifs et sur le contrôle des personnes morales[59]. Les informations sur les bénéficiaires effectifs d'une société devraient être accessibles en temps opportun par une autorité compétente par soit un registre ~~de propriété effective~~sur les bénéficiaires effectifs ou un mécanisme alternatif. [Afin de déterminer les bénéficiaires effectifs, les pays sont tenus de s'assurer que les sociétés coopèrent dans toute la mesure du possible avec les autorités compétentes, i) en exigeant qu'une ou plusieurs personnes physiques résidant dans le pays, autorisées par la société et responsables vis-à-vis des autorités compétentes communiquent toutes les informations disponibles sur les bénéficiaires effectifs ; et ii) en exigeant qu'une EPNFD dans le pays soit autorisée par la société à communiquer toutes les informations disponibles sur les bénéficiaires effectifs ou à prendre d'autres mesures comparables, et en soit responsable vis-à-vis des autorités.] Dans le même

[57] Recommandations du GAFI pertinentes : 24, 25.
[58] Recommandation du GAFI 21.
[59] GAFI, recommandation 24.

Commented [A64]: CH : Cette abréviation anglaise n'a jamais été utilisée auparavant dans le texte en français. Il faudrait s'en tenir à la terminologie employée en début du document.

Commented [A65]: CH : pas vraiment certaine de la traduction (monitoring orders) ou de ce qui est visé ici.

Formatted: Highlight

Commented [A66]: CH : Ce passage se réfère à l'ancien paragraphe 9 de la note interprétative de la Recommandation 24. Or le GAFI a révisé cette note interprétative et a notamment renoncé à l'exigence d'une personne physique résidente dans le pays. Cette ancienne exigence ne figure désormais plus que dans les lignes directrices sur la transparence des personnes morales Guidance-transparency-beneficial-ownership.pdf à titre d'exemple de meilleures pratiques.

Ce passage devrait être révisé sur la base de la nouvelle version de la note interprétative à la Recommandation 24, désormais disponible également en français. Les Recommandations du GAFI (fatf-gafi.org)

Cf. le passage pertinent : FATF Recommendations 2012.pdf (fatf-gafi.org), paragraphe 7, lettre (a), p. 93.

(a)Countries should require companies […]; **to co-operate with competent authorities to the fullest extent possible in determining the beneficial owner, including making the information available to competent authorities in a timely manner; and to co-operate with financial institutions/DNFBPs to provide adequate, accurate and up-to-date information on the company's beneficial ownership information.**

(a) Les pays devraient obliger les sociétés à : […]; **coopérer avec les autorités compétentes dans toute la mesure du possible afin de déterminer le bénéficiaire effectif, y compris rendre disponible l'information aux autorités compétentes en temps opportun ; coopérer avec les institutions financières/EPNFD afin de fournir les informations satisfaisantes, exactes et à jour sur leurs bénéficiaires effectifs.**

Il conviendrait de modifier **l'anglais e**n conséquence.

temps, lorsqu'elles donnent accès aux informations ~~de BO~~sur les bénéficiaires effectifs, les autorités compétentes devraient dûment tenir compte du droit au respect de la vie privée des personnes concernées, en tenant compte de leurs droits et libertés et de l'incidence que cet accès peut avoir ~~en ayant une incidence~~ sur ces droits.

- L'existence d'initiatives de partage d'information à travers des partenariats public-privé (PPP) a été notée dans plusieurs ~~administrations~~juridictions. Si les possibilités qu'ils offrent dans la lutte contre la criminalité financière sont importantes, il reste des défis qui sont également de nature législative (par exemple, des modifications législatives peuvent être nécessaires pour garantir une base juridique appropriée et permettre aux partenaires d'atteindre leurs objectifs).

Recommandations

- Le traitement des données dans le contexte LBC/FT devrait être effectué sur la base d'un fondement légal clair et détaillé ~~[~~respectant les principes de nécessité et de proportionnalité~~]~~ ~~[~~/et avec des garanties appropriées~~]~~.

(…)

- Des dispositions claires et détaillées qui tiennent compte de tous les droits et intérêts concernés sont établies en ce qui concerne les PPP créés pour le partage d'informations opérationnelles ~~sur~~ et les renseignements concernant les suspects, y compris en ce qui concerne les données à caractère personnel partagées par les autorités répressives et la base juridique claire pour le traitement ultérieur. Ces règles devraient couvrir: (i) qui ~~participe, pour~~ peut s'assurer que les informations sont fournies selon le principe du strict besoin d'en connaître, (ii) la finalité ~~de l'utilisation~~ du partage de données à caractère personnel~~, des engagements~~ et des autres traitements partagés et (iii) l'exigence ~~d'assurances~~ que les destinataires de données à caractère personnel auront mis en place des garanties appropriées et (iv) garantir que seules les données à caractère personnel strictement nécessaires à l'analyse ou à l'enquête opérationnelle en cours sont divulguées et partagées, et des demandes claires et précises concernant l'ensemble de données nécessaires à soumettre par les entités soumises à obligation de déclaration.

- L'accès aux données ~~personnelles~~ à caractère personnel des registres centraux des bénéficiaires effectifs ne devrait être autorisé que dans les situations ou dans la mesure prévue par la loi, et dans le respect des normes et réglementations internationales en matière de protection des données.

3.3 La loyauté et la transparence des principes de traitement

Principe général

- Les données à caractère personnel sont traitées de manière non seulement licite, mais aussi loyale, tant par le responsable du traitement que par le sous-traitant (article 5.4 de la Convention). Ce principe requiert~~, dans la mesure du possible,~~ la communication à la personne concernée d'informations sur le traitement de ses données, y compris sur les risques éventuellement identifiés par le responsable ou le sous-traitant, pour lui permettre de prendre une décision éclairée et d'exercer ses droits en matière de protection des données sauf si une exception s'applique conformément à la Convention. En outre, ~~l'équité~~ la loyauté exige également d'évaluer les conséquences que le traitement des données aura sur la personne concernée. Les opérations de traitement ne sauraient être réalisées en secret.

(…)

Dans le contexte de la LBC/FT[60]

- Le traitement de données à des fins d'intérêt public ne devrait pas être par définition considéré comme loyal : les responsables du traitement relevant du secteur public doivent observer ces principes, sauf si une exception s'applique conformément à l'Aarticle 11 de la Convention.

- Les ~~institutions financières~~ EO sont obligées[61] de prendre des mesures de vigilance à l'égard de leur clientèle par exemple dans les cas suivants : fi) ~~par exemple lorsqu'~~elles établissent des relations d'affaires, ii) elles effectuent des opérations occasionnelles supérieures au seuil désigné applicable ~~(15 000 USD/EUR)~~, iii) elles effectuent des opérations occasionnelles sous forme de virements électroniques[62], iv) il existe un soupçon de BC/FT ou v) elles doutent de la véracité ou de la pertinence des données d'identification personnelle précédemment obtenues]. Il appartient aux ~~institutions financières~~EO d'identifier le client (personne physique ou morale ou ~~structure~~construction juridique, permanente ou occasionnelle) et de vérifier son identité au moyen de sources fiables et indépendantes[63]. Elles doivent aussi vérifier que toute personne prétendant agir pour le compte du client ou du bénéficiaire effectif est autorisée à le faire et identifier et vérifier l'identité de cette personne. Les ~~institutions financières~~EO, en particulier les banques, informent généralement leur clientèle des finalités pour lesquelles ses données seront traitées et, le cas échéant, partagées avec des tiers et requièrent son consentement, bien que cela ne fasse pas partie des exigences du GAFI et que les pratiques varient d'un pays à l'autre, en fonction de la législation locale sur la protection des données. Dans certaines circonstances spécifiques, les EO peuvent aussi requérir le consentement d'un client, en particulier pour la prestation de certains services ou à l'occasion de la divulgation à des tiers de données relatives à la clientèle.

- Dans certains cas, outre la réglementation sur la protection des données, il existe des obligations de secret bancaire[64] ou d'autres obligations de secret professionnel qui s'appliquent à ~~certaines personnes~~des professionnels du droit ~~indépendants~~ ~~(par~~

[60] Recommandation pertinente du GAFI : 10, 22 et 23.
[61] La recommandation 10 du GAFI fait de ces mesures la norme minimum que les pays devraient mettre en place.
[62] Dans ces circonstances, voir la recommandation 16 du GAFI sur les virements électroniques.
[63] GAFI, recommandation 10.
[64] La recommandation 9 du GAFI stipule que les lois sur le secret professionnel des institutions financières ne doivent pas entraver la mise en œuvre des recommandations du GAFI.

~~exemple, les avocats)~~[65] ~~des professionnels du droit~~ tels que les avocats, les notaires, les membres des autres profession~~nel~~s juridiques indépendante~~s~~ et les comptables agissant à titre de professionnels juridiques indépendants~~indépendants~~. Ils ne sont pas tenus de ~~signaler les transactions~~déclarer les opérations suspectes ou de fournir des informations sur les clients ~~des clients~~ aux forces de l'ordre ou aux CRF lorsque ces informations ~~seraient~~sont obtenues: a) dans le cadre de l'évaluation de la situation juridique de leur client, ou b) dans l'exercice de leur mission de défense ou de représentation de ce client ~~client~~ dans ~~ou concernant des~~le cadre de procédures judiciaires, administratives, arbitrales ou de médiation, ou en lien avec ces procédures[66].

- Afin de faciliter l'accès à des informations ~~précises~~ exactes et ~~actualisées~~ à jour sur ~~la propriété effective~~les bénéficiaires effectifs, certains États ont créé des registres centraux comprenant des informations fournies par des personnes morales. L'accès à ces informations est généralement donné aux EO ~~aux fins de diligence raisonnable~~ à des fins de vigilance à l'égard de la clientèle, ainsi qu'aux autorités compétentes, en particulier la CRF. L'accès à ces informations est important, notamment pour les autorités chargées des enquêtes et des poursuites, afin de retracer les activités criminelles.

Recommandations

- Lorsqu'elles établissent des relations commerciales avec des clients ou effectuent des transactions pour des clients occasionnels, les EO, dans leur rôle de responsables du traitement, devraient communiquer à la personne concernée *inter alia* des informations concernant entre autres la base juridique et les finalités du traitement envisagé, les catégories de données que l'IF et l'EPNFD (ou d'autres tiers) traiteront, les destinataires ou les catégories de destinataires des données à caractère personnel, le cas échéant ; les moyens d'exercer les droits énoncés à l'article 9 de la Convention et les restrictions éventuelles, en cas de besoin, ainsi que toute information supplémentaire nécessaire pour assurer un traitement ~~équitable~~ loyal et transparent des données à caractère personnel et l'utilisation qui en est faite, d'une manière compréhensible et conviviale.

- Conformément à l'article 14 de la Convention, ~~L~~les EO devraient procéder à l'examen de l'impact potentiel des transferts prévus et/ou d'autres activités de traitement de données, préalablement à ce traitement, sur les droits et libertés fondamentales des personnes concernées, et concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales. Si aucune exception selon l'article 14.4 ne s'applique, c~~C~~ette évaluation du pays ou de l'organisation de destination devrait viser à garantir que le niveau de protection offert par la convention est garanti par les destinataires et que la personne concernée est en mesure de défendre ses intérêts en cas de non-respect. Les EO devraient également tenir compte de l'opposabilité des droits des personnes concernées et de la mise en place d'un recours administratif et juridictionnel effectif pour les personnes concernées dont les données à caractère personnel sont transférées.

(…)

- L'accès aux données ~~personnelles~~ à caractère personnel des registres centraux des bénéficiaires effectifs ne devrait pas être accordé librement, car il peut constituer une ingérence grave dans les droits de l'homme, y compris le droit à la vie privée et à la protection des données à caractère personnel et ne devrait être autorisé que dans les situations ou dans la mesure prévue par la loi, et dans le respect des réglementations en matière de protection des données, notamment pour ce qui est des principes de nécessité, de proportionnalité et de limitation. L'accès aux données non accessibles au public est géré avec soin en tenant compte de la législation nationale, des droits et des intérêts concernés.

Commented [A67]: CH : Il conviendrait d'éviter d'utiliser encore une autre formulation pour définir ce que l'anglais entend par LEA.

Commented [A68]: CH : reprise de la même expression qu'auparavant en page 6.

3.4 Le principe de la minimisation des données

(…)

Dans le contexte de la LBC/FT

- Les lois sur la LBC/FT peuvent prévoir différents niveaux de traitement des données ~~personnelles~~ à caractère personnel (données de CDD) par les EO, notamment une ~~diligence raisonnable~~vigilance simplifiée, normale et renforcée à l'égard des clients. En principe, le renforcement de la ~~diligence raisonnable~~vigilance exige le traitement d'une plus grande quantité de données à caractère personnel, y compris la vérification de ces données à partir de diverses sources accessibles à l'EO. Une ~~diligence~~ vigilance renforcée peut être exigée en fonction des risques que posent certains types de clients (par exemple, les personnes politiquement exposées (PPE[67]) ou lorsque les risques liés au BC/FT sont plus grands) ou certains types de services ou de transferts (par exemple, les transferts de capitaux vers des pays à haut risque), voire des clients particuliers dans des situations où des risques ou des transactions suspectes ont été détectés. Les lois sur la LBC/FT peuvent prévoir différentes périodes de conservation des données pour différents types de données à caractère personnel.

- En pratique, il s'avère que dans de nombreux cas, les entités du secteur privé manquent d'orientations claires et spécifiques nécessaires à la collecte des données ~~personnelles~~ à caractère personnel de leurs clients dans le cadre de leurs obligations de LBC/FT. Lorsqu'elles collectent, par exemple, des jeux de données spécifiques dans le cadre des obligations de CDD, les EO ~~normes de connaissance de leur clientèle (« Know Your Customer » KYC),~~ ~~elles~~ doivent observer tant des obligations juridiques de protection des données et des obligations LBC/FT et peuvent rencontrer des difficultés à ~~comprends~~ comprendre comment atteindre ces deux buts de manière consistante et compatible, ~~–~~en particulier eu égard au principe de minimisation des données. Par conséquent, par crainte de s'exposer à des risques de réputation et autres causés par (i) le traitement involontaire de produits du crime ou (ii) la possibilité de faire l'objet d'amendes administratives ou de mesures de la part des autorités de contrôle ~~d'omettre une menace ou de se voir infliger une amende par les autorités de surveillance financière~~, les entités du secteur privé peuvent finir par partager « au cas où » un plus grand volume de données.~~–~~ En ce sens, la mise en œuvre correcte d'une approche fondée sur les risques du point de vue de la LBC/FT permettrait également de s'aligner sur l'exigence de proportionnalité envisagée dans les exigences en matière de protection des données. ~~Inversement, en raison de la position d'information limitée de chaque EO, la minimisation des données peut être favorisée par un partage d'informations plus ciblé et rationalisé entre les EO afin d'éviter la collecte inutile d'informations par chaque EO individuelle dans tous les cas.~~ L'application efficace d'une approche fondée sur les risques nécessite des orientations et une formation claires et pratiques de la part des autorités de ~~surveillance~~contrôle, des investissements dans les ressources et l'expertise par les EO, ainsi qu'une application et une ~~application~~ mise en œuvre proportionnées des lois nationales en matière de LBC/FT.

~~[65] La Recommandation 23 du GAFI indique que Les avocats, notaires, autres juristes indépendants et comptables agissant en qualité de juristes indépendants ne sont pas tenus de signaler les opérations suspectes si les informations pertinentes ont été obtenues dans des circonstances où elles sont soumises au secret professionnel ou aux règles c communications entre un avocat et son client.les obligations de déclaration de certaines EPNFD ne s'appliquent pas si les informations pertinentes ont été obtenues dans des circonstances où elles sont soumises au secret professionnel ou au secret professionnel de l'avocat.~~

[66] GAFI, recommandation 23.

[67] Selon les normes du GAFI, les personnes politiquement exposées (PPE) sont classées comme suit: (i) PPE étrangères, (ii) PPE nationales, et (iii) personnes qui ~~sont ou ont été chargées d'une fonction importante par~~exercent ou ont exercé d'importantes fonctions au sein de ou pour le compte d'une organisation internationale. Cela désigne les membres de la haute direction, c'est-à-dire les ~~administrateurs~~directeurs, les directeurs adjoints et les membres du conseil d'administration ou toutes les personnes exerçant des fonctions équivalentes.~~-~~ La définition des PPVE ne ~~vise~~couvre pas les personnes de rang ~~intermédiaire~~moyen ou ~~plus subalterne~~ inférieur ~~dans les~~relevant des catégories susmentionnées. Voir annexe 1 pour plus de détails.

Recommandations

(…)

- Dans le cadre du PPP, le partage de données de transaction impliquant le traitement d'une grande quantité de données, le traitement devrait être effectué, le cas échéant, avec des données anonymisées ou pseudonymisées. L'identification d'une personne relativement à une transaction ne ~~devraient~~ devrait être limitée que lorsque le résultat du traitement basé sur des conditions liées à un soupçon raisonnable/une cause probable révèle des schémas, modus operandi ou des activités concrètes qui pourraient nécessiter la déclaration de l'opération à la CRF comme étant suspecte, ou lorsqu'il est nécessaire d'identifier des liens avec un terroriste identifié. Par exemple, lorsque le traitement des données est effectué pour identifier des tendances, des modèles et des typologies, il n'est pas nécessaire d'utiliser des données ~~personnelles~~à caractère personnel.

(…)

3.5 Le principe de l'exactitude des données

(…)

Dans le contexte de la LBC/FT[68]

- Les EO doivent s'assurer que les documents, données et informations obtenues dans l'exercice du devoir de vigilance restent à jour et pertinents. Ceci implique d'examiner les éléments existants et effectuer ~~des opérations de suivi récurrentes~~une surveillance continue, sur une base régulière, pour les catégories de clients présentant des risques plus élevés[69].

- Les EO peuvent faire appel à des prestataires externes à diverses fins (par exemple, vérification des sanctions, identification des PPE, des membres de la famille et des proches), qui, s'ils sont fournis avec des données ~~personnelles~~à caractère personnel inexactes ou obsolètes, peuvent donner des résultats inexacts en termes de CDD ou d'autres fins de LBC/FT (par exemple, le reporting),~~ce qui peut affecter l'exactitude des données qu'ils traitent dans des finalités de CDD~~. Elles peuvent recourir à des systèmes basés sur l'IA pour surveiller les transactions afin d'identifier des modèles et des tendances suspects, et générer des alertes qui, si elles n'utilisent pas des données ~~précises~~ exactes et ne sont pas correctement calibrées, risquent de ~~devenir des donnes faussement positives/négatives~~donner lieu à des faux positifs/négatifs et/ou être trop nombreuses et ne peuvent pas être traitées de manière légale. Bien que les Recommandations du GAFI fassent référence à l'exigence de garantir l'exactitude des informations, les implications concrètes de la vérification de l'exactitude de toutes les données à caractère personnel restent à déterminer, étant donné que l'obligation susmentionnée de tenir à jour des données et informations de CDD s'applique même aux données collectées auprès de fournisseurs externes.

- Les EO sont autorisées à ~~s'appuyer sur~~recourir à des tiers pour l'exécution de certains éléments du processus de vigilance à l'égard de la clientèle[70]. Le fait que les informations de CDD aient été collectées et traitées par une tierce partie sur laquelle l'EO n'a pas de contrôle peut entraîner des inexactitudes dans les informations collectées pour le processus de CDD. Cependant, les normes du GAFI

Commented [A69]: CH : est-ce le bon terme ? Ne vise-t-on pas ici la déclaration [des opérations suspectes] ?

Commented [A70]: CH : Remarque générale concernant la la traduction des recommandations du GAFI : « Il y a une version française qui tient compte des modifications jusqu'à mars 2022. Elle est accessible par le lien suivant Les Recommandations du GAFI (fatf-gafi.org). La version de mars 2022 tient compte de la dernière révision de la R24 et de sa note interprétative (transparence des personnes morales). Il y a par contre eu une nouvelle révision de la R25 et de sa note interprétative (transparence des constructions juridiques [trusts] en février 2023 qui n'est actuellement disponible qu'en anglais. »

[68] Recommandations pertinentes du GAFI : 6, 7, 10, 17, 24, 37, 40.
[69] GAFI, recommandation 10.
[70] GAFI, recommandation 17.

indiquent clairement que la responsabilité de l'accomplissement de l'obligation de CDD incombe à l'EO qui ~~se fie à la tierce partie~~recourt au tiers. Ceci est cohérent avec le rôle du responsable du traitement des EO, tel que défini dans la Convention 108+. Par conséquent et sur la base des ~~-~~recommandations du GAFI impliquant de vérifier toutes les données ~~personnelles~~à caractère personnel, l'obligation susmentionnée de maintenir à jour les données et informations de CDD s'applique même aux situations où l'on ~~se fie à des tiers~~recourt à des tiers.

- Les pays sont tenus de mettre en place des mécanismes pour s'assurer que les informations sur les bénéficiaires effectifs sont obtenues par ~~l'entreprise~~ la société ou autrement disponibles en temps opportun[71]. Dans la pratique, les lois sur la LBC/FT exigent généralement la même chose pour les autres entités juridiques inscrites dans les registres des bénéficiaires effectifs. En outre, les données de base (c'est-à-dire le nom de la société, la preuve de sa constitution, sa forme et son statut juridique, l'adresse du siège social, les ~~pouvoirs réglementaires de base~~éléments principaux régissant le fonctionnement de la société et la liste des ~~administrateurs~~membres du conseil d'administration) doivent être accessibles au public dans un registre des sociétés, et envisage également la possibilité d'exiger des sociétés ou des registres de sociétés qu'ils obtiennent et détiennent des informations sur les bénéficiaires effectifs[72].

Commented [A71]: CH : A quoi se réfère « et envisage » ? Le sujet de la phrase est « les données de base ». La phrase doit être revue, aussi en anglais où elle ne fait également guère de sens.

(…)

Recommandations

(…)

- Si les EO utilisent des systèmes automatisés, y compris lorsqu'il est géré par un traitement algorithmique ou l'intelligence artificielle pour le profilage du risque des clients ou des bénéficiaires effectifs, des mesures appropriées doivent être prises pour corriger les facteurs d'inexactitude des données et limiter les risques d'erreurs inhérents au profilage. La réévaluation périodique (ou basée sur un élément déclencheur) doit également inclure une réévaluation des données et des déductions statistiques, y compris pour l'élimination des biais potentiels utilisés pour le profilage du risque, afin de déterminer si elles sont toujours exactes et pertinentes. En ce qui concerne le traitement des données à caractère personnel par les nouvelles techniques et technologies de traitement, les EO sont invitées à suivre la Recommandation CM/Rec(2021)8 du Comité des Ministres aux Etats membres sur la protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnel dans le contexte du profilage[73] ~~et~~ ainsi que les Lignes directrices sur l'intelligence artificielle et la protection des données[74].

- Si les EO font appel à des fournisseurs de bases de données externes pour mettre en œuvre les obligations de vigilance à l'égard des bénéficiaires effectifs de leurs clients (par exemple, la vérification de l'identité du client et du bénéficiaire effectif, l'identification des relations potentielles avec les PPE, ainsi que des membres de la famille et des proches de la PPE), elles devraient vérifier que les données à caractère personnel utilisées sont exactes et à jour et ~~de~~ procéder à une évaluation périodique de l'exactitude des données mises à disposition par le fournisseur.

(…)

[71] GAFI recommandation 24.
[72] Idem.
[73] Result details (coe.int)
[74] Lignes-directrices-sur-l-intelligence-artificielle-et-la-protection des données

- L'entité obligée qui reçoit des données spécifiques sur les clients, les bénéficiaires effectifs et les transactions dans des buts spécifiques, est considérée comme le responsable du traitement et doit donc être tenue responsable ~~de leur~~du traitement des données comme de leur exactitude, même dans le cas où elle fait appel à des tiers pour la collecte et le traitement. Ces tiers peuvent être considérés comme des responsables du traitement au sens de la Convention 108+.

- Conformément à l'article 10 de la Convention 108+, les EO doivent mettent en œuvre des mesures visant à prévenir ou minimiser le risque ~~d'ingérence~~ d'atteinte ~~dans les~~aux droits et libertés fondamentales des clients.

- Les EO sont également invitées à adopter une approche de confidentialité dès la conception, lors de la mise en place du système pour le traitement des données ~~personnelles~~ à caractère personnel y compris durant la phase d'intégration et d'automatisation de cette vérification.

Commented [A72]: CH : cf. version anglaise

(…)

3.6 Le principe de la limitation de la conservation

Principe général

- L'article 5, paragraphe 4, point *e)* de la Convention 108 modernisée exige que les données à caractère personnel soient effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont été collectées. Il existe toutefois des exceptions à ce principe à condition (i) qu'elles soient prévues par la loi, (ii) qu'elles respectent l'essence des droits et libertés ~~fondamentaux~~ fondamentales et (iii) qu'elles soient nécessaires et proportionnées à la poursuite d'un nombre limité d'objectifs légitimes (article 11). Il s'agit, entre autres, de la ~~préservation~~ protection de la sécurité nationale, des enquêtes sur les infractions pénales et leur poursuite, de la protection de la personne concernée et de la protection des droits et des libertés fondamentales d'autrui.

Dans le contexte de la LBC/FT[75]

Commented [A73]: CH : il conviendrait d'ajouter une référence à la R25 également dans la note de bas de page de la version anglaise.

- Des exigences claires sont définies en matière de durée de conservation des informations relatives à la CDD, des dossiers de comptes, de la correspondance commerciale et des résultats de toute analyse entreprise (au moins 5 ans après la fin de la relation d'affaires ou après la transaction occasionnelle) et des dossiers sur les transactions internes ou internationales (au moins 5 ans après la fin de la transaction)[76].

- Le traitement des données est nécessaire pour éviter l'utilisation de personnes morales et de ~~dispositions~~constructions juridiques à des fins de BC ou de FT, en assurant des informations satisfaisantes, exactes et à jour sur les bénéficiaires effectifs et sur le contrôle des personnes morales et constructions juridiques[77]. En cas de cessation d'existence (dissolution ou autre) d'une société, toutes les parties prenantes et la société elle-même (ou ses dirigeants, liquidateurs ou autres personnes impliquées dans sa dissolution) sont tenues de conserver les informations et pièces mentionnées pendant au moins cinq ans après la date à laquelle la société est dissoute ou cesse d'exister, ou pendant au moins cinq ans après la date à laquelle la société cesse d'être cliente de l'intermédiaire professionnel ou de l'institution financière.

Commented [A74]: CH : il convient d'ajouter les constructions juridiques dans les versions anglaises et françaises ainsi qu'une référence à la R25 dans la note de bas de page.

[75] Recommandations pertinentes du GAFI : 2, 11, 24, 25, 29, 40.
[76] GAFI, recommandation 11.
[77] GAFI, recommandations 24 et 25.

(…)

Recommandations

(…)

- La coopération au niveau national entre les autorités chargées de la protection des données et les autres autorités de ~~surveillance~~contrôle[78] devrait être facilitée afin que des orientations spécifiques puissent être élaborées pour assurer un équilibre entre les obligations légales applicables, tant du point de vue de la LBC/FT que de la protection des données, y compris sur la question de la conservation des données. Ce type de coopération pourrait être renforcé, par exemple: (i) en organisant des réunions conjointes entre les autorités chargées de la protection des données ~~de surveillance~~ et d'autres autorités de contrôle sur la LBC/FT et la protection des données, (ii) en publiant des lignes directrices communes sur des aspects liés, tels que la technologie nécessaire (par exemple, le niveau de cryptage ou le calcul multipartite), les ensembles de données nécessaires au traitement pour atteindre les objectifs de LBC/FT, ou comment les personnes concernées devraient pouvoir exercer leurs droits vis-à-vis des responsables du traitement (iii) organiser des consultations avec les autorités chargées de la protection des données ~~de surveillance~~[79] dans le cadre de l'élaboration de normes, de lignes directrices et de recommandations, ainsi que la possibilité d'un dialogue informel avec d'autres autorités de contrôle; iv) Les autorités chargées de la protection des données ~~de surveillance~~ pourraient également être invitées à participer à des réunions informelles sur les PPP, auxquelles des entités du secteur privé ont également la possibilité d'y assister en plus des autorités compétentes; v) associer les autorités chargées de la protection des données ~~de surveillance~~ à l'examen des différents documents d'orientation expliquant comment les institutions financières/EPNFD devraient se conformer à chacune de leurs obligations en matière de LBC/FT, afin de s'assurer que ces documents fournissent suffisamment de détails et d'orientations sur les exigences en matière de ~~DPP~~protection des données et de la vie privée et sur la manière dont les OE peuvent satisfaire aux deux ensembles d'exigences. Cela pourrait également aider à cerner les domaines où il existe une incompatibilité des politiques – qui pourrait ensuite être traitée par un autre forum (p. ex., par voie législative).

Commented [A75]: CH : La convention 108+ parle d'autorités de contrôle à l'article 15 (en anglais supervisory authorities). La même expression (autorités de contrôle) est employée pour désigner les autorités de « surveillance » au niveau de la LBC/FT. Cela crée une certaine confusion dans ce passage ainsi que dans la note de bas de page. Il serait donc mieux de faire comme dans la version anglaise et de parler des autorités chargées de la protection des données, plutôt que des autorités de surveillance ou de contrôle.

3.7 Le principe de la sécurité des données

Principe général

- La sécurité et la confidentialité des données à caractère personnel sont essentielles pour éviter que la personne concernée ne pâtisse d'événements comme l'accès, l'utilisation, la modification, la divulgation, la perte, la destruction ou l'endommagement des données, que ces événements soient illicites, accidentels ou non autorisés (article 7 de la Convention). Le responsable du traitement et, le cas échéant, le sous-traitant, doivent prendre des mesures de sécurité particulières qui tiennent compte de la spécificité des opérations et des méthodes et techniques les

[78] Ceci nonobstant le fait que la législation sur la protection des données mettant en œuvre la Convention, en particulier l'article 15, prévoit les tâches et les pouvoirs des autorités de ~~surveillance~~contrôle. Toute recommandation concernant la coopération entre les autorités de ~~surveillance~~contrôle en matière de protection des données et d'autres autorités de contrôle (autorités de LBC/FT) devrait être conforme aux tâches et pouvoirs des autorités de ~~surveillance~~contrôle, et en particulier au rôle de surveillance indépendante des autorités de ~~surveillance~~ contrôle.

[79] Les autorités chargées de la protection des données ~~de surveillance~~ sont également régulièrement consultées sur les propositions législatives, y compris dans le cadre d'une consultation publique. La possibilité de consultation est également utilisée au niveau de l'UE: lettres du comité européen de la protection des données aux institutions européennes sur la protection des données à caractère personnel dans les propositions législatives de LBC-FT | Comité européen de la protection des données (europa.eu).

plus avancées en matière de sécurité des données. La pertinence des mesures de sécurité doit être déterminée au cas par cas et ~~revu~~ revue régulièrement.

- La «pseudonymisation» est un traitement de données à caractère personnel qui permet qu'elles ne puissent plus être attribuées à une personne concernée précise sans qu'il soit nécessaire d'avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles garantissant que les données ~~personnelles~~ à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable; Les mesures de pseudonymisation, qui ne dispensent pas de l'application des principes pertinents de protection des données, peuvent réduire les risques pour les personnes concernées.[80]

(…)

Dans le contexte de la LBC/FT[81]

(…)

- Garantir la confidentialité des ~~STRs~~ DOS est essentiel à l'efficacité des systèmes de ~~rapport~~déclaration des soupçons, en évitant que la personne visée de même que des tiers ne soient prévenus, car cela pourrait compromettre la collecte d'informations et porter atteinte aux ~~les~~ efforts d'enquête, y compris ~~et~~ permettre ~~la dissémination d'~~ le déplacement des avoirs. Les règles de confidentialité des ~~STR~~ DOS sont aussi importantes pour protéger la réputation d'une personne qui ~~y serait sujette~~ en ferait l'objet, ainsi que la sécurité de ~~l'enquêteur~~ la personne qui a effectué la déclaration. A un niveau plus opérationnel, des exigences sont déjà en place pour que les CRF protègent l'information, en particulier (i) en mettant en place des règles sur la sécurité et la confidentialité des informations, y compris des procédures ~~de gestion~~pour leur traitement, ~~de conservation~~leur stockage, ~~de diffusion~~leur dissémination, ~~et de~~leur protection et ~~sur l'accès à cette information~~leur consultation, (ii) en veillant à ce que le personnel ~~ait un niveau de vérification~~dispose des autorisations d'accès nécessaires et ~~de compréhension~~comprenne ~~de~~ ses responsabilités lorsqu'il traite et ~~diffuse~~ dissémine des informations sensibles et confidentielles et (iii) en veillant à limiter l'accès ~~aux locaux et aux systèmes, y compris les technologies de l'information~~à ses installations et ses informations, y compris ses systèmes informatiques[82]. Outre le GAFI, les Principes d'Egmont stipulent aussi des mesures de sécurité applicables aux échanges d'information. Par ailleurs, des exigences sont prévues pour l'utilisation de canaux sécurisés pour l'échange d'informations applicables aux autorités compétentes comme les ~~cellules~~ autorités d'investigation[83].

- Il est possible que la législation sur la protection des données applicable~~s~~ dans les États parties prévoie des exigences détaillées concernant la sécurité des données, lesquelles peuvent être applicables aux EO en tant que responsables du traitement. Parallèlement, la LBC/FT ou d'autres législations nationales spécifiques peuvent également prévoir des exigences supplémentaires pour garantir la sécurité des données et des informations portées à la connaissance des agents publics des autorités compétentes. Les agents publics peuvent avoir une responsabilité disciplinaire, civile, administrative et pénale en cas de manquement à l'obligation de garantir la sécurité des informations qui sont liées à leurs activités constituant un secret officiel, bancaire, fiscal, commercial ou de communication.

Commented [A76]: CH : il conviendrait d'ajouter une référence à la recommandation 21 du GAFI dans la note de bas de page.

[8] Lignes directrices du Conseil de l'Europe sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des méga données (2017), voir : https://rm.coe.int/16806ebe7a
[81] Recommandations pertinentes du GAFI : 2, 21, 29, 40.
[82] GAFI, recommandation 29.
[83] GAFI, recommandation 40.

Recommandations

- Des exigences spécifiques devraient être imposées aux EO pour qu'elles appliquent des mesures de sécurité strictes et des plus récentes afin de garantir la protection des données à caractère personnel, en particulier dans le cas de données sensibles au sens de l'article 6 de la Convention 108+ (par exemple sur les PPE, qui pourraient révéler des affiliations politiques ou l'orientation sexuelle dans le cas, par exemple, d'un partenariat entre personnes de même sexe), sauf si le cadre applicable en matière de protection des données prévoit déjà de telles exigences directement applicables et donc contraignantes pour les EO en tant que responsables du traitement.

Commented [A77]: CH : cf. version anglaise

(…)

4. Types de données faisant l'objet d'un traitement de données à caractère personnel dans le cadre des obligations en matière de LBC/FT

Principe général

- ~~Tout type d'information peut être une donnée à caractère personnel si elle se rapporte à une personne identifiée ou identifiable, ce qui peut être une information relative à la vie privée d'une personne, ce qui inclut également les activités professionnelles, ainsi que des informations publiques sur la vie d'une personne ((article 2 a) de la Convention 108+).~~Comme mentionné ci-dessus, toutes les informations peuvent être des données ~~personnelles~~à caractère personnel à condition qu'elles ~~permettent~~identifient ou permettent l'identification d'une personne physique. L'identification n'a pas besoin d'être directe, les informations qui pourraient éventuellement conduire à l'identification d'une personne, ~~avec~~ associées à d'autres informations qui ne sont ~~,~~ peut-être ~~seulement des informations~~ accessibles qu'à distance, constitueraient également des données ~~personnelles~~à caractère personnel.

  Parallèlement, il existe ~~également~~ des catégories particulières de données ~~personnelles~~ à caractère personnel définies à l'article 6 de la Convention 108+ qui exigent que des garanties appropriées soient consacrées par la loi, complétant celles de la Convention. Ces données sont : ~~telles que~~ les données génétiques ; les données à caractère personnel concernant des infractions, des procédures ~~pénales~~ et des condamnations pénales et des mesures de ~~sécurité~~ sûreté connexes ; les données biométriques identifiant une personne de façon unique ; les données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle, dont le traitement est, par nature, susceptible de présenter un risque plus élevé pour les personnes concernées et doit donc faire l'objet d'une protection accrue. Cela inclut les données dont ces informations ne peuvent être que dérivées ou déduites. Ces données sont soumises à des garanties supplémentaires complétant celles déjà en place pour les « ~~catégories normales de~~ données ~~personnelles~~à caractère personnel en général» et ne peuvent être traitées légalement que dans un nombre limité de conditions ~~(article 6 de la Convention 108+)~~.

Dans le contexte de la LBC/FT[84]

- Afin d'atténuer les risques de ~~L~~BC/FT, le secteur privé est tenu de prendre des mesures visant la collecte, le traitement et le partage sécurisé des données pertinentes avec les autorités compétentes (par exemple, les autorités de ~~surveillance~~contrôle et les LEA, au niveau national et parfois international, généralement par l'intermédiaire de leurs CRF nationales) et au sein des groupes financiers à des fins de LBC/FT pour la prévention, la détection et le signalement des clients et des opérations qui suscitent

Commented [A78]: CH : Il faudrait s'en tenir à la terminologie employée en début du document plutôt que d'employer cette abréviation anglaise.

[84] Recommandations pertinents du GAFI : 1, 10, 11, 18, 20, 21.

un soupçon de BC, d'infraction sous-jacente associée et de FT, ~~notamment en collectant et en traitant les données pertinentes et en les partageant de façon sécurisée avec les autorités compétentes (superviseurs et services répressifs par exemple, au niveau national et parfois international généralement par l'intermédiaire de leurs CRF nationales) et au sein des groupes financiers à des fins de LBC/FT~~.

(…)

- Connaître ses clients et appliquer à leurs comptes et à leurs activités un suivi approprié à des fins de LBC/FT[85], en prenant des mesures de vigilance à l'égard de la clientèle pour identifier chaque client et vérifier son identité au moment de l'établissement des relations d'affaires, et en ~~maintenant des mesures de~~exerçant une vigilance constante pendant toute la durée de ces relations ;

(…)

- Être capable de détecter et de signaler les ~~transactions~~ opérations suspectes[86] et de veiller à ce que les clients ignorent qu'une DOS ou une information s'y rapportant est communiquée aux autorités[87]. Il convient également de reconnaître que des catégories particulières de données, notamment celles qui concernent les ~~suivant d'autres cadres de prévention des délits, sur la base d'autres obligations légales, de~~les contributions à des organisations idéologiques / politiques, ~~de~~ les paiements d'amendes, etc., ~~toutes les catégories spéciales de données~~ sont traitées indépendamment de tout contrôle supplémentaire en matière de LBC/FT découlant d'obligations juridiques énoncées dans d'autres cadres internationaux de prévention de la criminalité.

- Les objectifs de LBC/FT~~C~~ peuvent conduire au traitement de catégories ~~spécialesparticulières~~ de données qui méritent une protection renforcée conformément à l'article 9 de 108+, mais A~~a~~ctuellement, les données sensibles sont rarement demandées à des fins de LBC/FT. Par exemple, dans les cas où les clients peuvent avoir à s'identifier comme faisant partie d'une relation homosexuelle, ~~l'OE~~ l'EO doit seulement savoir que le client correspond à la définition d'un membre de la famille ou d'un proche étroitement associé d'une ~~PPV~~PPE, sans nécessairement avoir besoin de connaître la nature de la relation.

(…)

Recommandations

(…)

- Les données ~~personnelles~~ à caractère personnel relatives aux infractions, aux procédures et aux condamnations pénales, ainsi que les mesures de ~~sécurité~~ sûreté qui s'y rapportent, font partie des catégories ~~spéciales~~ particulières de données à caractère personnel susmentionnées qui sont également pertinentes pour la lutte contre le blanchiment de capitaux et le financement du terrorisme. Le traitement de ces données ne peut être effectué que s'il est spécifiquement autorisé par la loi et si des garanties appropriées sont en place (par exemple, obligation de secret professionnel, mesures faisant suite à une évaluation de l'impact sur la vie privée, mesure de sécurité organisationnelle ou technique particulière et qualifiée telle que le cryptage et la journalisation des données).[88]

- Les registres contenant des informations sur les condamnations pénales ~~peuvent~~ devraient être limités aux ~~traitement et à l'utilisation par les~~ autorités compétentes, ou au traitement sous le contrôle de ces autorités. Des lignes directrices internes

[85] GAFI, recommandation 10.
[86] GAFI, recommandation 20.
[87] GAFI, recommandation 21.
[88] Voir le Rapport explicatif de la Convention 108+, paragraphe 56.

devraient être élaborées pour permettre d'évaluer au cas par cas si la collecte et/ou le transfert de données sensibles (notamment en ce qui concerne la religion et d'autres données sensibles) est nécessaire et proportionnée à l'objectif poursuivi, compte tenu des risques possibles pour la vie et l'intégrité des personnes concernées en cas d'incident sur la sécurité des données, y compris une violation des données.

- Il faudrait des lignes directrices, édictées par les autorités de ~~surveillance~~contrôle, pour le traitement de catégories particulières de données à caractère personnel, y compris sur les mesures appropriées et complémentaires visant à protéger les droits et libertés des personnes concernées, et de prévoir que les décisions de l'EO et des autorités compétentes ne soient pas fondées uniquement sur ces catégories de données à caractère personnel.

- Toutes les entités impliquées dans la LBC/FT, notamment les entités privées, les CRF et les services répressifs, doivent assurer la formation de leur personnel, en ce qui concerne par exemple le traitement des catégories ~~spéciales~~ particulières de données, par exemple en ce qui concerne la mesure dans laquelle le traitement de ces données est autorisé par la loi.

(…)

5. Droits des personnes concernées, exceptions et restrictions dans le contexte de la LBC/FT

Principe général

- Les personnes concernées ont de nombreux droits, détaillés dans l'article 9 de la Convention :

  - le droit de ne pas être soumises à une décision les affectant de manière significative qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que leur point de vue soit pris en compte ;~~ le droit :~~

  - le droit d'obtenir, à leur demande, à intervalle raisonnable et sans délai ou frais excessifs, la confirmation d'un traitement de données les concernant, la communication intelligible des données traitées, et toute information disponible sur leur origine, la durée de leur conservation ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements, conformément à l'article 8, paragraphe 1 ;

  - le droit d'obtenir, à leur demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement leur sont appliqués ;

  - le droit de s'opposer à tout moment, pour des raisons tenant à leur situation, à ce que des données à caractère personnel les concernant fassent l'objet d'un traitement, à moins que le responsable du traitement ne démontre des motifs légitimes justifiant le traitement qui prévalent sur les intérêts ou les droits et libertés fondamentales des personnes concernées ;

  - le droit d'obtenir, à leur demande, sans frais et sans délai excessifs, la rectification de ces données ou, le cas échéant, leur effacement lorsqu'elles sont ou ont été traitées en violation des dispositions de la présente Convention ;

- le droit de disposer d'un recours, conformément à l'article 12, lorsque leurs droits prévus par la présente Convention ont été violés ;

- le droit de bénéficier, quelle que soit leur nationalité ou leur résidence, de l'assistance d'une autorité de contrôle au sens de l'article 15 pour l'exercice de leurs droits prévus par la présente Convention.

- Les conditions d'éventuelles restrictions de ces droits sont énoncées à l'article 11 de la Convention ; elles doivent être prévues par la loi, respecter le contenu essentiel des libertés et des droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique. Les restrictions au droit d'accès ne devraient être levées dès que l'accès ne compromet plus les enquêtes.

- Les exceptions ne doivent être établies qu'aux fins énumérées à l'article 11 qui comprennent notamment la protection de la sécurité nationale, de la défense, de la sûreté publique et des les intérêts économiques et financiers importants de l'État, et ce uniquement en relation avec des droits ou obligations spécifiques énoncés dans l'article.

Dans le contexte de la LBC/FT[89]

- Certains des droits énoncés dans la Convention peuvent être restreints à des fins de LBC/FT. En général, les restrictions fondées sur les lois relatives à la LBC/FT reposent sur l'intérêt public général (c'est-à-dire l'intégrité du système financier ; la prévention, les enquêtes et les poursuites relatives à des infractions pénales et l'exécution de sanctions pénales). Les droits de la personne concernée sont restreints, par exemple dans une situation où l'EO signale une transaction opération suspecte à la CRF. Les lois relatives à la LBC/FT exigent que la déclaration de soupçon ne soit pas divulguée à la personne concernée et permettent ainsi de restreindre son accès aux données personnelles à caractère personnel relatives à cette déclaration. D'autres restrictions peuvent être imposées en ce qui concerne le traitement des déclarations de soupçon par la CRF. Dans le même temps, il n'y a généralement aucune raison de restreindre l'accès aux données relatives à la vigilance à l'égard de la clientèle et les EO sont plutôt invitées à informer les clients que leurs données à caractère personnel peuvent être utilisées à des fins de LBC/FT, y compris lors d'analyses ultérieures.

Recommandations

- Des mesures devraient être mises en place par les responsables du traitement pour faciliter l'exercice de ces droits par la personne concernée, en principe gratuitement. En cas de prise de décision automatisée, et si aucune exception ne s'applique, les informations relatives à la décision doivent être disponibles sur demande de la personne concernée. Un autre exemple pourrait concerner Il e droit de ne pas être soumis uniquement à une prise de décision automatisée devrait également s'appliquer même si , ce qui serait pertinent lorsque l'IA est utilisée également pour analyser les données de transaction et pour éclairer une décisiondécider si une transaction est suspecte ou non et devrait être transmise aux LEAà la CRF. Des règles et des instructions claires devraient être fournies conformément à l'article 11 sur la question de savoir si et quand les personnes concernées peuvent exercer leur droit, ou si une exception s'applique et comment l'interdiction dela règle de

Commented [A79]: CH : ne devrait pas être effacé (figure dans le texte anglais).

« divulgation »[90] peut être mise en œuvre conformément aux exigences en matière de protection des données.

Commented [A80]: CH : ad note de bas de page : il n'y a pas de Recommandation 21.2. Cela fait-il référence à la lettre (b) de la recommandation 21 ?

- En ce qui concerne le droit d'opposition, le rapport explicatif (paragraphe 80) indique que même lorsque ce droit est limité aux fins de ~~la recherche ou de la poursuite~~l'investigation ou de la répression d'infractions pénales, la personne concernée peut contester la ~~légalité~~ licéité du traitement. Toute restriction à l'exercice des droits justifiée par le risque de compromettre des enquêtes devrait être levée dès lors que ce risque n'existe plus.

- La mise en œuvre effective des droits des personnes concernées peut également nécessiter des actions supplémentaires afin que ces droits s'inscrivent dans une architecture de protection de la vie privée dès la conception, conformément à l'article 10 de la Convention 108+. Par exemple, le droit d'accès peut exiger que l'architecture permette à l'utilisateur d'identifier de manière transparente tous les ensembles de données contenus dans le système liés aux personnes concernées et de les choisir, et ce ~~que~~ sans divulguer les données d'autres personnes (séparation des données ou données structurées intégrées dans l'architecture).

6. Exceptions et restrictions (article 11)

Principe général

Seules des exceptions aux dispositions de l'article 5, paragraphe 4, de l'article 7, paragraphe 2, de l'article 8, paragraphe 1, et de l'article 9 de la Convention peuvent être faites, lorsqu'une telle exception est prévue par la loi, respecte l'essence des droits et libertés fondamentaux~~ux~~les et constitue une mesure nécessaire et proportionnée dans une société démocratique ~~pour~~.

Commented [A81]: CH : Selon le texte de l'art. 11 de la convention 108 +.

(…)

Dans le contexte de la LBC/FT

- Sur la base de cette exception, le régime de LBC/FT pourrait prévoir des situations dans lesquelles le client (la personne concernée) n'est pas informé du traitement, en particulier lorsque l'EO applique une vigilance ~~raisonnable accrue~~renforcée ou déclare des ~~transactions~~ opérations suspectes. Cela impliquerait une information préalable du client, ce qui contreviendrait aux interdictions de LBC/FT, en particulier aux exigences en matière de divulgation. De plus, le droit d'accès des clients devrait être garanti aux données traitées par les autorités compétentes, ~~y compris les CRF,~~ dans la mesure où, et aussi longtemps qu'une telle mesure constitue une mesure nécessaire et proportionnée dans une société démocratique. ~~est généralement restreint, mais lorsque les exceptions ne peuvent légalement plus être utilisées, tant que les raisons de cette restriction persistent. En dehors des délais et du champ d'application d'une exception licite, il convient de garantir pleinement les droits des personnes concernées~~.

Recommandation

(…)

[90] GAFI, recommandation 21.~~2~~(b).

7. Le rôle des autorités de protection des données et leur relation avec les autorités de la LBC/FT

(…)

Dans le contexte de la LBC/FT

Les activités qui sont nécessaires pour se conformer à la réglementation en matière de LBC/FT impliquent l'activité de différents acteurs parfois dans de multiples juridictions ainsi que le traitement de vastes volumes de données à caractère personnel. ~~Conformément à l'article 15 de la Convention, les autorités chargées de la protection des données devraient être compétentes en ce qui concerne le traitement effectué par différents responsables du traitement dans le domaine de la LBC/FT.~~ La Convention prévoit que les pouvoirs des autorités de contrôle, notamment en ce qui concerne les enquêtes, les interventions, l'autorisation, le blocage du transfert transfrontalier de données à caractère personnel, s'appliquent au traitement de données à des fins de LBC/FT. Bien qu'aucune restriction ne puisse être apportée à l'utilisation de ces pouvoirs lors du traitement des donnée dans le cadre du maintien de l'ordre (et d'autres objectifs généraux d'intérêt public), l'article 11.3 prévoit en ce qui concerne les activités de traitement à des fins de sécurité nationale et de défense, que certains de ces pouvoirs[91] peuvent être restreints (article 11, paragraphe 3), à condition que cette restriction soit prévue par la loi, respecte l'essence des libertés et droits fondamentaux et constitue une mesure nécessaire et proportionnée dans une société démocratique. Même dans ce dernier cas, la Convention exige que les activités de traitement à des fins de sécurité nationale et de défense fassent l'objet d'un contrôle et d'une supervision indépendants effectifs en vertu de la législation nationale de la Partie concernée.

Commented [A82]: CH : Le contenu de la note de bas de page a été supprimé, mais pas la note de bas de page en tant que telle.

Recommandations

- Les traitements pour la LBC/FT doivent faire l'objet d'une autorisation ex-ante et/ou d'un examen ~~ex-ante et/ou~~ ex-post effectif, ~~[~~cohérent~~]~~ et indépendant fondé sur le cadre juridique national conformément à l'Aarticle 11.3 de la Convention. ~~En outre,~~ Cela peut inclure le fait que les cadres juridiques nationaux ~~devraient~~ prévoi~~r~~ent un niveau spécifique d'habilitation de sécurité pour le personnel des autorités chargées de la protection des données désigné~~s~~ afin qu'il accède aux données traitées par les CRF relevant de la catégorie des services de renseignement.

- Les autorités de protection des données doivent coopérer avec les autres autorités nationales chargées de la LBC/FT, afin de mener des activités conjointes pour assurer la conformité avec les normes de protection des données dans le cadre de la répression du BC/FT.

- En général, la nécessité d'un dialogue et d'une coopération entre les autorités de protection des données et d'autres autorités ~~LBT/FR~~LBC/FT (éventuellement aux niveaux national et international) devrait être soulignée afin de développer des outils d'orientation efficaces tant pour le secteur public que privé et d'élaborer des modules de formation spécifiques.

- Dans le domaine de la LBC/FT, les autorités de protection des données devraient travailler avec ~~des~~ les autorités ~~LBT/FT~~ LBC/FT compétentes et les EO en vue de suggérer des outils et des modes opératoires efficaces en matière de conformité (qui

[91] ~~Demander des informations relatives au transfert international de données à caractère personnel, exiger du responsable du traitement qu'il démontre les conditions légales du transfert international et sa capacité d'intervention et le pouvoir d'enquête et d'intervention de l'autorité de contrôle, les fonctions relatives à l'autorisation/blocage du transfert international, le pouvoir de prendre des décisions réglementaires et des sanctions et de saisir le pouvoir judiciaire~~

pourraient, s'ils sont dûment mis en œuvre, contribuer aussi à une surveillance plus efficace) et de proposer des formations spécifiques.

8. Transferts internationaux de données dans le domaine de la LBC/FT

Principe général

(…)

- Les données à caractère personnel circulent librement entre les Parties à la Convention 108+. Des restrictions à la libre circulation transfrontière des données à caractère ~~personnelle~~ personnel sont prévues lorsque 1) il existe un risque réel et sérieux que la communication à une autre Partie entraîne le contournement des dispositions de la Convention, ou 2) lorsque des Parties sont liées par des règles de protection harmonisées partagées par des États appartenant à une organisation internationale régionale (article 14.1 de la Convention).

- Les transferts de données à caractère personnel à des pays tiers ou à des organisations internationales ne sont possibles que si un niveau approprié de protection peut être garanti, soit par la législation du pays ou de l'organisation internationale destinataire, soit par des garanties ad hoc ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables, adoptés par les personnes impliquées dans le transfert et le traitement ultérieur des données (article 14, paragraphes 2 et 3 de la Convention 108+).

(…)

Dans le contexte de la LBC/FT[92]

Commented [A83]: CH : Il conviendrait d'ajouter la R18 dans la liste des recommandations pertinentes dans la note de bas de page, et ce, aussi bien dans le français que l'anglais. Cf. remarque relative au dernier bullet point.

- Compte tenu de la nature multilatérale des mécanismes d'échanges interétatiques de données à caractère personnel à des fins de LBC/FT, la question du niveau de protection approprié se pose dans tous les cas où l'échange de telles données concerne un pays qui ne dispose pas d'un niveau (essentiellement) équivalent de protection des données à caractère personnel.

- Il y a dans les recommandations du GAFI ~~adressées aux autorités publiques~~ plusieurs exigences adressées aux autorités publiques en matière de sécurité des données, qui s'appliquent lorsque les données franchissent les frontières. La version révisée de la recommandation 2 exige des pays une coopération et une coordination entre les autorités de protection des données et de LBC/FT afin de veiller à ce que les principes, règles et considérations en matière de protection des données soient dûment intégrés dans les obligations en matière de LBC/FT.

- Le GAFI[93] demande aux autorités compétentes, indépendamment des voies et moyens de la coopération internationale, ~~de garder confidentielles~~d'assurer un degré de confidentialité approprié à ~~les~~ toute demande~~s~~ de coopération et ~~les~~ aux informations échangées, conformément aux obligations des deux parties en matière de protection des données et de respect de la vie privée. Les autorités compétentes sont tenues, au minimum, de protéger les informations échangées de la même façon qu'elles protègent les informations similaires reçues de sources nationales. Les autorités compétentes devraient avoir la possibilité de refuser de fournir des

[92] Recommandations pertinentes du GAFI : 2, 40.
[93] GAFI, recommandation 40.

informations si l'autorité compétente requérante n'est pas en mesure de les protéger efficacement.

- [Le partage d'informations sur un client entre EO appartenant au même groupe (données de vigilance à l'égard du client, indication que ce client a fait l'objet d'une déclaration d'opération suspecte, etc.) est généralement considéré comme moins délicat si des exigences et politiques claires précisent quelles informations peuvent être partagées et à quelles fins spécifiques, et si l'échange se produit entre EO situées dans le même pays (et donc soumises aux mêmes exigences). Cependant, il se peut que des EO appartenant au même groupe opèrent depuis différents pays, aux exigences variables (voir les considérations sur les flux transfrontières).]

Commented [A84]: CH : On est ici hors de la coopération internationale entre autorités. Dans ce contexte, ce n'est pas la R40 mais la R18 qui est pertinente.

Recommandations

(…)

- Les autorités de protection des données jouent un rôle important, conformément à l'article 15.2 b de la Convention 108 modernisée, pour garantir la licéité du traitement, même dans un contexte de flux transfrontalier de données, y compris, le cas échéant, en renvoyant les cas individuels de transferts transfrontaliers de données devant les tribunaux nationaux. Les autorités de protection des données doivent avoir le pouvoir, les ressources et les accords institutionnels nationaux et internationaux en place pour traiter ces questions conformément à l'article susmentionné et aux exceptions prévues à l'Aarticle 11. ~~Elles devraient également être autorisées à et, le cas échéant, renvoyer des cas individuels sur les transferts transfrontaliers de données aux tribunaux nationaux~~.

(…)

- Si une EO appartient à un groupe dont les établissements, tels que des succursales/filiales se trouvent dans différents pays, et si la législation nationale n'interdit pas les ~~échanges~~ transferts transfrontières de données, y compris pour des motifs de protection des données, de tels transferts reposeront sur des garanties standardisées ad hoc ou approuvées, ~~énoncées dans des instruments contraignants et opposables adoptés et mis en œuvre par les personnes impliquées dans le transfert des données et dans leur traitement ultérieur, à condition qu'un niveau de protection adéquat soit assuré pendant le transfert dans le traitement des données personnelles, et le niveau de protection adéquat ne doit pas être compromis par le transfert~~. Le transfert ne doit pas porter atteinte au niveau approprié de protection des données à caractère personnel.

- Les CRF des États parties devraient échanger des informations avec d'autres autorités compétentes et avec leurs homologues étrangers conformément aux exigences applicables et limiter les données à caractère personnel traitées à ce qui est directement pertinent pour fournir ou obtenir les informations demandées. En ce qui concerne les transferts de données à caractère personnel vers des États non parties à la Convention, les exigences prévues à l'article 14 de la Convention doivent être respectées. Des ~~autres~~ normes additionnelles ~~applicables à l'échange d'informations~~ pourraient s'appliquer à l'échange d'informations et préciser les exigences en matière de protection ou de sécurité des données[94], ~~telles que les~~

[94] ~~tellesTels~~ que les principes du Groupe Egmont.

~~principes du Groupe Egmont.~~[95] Il convient de noter que le deuxième protocole additionnel à la Convention de Budapest (STE No.185) et ses Protocoles pourrait donner des indications supplémentaires sur les garanties applicables en matière de transferts internationaux entre autorités et, dans une certaine mesure, entre autorités et parties privées.

(…)

- La coopération entre les autorités de protection des données et d'autres autorités LBC/FT compétentes doit être recommandée.

Annexe 1 ~~au chapitre I~~

(…)

- Données clients – Les normes du GAFI définissent des paramètres pour le partage d'informations uniquement dans le contexte d'un groupe financier[96]. En raison des exigences en matière de protection des données et de confidentialité, le partage de données en dehors d'un groupe financier est limité. Les ensembles de données CDD requis qui doivent être obtenus auprès d'une personne physique comprennent principalement des données ~~personnelles~~à caractère personnel, telles que: le nom complet, l'adresse résidentielle, le numéro de contact et les adresses électroniques, le lieu de naissance, la date de naissance, le sexe, la nationalité, ~~la race, l'origine ethnique,~~ le numéro d'identification délivré par le gouvernement et le numéro d'identification fiscale, la signature. Pour une personne morale, certaines données ~~personnelles~~ à caractère personnel sont également requises sur les administrateurs, les actionnaires, la haute direction et les bénéficiaires effectifs, qui sont généralement accessibles au public en raison de dispositions légales fondées sur l'intérêt public[97].

- Informations sur les bénéficiaires effectifs : d'après la définition du GAFI, le bénéficiaire effectif est toujours une ou plusieurs personnes physiques qui, en dernier lieu, possèdent ou contrôlent un client, une personne morale ou une construction juridique et/ou la personne physique pour le compte de laquelle une opération est effectuée. Dans ce contexte, les jeux de données comportent principalement l'identification du bénéficiaire effectif et ses coordonnées de contact (nom complet, nationalité(s), lieu et date de naissance détaillés, adresse du domicile, numéro d'identification national et type de document, numéro d'identification fiscale ou équivalent dans le pays de résidence) et des informations sur le patrimoine immobilier, l'origine du patrimoine et des fonds, l'activité professionnelle et le fait que le bénéficiaire effectif soit ou non une PPE. Les données d'identification pertinentes peuvent être obtenues à partir des registres publics ou auprès du client ou d'autres sources fiables. Pour être jugées ~~suffisantes~~satisfaisantes, les informations doivent permettre l'identification de la personne physique qui est bénéficiaire effectif et des moyens et mécanismes par lesquels son contrôle s'exerce. Pour être exactes, elles doivent être vérifiées à l'aide de sources/de l'obtention de documents, données ou informations fiables et indépendants, dans la mesure du nécessaire au regard du niveau de risque spécifique. Les informations doivent être actuelles, et mises à jour dans un délai raisonnable à chaque changement.

- Personnes politiquement exposées (PPE) – sont classées, selon les normes du GAFI, dans trois catégories principales, comme décrit ci-dessous. La définition des PP~~V~~E ne vise pas les personnes de rang ~~intermédiaire ou plus subalterne~~moyen ou inférieur relevant ~~dans l~~des catégories ~~précédentes~~suivantes.

  - Les PPE étrang~~è~~ères, qui sont des personnes physiques qui ~~sont ou ont été chargées de~~exercent ou ont exercé d'importantes fonctions publiques ~~importantes par~~dans un pays étranger, par exemple des chefs d'État ou de

Commented [A85]: CH : Puisqu'on mentionne les normes du GAFI, il conviendrait de reprendre la définition du glossaire du GAFI.

gouvernement, des ~~hauts responsables politiques~~politiciens de haut rang, ~~des hauts fonctionnaires, des fonctionnaires judiciaires ou militaires, des cadres supérieurs de sociétés d'État, des responsables importants~~ des hauts responsables au sein des pouvoirs publics, des magistrats et militaires de haut rang, des dirigeants d'entreprise publique et des hauts responsables de partis politiques.

- Les PPE nationa~~ux~~les, qui sont des personnes physiques qui exercent ou ont exercé d'importantes fonctions publiques dans le pays, par exemple, des chefs d'État et de gouvernement, des politiciens de haut rang, des hauts responsables au sein des pouvoirs publics, des magistrats et militaires de haut rang, des dirigeants d'entreprise publique et des hauts responsables de partis politiques.~~qui sont ou ont été chargées au niveau national de fonctions publiques importantes, par exemple des chefs d'État ou de gouvernement, des hauts responsables politiques, des hauts fonctionnaires, des fonctionnaires judiciaires ou militaires, des cadres supérieurs d'entreprises publiques, des responsables importants de partis politiques.~~

- Les personnes qui exercent ou ont exercé d'importantes fonctions au sein de ou pour le compte d'une organisation internationale désigne les membres de la haute direction, c'est-à dire les directeurs, les directeurs adjoints et les membres du conseil d'administration et toutes les personnes exerçant des fonctions équivalentes. ~~sont ou ont été chargées d'une fonction importante par une organisation internationale désignent les membres de la haute direction, c'est-à-dire les administrateurs, les directeurs adjoints et les membres du conseil d'administration ou des fonctions équivalentes.~~

(…)

- Statistiques : la recommandation 33 du GAFI demande aux pays de tenir des statistiques complètes sur les questions relatives à l'effectivité et à l'efficacité de leur système de LBC/FT, qui devraient comprendre des statistiques sur 1) les DOS reçues et ~~diffusées~~disséminées, 2) les enquêtes, poursuites et condamnations relatives au BC/FT, 3) les biens gelés, saisis ou confisqués et 4) l'entraide judiciaire et les autres demandes internationales de coopération. L'une des principales difficultés identifiées tient à l'absence, au niveau international, de consensus et d'orientations sur les types de données spécifiques qui devraient être collectés[98].

- D'après la recommandation 24 du GAFI, le traitement de données, y compris le cas échéant à caractère personnel, est requis pour les actionnaires ou administrateurs ~~agissant pour le compte d'une autre personne~~mandataires. Un actionnaire ~~désigné~~ mandataire (*nominee shareholder*) est un individu ou une personne morale qui agit, à un certain titre, pour le compte d'un autre individu ou personne morale (« le ~~désignateur~~mandant[99] ») ~~au sujet~~vis-à-vis d'une personne morale. Un administrateur ~~désigné~~ mandataire (*nominee director*) est un individu ou une personne morale qui exerce au quotidien des fonctions d'administration dans une entreprise pour le compte du ~~désignateur~~ mandant et en suivant ses instructions, directes ou indirectes. Les

~~[95] Tel qu'approuvé par les chefs des cellules de renseignement financier du Groupe Egmont en juillet 2013., voir : https://egmontgroup.org/~~

[96] Selon la définition du glossaire du GAFI, un groupe financier constitue « un groupe constitué d'une société mère ou de tout autre type de personne morale exerçant ~~des fonctions de~~un contrôle et des fonctions de coordination sur le reste du groupe~~, pour l'application de la surveillance du groupe en vertu des principes fondamentaux,~~ ainsi que des succursales et/ou ~~des~~ filiales soumises aux politiques et procédures de LBC/FT au niveau du groupe ».

[97] Toutefois, les exigences du GAFI exigent seulement que la liste des administrateurs soit accessible au public. Le reste ne doit être accessible qu'aux autorités compétentes.

[98] ~~Guide~~ Lignes directrices du GAFI sur les données et statistiques relatives à la LBC/FT, page 10.

[99] Par ~~désignateur~~ mandant (*nominator*), on entend un individu (ou groupe d'individus) ou une personne morale qui adresse (directement ou indirectement) des instructions à ~~une personne désignée~~un mandataire pour ~~qu'elle~~ qu'il agisse ~~pour son compte~~en son nom en qualité d'administrateur ou d''actionnaire ; on parle parfois de « commanditaire » (*silent partner*) ou d'« administrateur de fait » (*shadow director*).

actionnaires et administrateurs ~~désignés~~ mandataires ne sont jamais les bénéficiaires d'une personne morale.

- Conformément à la Recommandation 25 du GAFI, le traitement de données, y compris à caractère personnel, est nécessaire pour les trusts et les autres ~~structures~~ constructions juridiques. Ces données comprennent l'identité du constituant, du ou des administrateurs ou *trustees*, du protecteur (le cas échéant), des bénéficiaires ou de la catégorie de bénéficiaires et de toute autre personne physique exerçant en dernier lieu un contrôle effectif sur le trust, y compris au travers d'une chaîne de contrôle ou de propriété. Les termes « trust » et « *trustee* » sont à comprendre au sens de l'article 2 de la Convention de La Haye relative à la loi applicable au trust et à sa reconnaissance. Les *trustees* peuvent être professionnels (avocats ou sociétés de fiducie par exemple, selon les ~~territoires~~juridictions) s'ils sont rémunérés pour agir en cette qualité dans le cadre de leurs activités commerciales, ou non professionnels (si par exemple ils opèrent sans rétribution pour le compte ~~d'une~~ de la famille).

(…)

UNITED KINGDOM / ROYAUME-UNI

8. International data transfers in the AML/CFT field

(…)

Recommendation

(…)

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

(…)

Commented [A86]: Suggested amendment as discussed at PLEN and after agreement of our ES colleague
"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 cross-border transfer of data…"*

Comment based on the UK definition of 'branches' (In the UK there is no transfer where a transfer is made to a branch - but the situation differs in other countries/ this wording should now address all situations)

EDPS

Data protection rules and principles

1. Introduction

1.1. Background

(…)

Recent developments in important areas such as the general public's access to information on beneficial ownership[100], which was deemed to constitute a serious interference with the rights to respect for private life and to the protection of personal data[101] as it made public every personal data of every beneficial owner in a country. ~~This case~~ shows ~~s~~ that this area is in constant evolution and more regulation, including hard law, but also further jurisprudence ~~case law~~ in this field, is expected to come in the near future.

(…)

3. Basic principles for the protection of personal data

3.1 The principle of purpose limitation

(…)

AML/CFT contextualisation[102]

- 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, or with third parties[103] 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~~ an insurance intermediary gathering CDD data which is in turn passed on to the insurance company who would sell and issue the life insurance policy). 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.

(…)

3.2 The lawfulness of processing – legal basis

(…)

AML/CFT contextualisation[104]

Commented [A87]: We recommend deleting "every personal data of every beneficial owner" since the scope of the Sovim judgement is more limited, it refers to the information to be published according to the AML Directive

Commented [A88]: The text does not clarify how this secondary use would be compatible (compatible purpose test) with the primary use. We therefore recommend deleting this example.

[100] See the definition of "beneficial ownership information" under Annex I.
[101] ECJ judgement of 22nd of November 2022 in joined cases C-37/20 Luxembourg Business Registers and C-601/20 Sovim
[102] Relevant FATF Recommendations: Rec. 10-12,13, 15-18, 20, 22-27, 29, 31, 40
[103] In this context, «"third parties" should be interpreted as aAny natural or legal person that is external to and does not form part of the obliged entity or its financial group.
[104] Relevant FATF Recommendations: Rec. 24, 25.

(…)

- As explained before, Cconsent 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 an alternative legal basis~~can occur in compliance with a legal obligation.[Therefore, this legal basis could very unlikely be used for AML/CFT purposes as it will be probably overridden by other legal basis]. However, this legal basis could very unlikely be used for AML/CFT purposes as among other considerations data subject has no real choice. An alternative legal basis must be found because even if consent is obtained it is unlike to be valid (potentially rendering the processing unlawful~~). ~~More precisely,] the~~The AML/CFT framework ~~which~~ often involves specific investigations into suspicions of or actual ML/TF activities provides for situations where the customer is not or only ~~not completely~~partially informed of the data processing, particularly in relation to ~~enhanced due diligence measures and~~ 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 ~~by the OE~~. In those cases, ~~, because~~ prior information of the customer would contravene to AML/CFT prohibitions, in particular to tipping-off[105].

(…)

- The existence of i~~I~~nformation 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 are also of a legislative nature (e.g. legislative amendments may be needed to ensure a proper legal basis and allow partners to achieve their objectives). Data Protection Authorities in the EEA have recently expressed concerns having regard to possible compliance of PPPs with the fundamental rights to privacy and to the protection of personal data insofar as PPPs provide for the sharing of personal data[106].

(…)

3.3 The fairness and transparency of processing principles

(…)

Recommendation

(…)

- Access to personal data in central beneficial ownership registries should not be freely given as it may constitute 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 ~~specification~~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

(…)

AML/CFT contextualisation

[105] FATF Recommendation 21.

[106] EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations, 28 March 2023.

Commented [A89]: Suggestion: replace "alternative" with "a different and appropriate"

Commented [A90]: This word should be deleted for the sentence to make sense

Commented [A91]: We suggest adding this.

Commented [A92]: We suggested specifying "Public access by default", as this was the issue in the SOVIM judgment. Access by competent authorities and obliged entities (as interested parties) may still be necessary and proportionate for CDD and AML/CFT purposes

(…)

- 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 ~~"Know Your Customer" (KYC) standards~~CDD obligations, ~~they~~ 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 supervisory authorities~~missing an element of threat or of being fined by financial supervisory authorities~~, 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. ~~Conversely, due to the limited information position of each individual OE, data minimalisation can be promoted by more focused and streamlined information sharing between OE's to avoid unnecessary information collection by each individual OE in every instance.~~ 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.

Formatted: English (United Kingdom), Strikethrough

Commented [A93]: This should be reflected in a Recommendation below

(…)

3.6 The storage limitation principle

(…)

AML/CFT contextualisation[107]

- Clear requirements are set for the record keeping period of CDD information, account files, business correspondence and results of any analysis undertaken (at least 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)[108].

Commented [A94]: The establishment of a minimum instead of a maximum storage period for personal data runs counter to the principle of storage limitation. We propose deleting the wording "at least"

Commented [A95]: The establishment of a minimum instead of a maximum storage period for personal data runs counter to the principle of storage limitation. We propose deleting the wording "at least"

(…)

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

(…)

AML/CFT contextualisation[109]

(…)

- Being able to detect and report suspicious transactions[110] and ensure that customers are not aware that an STR or underlying information is filed with authorities[111] . It is also to be acknowledged that certain special categories of data, notably those which relate to ~~based on other legal obligations~~following other international crime-preventing ~~frameworks~~, contributions to ideological/political organisations, payments of fines etc. ~~that all can contain special categories of data~~ are processed regardless of any extra

Commented [A96]: Addition suggested

Commented [A97]: We suggest replacing "are" with "can be processed, insofar as strictly necessary and proportionate for the purpose(s) of AML or CFT"; see recommendation ahead in the text, second bullet point.

[107] Relevant FATF Recommendations: Rec. 2, 11, 24, 29, 40
[108] FATF Recommendation 11.
[109] Relevant FATF Recommendations: Rec. 1, 10, 11, 18, 20, 21
[110] FAFT Recommendation 20.
[111] FAFT Recommendation 21.

AML/CFT checks stemming from legal obligations set out by other international crime-preventing frameworks.

- AML/~~FTC~~CFT purposes may lead to the processing of special categories of data which deserve a strengthened protection ~~as per~~according to Article 9 of 108+, but ~~C~~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.

Commented [A98]: It is Article 6 of the Convention, not 9

(…)

8. International data transfers in the AML/CFT field

(…)

Recommendation

(…)

- The cooperation between data protection authorities and ~~other~~ AML/CFT competent authorities is to be recommended.

Commented [A99]: We recommend deletion