DT4C Alliance response to the public consultation on the EDPB's draft guidelines for applying Article 6(1)(f) GDPR

19 November 2024

DATA & TECHNOLOGY FOR COMPLIANCE

Introduction

The **Data and Technology for Compliance (DT4C) Alliance** represents the united voice of data and technology companies in Europe, operating as trusted service providers to financial and non-financial institutions dedicated to fighting corruption and money laundering. DT4C members play a critical role in helping these actors identify, prevent and block fraudulent and criminal financial transactions.

Fully recognising the importance of ensuring regulatory clarity and the consistent application of data protection principles throughout Europe, the DT4C Alliance is pleased to contribute to the public consultation on the European Data Protection Board's (EDPB) draft guidelines for applying Article 6(1)(f) GDPR. Since its inception, the DT4C Alliance and its members have advocated for enhanced collaboration and information sharing as a core principle to improve effectiveness in combating financial crime.

I. General comments

Our response to the EDPB's consultation is informed by the progress achieved by the EU in its new anti-money laundering and countering the financing of terrorism (AML/CFT) package, particularly the 6th AML Directive (AMLD6).

We would first like to highlight the essential role the GDPR plays in enabling AML/CFT efforts across the EU. GDPR provides a robust foundation for data protection in the EU and globally, helpfully acknowledging that the processing of personal data is sometimes necessary to serve significant public interests, including the prevention of financial crime. In particular, Article 9(2)(g) GDPR provides exemptions that permit the processing of special categories of data for reasons of substantial public interest, as defined by EU or Member State law, while Article 10 GDPR allows for the processing of personal data relating to criminal convictions and offences. In conjunction with the legitimate interest basis under Article 6(1)(f) GDPR, these provisions are instrumental for AML/CTF activities, enabling entities to access and process data that are essential for identifying and mitigating risks associated with illicit financial activities. This approach reflects the balance GDPR seeks to maintain between safeguarding individuals' rights to privacy and enabling necessary data access for regulatory compliance. By allowing certain exemptions for public-interest-driven data processing, GDPR provides a structured, lawful basis for accessing personal data in ways that align with the EU's broader goals of transparency, financial integrity, and the fight against criminal networks. Ensuring that these exemptions are clearly defined and consistently applied across Member States is vital for both effective AML/CFT enforcement and the protection of individuals' fundamental rights.

However, this balance was unintendedly disrupted by the ruling of the Court of Justice of the EU (CJEU) of 22 November 2022, which found that the 5th EU AML Directive (AMLD5) provision enabling public access to beneficial ownership (BO) information constituted a serious interference with the rights to privacy and data protection. To address the CJEU's concerns, many Member States restricted public access to their national BO registers—which subsequently has prevented many actors—including DT4C members—from being able to access this critical data. **In the fight against financial crime, DT4C members play an indispensable role in supporting the AML compliance obligations of banks and other financial institutions. The restrictions following the CJEU ruling have made fulfilling this role considerably more challenging.**

Helpfully, the EU's AMLD6 has since provided much-needed clarity and certainty regarding the accessibility of registers in respect of the CJEU's ruling, including to AML data and technology service providers. In particular, Recital 49 AMLD6 recognises the "critical role" played by data and technology service providers in assisting obliged entities (OEs) in complying with their legal requirements under EU AML/CFT rules; and **Article 12(j) AMLD6 explicitly recognises AML/CFT product providers as having a legitimate interest** for *"accessing information on beneficial owners of legal entities and legal arrangement held in the interconnected central registers for the purpose of prevention and combating of money laundering, its predicate offences and terrorist financing."*

But beyond the issue of *access* to data, DT4C members also *aggregate* and *process* such information to assist obliged entities under the EU's AML/CFT legislation—such as banks and other financial institutions— to verify ownership identities, analyse complex ownership structures, and assign risk scores based on factors like location, ownership complexity, and connections to high-risk areas. Through advancements in perpetual Know-your-Customer (KYC), they also regularly monitor changes in beneficial ownership and detect patterns associated with money laundering, triggering alerts when red flags appear.

To better reflect the reality of how beneficial ownership data needs to be legitimately used in the context of the EU AML rulebook, **Article 6 GDPR should consider the further processing of personal data—including *storing*, *structuring*, and *enhancing* data—for the purposes of fighting money laundering and terrorist financing.** In addition, **we would welcome more clarification that Article 6 does not limit service offerings to obliged entities but rather enables the creation of products and data solutions intended to support and inform requirements laid out in the EU AML Regulation.**

To this effect, the recent CJEU ruling of 4 October 2024 on legitimate interest under GDPR was a positive step, with the Court holding that a wide range of interests—including commercial interests—can also qualify. The Court further emphasised that these interests do not need to be based in law but must meet a three-step test: (1) the interest must be legitimate; (2) the data processing must be necessary; and (3) the rights and freedoms of data subjects must not outweigh the interest.

Against this background, **the DT4C Alliance welcomes the practical approach followed by the EDPB in its draft guidelines, including the use of examples and a structured framework that clarifies legitimate interest as a basis for processing**. As explained above, data and technology companies like DT4C members rely on legitimate interest in order to process and access data in a way that responsibly supports compliance, innovation, and the safeguarding of privacy rights. We especially value the guidelines' emphasis on balancing these interests with the rights of data subjects, given its direct impact on our members' ability to develop solutions that align with GDPR requirements.

II. Elements to be taken into account when assessing the applicability of Article (6)(1)(f) GDPR as a legal basis

First step: Pursuit of a legitimate interest by the controller or by a third party

When assessing the applicability of Article 6(1)(f) GDPR as a legal basis for data and analytics providers, it should be considered that the use and processing of relevant information by data and technology service providers is crucial for the purpose of preventing financial crime and conducting customer due diligence (CDD) Examples of this include understanding the corporate structure (usually very complex) with emphasis on revealing beneficial owners and/or knowing that a prospect has been convicted for money laundering, fraud, or other relevant criminal activities.

Whereas data and technology service providers are not subject to the legal obligations of the EU's AML regulations as obliged entities are, they play a vital role in ensuring that the latter are compliant with their legal obligations. This reality should be further reflected in the EDPB's guidelines, building on the CJEU ruling of 4 October and its clarification that commercial interests can qualify as legitimate ones. Irrespective of the existence of an underlying commercial interest, the products and solutions offered by data and technology service providers serve a legitimate purpose in the fight against financial crime.

As such, in our view, Article 6(1)(f) GDPR should consider the imperative of the fight against financial crime as a "legitimate" purpose of the interest pursued by both the controller, i.e. the data and technology service provider, and by the third party, i.e. the obliged entity. We would request that this be added to the helpful examples provided in the guidelines in paragraph 25.

On top of this, data and technology service providers' legitimate interest in processing personal data is firmly rooted in the open data concept resulting from EU Directive 2019/1024 on open data and the re-use of public sector information. This directive is based on the general principle that public and publicly funded data (e.g. company or UBO registries) should be reusable for commercial or non-commercial purposes. It aims to boost the socioeconomic potential of public-sector information by increasing the supply of dynamic data and datasets with a particularly high economic impact (with companies and company ownership as one of the thematic categories of high-value datasets), and by promoting competition and transparency in the information market. **We believe that it would be helpful to recognise (also in paragraph 25) processing of personal data constituting public-sector information – which is conducted, amongst others, by data and technology service providers - under the umbrella of examples of processing based on the legitimate interest provision of Article 6(1)(f) GDPR.**

Second step: Analysis of the necessity of the processing to pursue the legitimate interests

We appreciate and commend that the guidelines specifically recognise that "necessity" must be examined in conjunction with the "data minimisation" principle enshrined in Article 5(1)(c) GDPR, in accordance with which personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Likewise, the recognition of Recital 47 GDPR, which states that "the processing of personal data strictly necessary for the purposes of preventing fraud […] constitutes a legitimate interest of the data controller concerned". In the context of this response, we would like to raise for your consideration the ability of data and technology service providers to provide assistance to obliged entities in achieving this principle. In the absence of curated limited purpose data, controllers subject to AML regulations may over ingest data not relevant in the determination of their legal obligations under Article 6(1)(c) in this context under AML/CFT regulations. As specialised service providers we can assist the obliged entities in this process by focusing on the most relevant information for this limited purpose. This also benefits the targeted data subject. To that extent, we would request a revision to paragraph 30 of the guidance to again recognise that a controller assisting a third party in the data minimisation process is a valid consideration for this second step of necessity assessment.

Third step: Methodology for the balancing exercise

We consider that the balancing exercise is vital to reach the main goal of the GDPR, i.e. protecting privacy of natural persons whilst ensuring legal certainty to controllers. To this end, we consider it paramount to avoid the instrumentalisation of GDPR as a channel to frustrate and limit the fight against criminal activities like money laundering and financing of terrorism.

In this regard, we would like to recall the consistent European Convention on Human Rights (ECHR) and CJEU case-law (lastly *Ligue de droits* ECJ C-817/19 and case-law recalled) which established the need to consider specific circumstances and context for balancing fundamental rights and interests at stake in the processing of data, which we would like to see clarified in order to contribute to a healthy EU financial ecosystem.

We acknowledge that any limitation of fundamental rights, including the right to privacy, must be provided for by law, respecting the essence of fundamental rights and in accordance with the principle of proportionality. As a result, the possibility to limit a right should be necessary and meet genuinely a general interest objective or the need to protect the rights and freedoms of others (Opinion 1/15 European Court of Justice).

In this regard, we consider that the fight against money laundering and the financing of terrorism in the financial system contribute to the protection of rights and freedom, in view of Article 6 of the Charter of Fundamental Rights of the EU which codifies the right to liberty and security. **As a consequence, AML/CTF could and should be considered clearly as a legitimate interest objective under Article 6(1)(f).** Specifically,

we consider that, as providers of AML/CTF services supporting obliged entities, our processing should be clearly considered lawful on the basis of legitimate interest and reflected in this guidance. Similarly, we consider this reasoning applicable to fraud prevention, which pose serious threats to the security and the financial interests of the EU as well as to its citizens, in line with Article 325 on the Treaty on the Functioning of the European Union.

Considering the delicate task to balance diverse fundamental rights and interest, we are fully conscious of the observance of the proportionality requirements and in full support of the need to not excessively interfere with the right to privacy, in line with CJEU joined *Cases C-37/20* and *C-601/20*.

On this issue, we highlight that our data processing is limited, in terms of:

- Subjects who can process data, namely providers of AML/CTF services in addition to obliged entities;
- Availability of the data, as this is provided for compliance with AML obligations and is not generally available to the public;
- Categories of processed data are those strictly necessary for the purpose;
- Additional data protection safeguards that are put in place (e.g. data encryption, cybersecurity standards, etc.).

When reviewing what would be considered a reasonable expectation of a particular data subject, that is a criminal actor, the GDPR should not be seen to question the purpose of the greater societal function of preventing, detecting and punishing criminal actions. For reference, Recital 4 GDPR states, *"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."* On the other hand - looking from the perspective of reasonable expectation of a data subject being a good actor in the AML framework – it should be noted that, amongst others, UBOs and companies' representatives can be assumed in their business capacity to reasonably expect that - due to the fact they operate in the business environment - their personal data is processed for anti-money laundering purposes and this may include processing conducted by data and technology service providers.

When expected to detect if money laundering is taking place, obliged entities do not have the same resources or authority as governmental agencies, and often rely on entities that specialise in gathering and organising this data. However, whereas law enforcement has protections for their activities and obliged entities can rely on legal obligations, criminal actors have the opportunity to use GDPR to obstruct organisations that specialise in gathering and fairly sharing this data in assistance to these obliged entities.

Thus, we request clarity on the context of the "average" data subject. Data subjects who are seeking to subvert the prevention of criminal activity should not be able to utilise GDPR.

Overall, we consider compliance with GDPR and all relevant EU law, as well as adherence to international standards and best practices not only as a legal duty and reputational obligation, but as a relevant competitive added value. For this reason, we ensure data subjects' rights from potential abuse and unlawful access to/use of their data.

III. Relationship between Article 6(1)(f) GDPR and data subject rights

The relationship between Article 6(1)(f) GDPR and data subject rights is complex and requires careful balancing. In this balancing exercise, data and technology service providers:

1. Conduct thorough Legitimate Interests Assessments (LIAs) and publish LIA summaries to demonstrate accountability.

2. Perform and document detailed LIAs before relying on Article 6(1)(f), carefully weighing the necessity of processing against potential impacts on data subject rights.
3. Provide clear, concise explanations of legitimate interests in privacy notices.
4. Implement strong data minimisation.
5. Only collect and retain the minimum personal data necessary to achieve the legitimate interests and reduce potential negative impacts on data subjects.

IV. Contextual application of Article 6(1)(f) GDPR

Money laundering and fraud threats are on the rise and posing significant risks to individuals, organisations, and society at large. This is underlined by the recently adopted EU's AML package and the European Commission's study on *Scams and Fraud Experienced by Consumers* that stresses that online fraud represents a significant portion (43%) of fraud cases, a finding also referenced in the Commission's recent Digital Fairness Fitness Check.

Sufficiently robust money laundering, terrorist financing and financial fraud detection is fundamental for the process of financial crime compliance and fraud prevention as otherwise prevention would only be limited to accidental findings or user reporting. An overly restrictive interpretation of legitimate interest in the context of financial crime compliance and fraud prevention therefore can inadvertently undermine efforts to protect citizens and society against bad actors. Data privacy rules therefore need to take into account the specific contextual application of Article 6(1)(f) GDPR. This is reflected in Recital 47 GDPR which clearly states that, *"processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."*

The processing of personal data is often necessary for financial crime compliance and fraud prevention measures, for which legitimate interest is the most applicable legal basis. The other legal bases provided under the GDPR simply do not work effectively in this specific context. This is particularly true for consent or contractual necessity if one considers the fact that it concerns bad or malicious actors who, by definition, won't collaborate or abide by the rules. Albeit obvious, this notion is often overlooked when considering an appropriate balance between data privacy and financial crime compliance objectives.

We therefore ask that the EDPB reconsiders the distinction between fraud prevention and detection, object to the EDPB's overly strict interpretation of Recital 47 GDPR in paragraph 100 and request the EDPB to improve the Guidelines' Chapter IV part 3 to reflect better the clear intention of the legislator.

Get in touch

For more information about the
DT4C Alliance and its role,
please contact:
Emanuel Santos, DT4C Secretariat
secretariat@dt4calliance.eu / M.: +32 492 11 02 20

DATA & TECHNOLOGY FOR COMPLIANCE