ARGUMENTS ACCORDING TO WHICH IT WOULD NOT BE MANDATORY FOR INVESTMENT FUNDS TO APPOINT A DATA PROTECTION OFFICER IN THE SOLE KYC/AML CONTEXT

DAVID ALEXANDRE
ISABELLE COMHAIRE
GARY CYWIE
CATHERINE DI LORENZO
ÉLISABETH GUISSART

OLIVIER REISCH
ERWIN SOTIRI
CAMILLE TULASNE
ASTRID WAGNER
VINCENT WELLENS
HERVÉ WOLFF

AVOCATS

CONTENTS

1. INTRODUCTION

Article 37(1) of the Regulation (EU) 2016/679 (the General Data Protection Regulation, **GDPR**) requires controllers and processors to designate a Data Protection Officer (**DPO**) if certain criteria are met.

Controllers and processors who are not public authorities or public bodies must designate a DPO when their core activities consist of either[1] :

(i) the processing of special categories of data pursuant to Article 9 of the GDPR[2] or personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR[3] ; and/or

(ii) processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects[4] ;

on a large scale.

Determining whether or not investment funds must appoint a DPO is complex and not clearly specified yet.

Although other considerations may apply (including the ongoing possibility to appoint a DPO voluntarily), this paper outlines the arguments according to which it would not be mandatory for investment funds to appoint a DPO only on the basis of the KYC/AML activities they carry out further to mandatory requirements of statutory laws to which they are subject. This paper is confined to this specific question as it is common to all persons subject to these legal requirements. Controllers and processors may have to examine other processing operations on a case-by-case basis to determine whether or not the appointment of a DPO is mandatory in their specific case.

With a view to providing the above-mentioned arguments, this paper will discuss to what extent the KYC/AML activities of investment funds, the exact nature

1. This paper does not deal with the hypothesis where the processing is carried out by a public authority or body, including courts acting in their judicial capacity.
2. That is "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".
3. Article 37(1)(c) of the GDPR.
4. Article 37(1)(b) of the GDPR.

of which mainly depend on the level of risk identified by them :

- may incidentally comprise the processing of special categories of data or personal data relating to criminal convictions and offences ;
- do not constitute regular and systematic monitoring ; and
- why these data processing activities do not form part of the core activities of investment funds.

Should any of the above-mentioned activities not be carried out on a large scale, then the analysis is not even required.

2. HOW TO APPLY DPO DESIGNATION CRITERIA FOR INVESTMENT FUNDS ?

The Law of 17 December 2010 relating to undertakings for collective investment (**UCIs**) defines an undertaking for collective investment in transferable securities (**UCITS**) as an undertaking with the sole object of collective investment in transferable securities and/or in other liquid financial assets referred to in Article 41(1), of capital raised from the public and which operate on the principle of risk-spreading, and with units which are, at the request of the holders, repurchased, directly or indirectly, out of this undertaking's assets.

Directive 2011/61/EU defines an alternative investment fund (**AIFs**) as a UCI other than a UCITS that raises capital from a number of investors with a view to investing it in accordance with a defined investment policy for the benefit of those investors.

By legal definition, the core activity of UCIs (i.e. investment funds) is, simply speaking, the investment of capital raised from their investors and management thereof. Their core activity is neither the processing of personal data for KYC/AML purposes nor the processing of special categories of personal data or of personnal data related to criminal convictions and offences.

2.1. Question 1 : Do the KYC/AML activities of investment funds consist of :

(a) processing of special categories of personal data or personal data relating to criminal convictions and offences ; and/or

In the context of their day-to-day business, investment funds may incidentally (i.e. only if and when such information pops-up in the course of legally required checks) come into possession and thus process special categories of personal data or personal data relating to criminal convictions and offences. This is particularly true in relation to the KYC/AML checks that investment funds are legally obliged to perform mainly on their investors. When performing these checks, investment funds may collect personal data revealing an individual's political opinion or trade union membership. This is, however, the exception. In most circumstances, the on-boarding of an investor in the fund will not entail the processing of these types of personal data. In any event, the processing of such personal data will not automatically occur in relation to, and does therefore not form part of, the core business of the activity of investment funds as it is not necessary *as such* in the context of such activity as defined above.

It can also not be excluded that investment funds may collect personal data relating to an individual's criminal convictions and offences where they are legally obliged to (e.g. when appointing directors/managers) and only if such information actually exists. Again, this processing will, however, be punctual and very limited, and only occur if any of their investors are actually concerned. The same reasoning as above applies, i.e. the processing of such personal data will not automatically occur in relation to, and therefore does not form part of, the core business of the activity of investment funds as it is not necessary *as such* in the context of such activity as defined above.

The core activity of investment funds, therefore, does not consist of or comprise the processing of special categories of personal data or of personnal data related to criminal convictions and offences.

For both situations described above, it is certain that the processing of these kinds of personal data is incidental only and that the activities of investment funds involve the management of their investors' money in their interest and do not require, as such, the processing of these kinds of personnal data. In the vast majority of cases, investment funds do not collect and process these kinds of personal data.

We further discuss below whether such processing forms part of the core activities of investment funds (please see point 2.2).

(b) processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects ?

Although it is key for the application of several of its provisions (e.g. Article 3(2)(b), 35 and 37), the GDPR does not

define the concept of monitoring nor of "regular and systematic" monitoring.

That said, Recital 24 of the GDPR gives some indication on the EU legislator's approach to this concept of monitoring in the context of the extra-territorial application of the GDPR : "*(...) In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*" (emphasis added).

The Article 29 Working Party (the **29WP**) has also provided some guidance in this respect, which is endorsed by the European Data Protection Board, the **EDPB**[5]. This guidance is however spread across various opinions which are not always easily reconcilable.

In its Guidelines on Data Protection Officers[6], the 29WP explains that "*The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but is mentioned in recital 24 and clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment.* (...)

Examples of activities that may constitute a regular and systematic monitoring of data subjects : profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering) ; location tracking, for example, by mobile apps ; loyalty programs ; behavioural advertising ; monitoring of wellness, fitness and health data via wearable devices ; closed circuit television ; connected devices e.g. smart meters, smart cars, home automation, etc." (emphasis added). Fraud prevention and money laundering are referred to as examples for profiling and scoring for purposes of risk assessment in the context of credit scoring and establishment of insurance premiums and would, therefore, only apply to credit institutions and insurance companies who are constantly carrying out these activities as part of their services and whose systems routinely track each and every financial activity and inevitably track the behaviour of the relevant account holders. As such, this activity could be considered as a core activity of banks and insurance companies unlike investment funds as explained in more detail in Question 2 below.

In its Guidelines on the territorial scope of the GDPR[7], the EDPB has given some additional clarifications on the notion of "monitoring" data subjects' behaviour by stating in the context of the determination of the application of the GDPR that "*neither Article 3(2)(b) nor Recital 24 expressly introduce a necessary degree of 'intention to target' on the part of the data controller or processor to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities. However, the use of the word 'monitoring' implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EU. The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as 'monitoring'. It will be necessary to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data*" (emphasis added). Applied to investment funds, it can be inferred from this example that the specific purpose they have in mind when performing their KYC/AML obligations is complying with the laws combating money laundering and terrorism financing. That purpose is a collective one pursued by law. In this context, although they may contribute to this collective effort, investment funds do not collect and reuse in the normal course of their business personal data for the specific purpose of monitoring the behaviour of data subjects. Although the aforementioned guidelines examines the territorial scope of the GDPR, the interpretation of the concept of monitoring should apply irrespective of the context.

As a result, although the concept of "monitoring" could potentially be construed as including a situation where a controller such as an investment fund obtains information about data subjects for the purposes of assessing their behaviour in the context of their compliance activities (e.g. KYC/AML checks), this wide construction of the concept of monitoring does not reflect the EU legislator's intention as stated in Recital 24 of the GDPR and as further developed by the EDPB, in particular in its guidelines referred to above.

The principle of "regular and systematic monitoring" requires an ongoing watchfulness of data subjects' behav-

5. The 29WP is the independent European working party that dealt with issues relating to the protection of privacy and personal data. As of the entry into application of the GDPR on 25 May 2018, it has been replaced by the European Data Protection Board, composed of representatives from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission.

6. WP 243 rev.01 available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

7. Guidelines 3/2018 adopted after public consultation, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.

iour and is a principle applicable, for example, to banks. Indeed, since their business is to handle cash and other transactions, they will constantly monitor their clients' accounts in order to offer them tailor-made services based on the establishment of their profile or to contact them proactively if there is suspicious activity on their bank accounts (due to an unusual use of their credits cards in a foreign country or a payment of an unusual amount of money compared to the pattern established for the use of their account by each relevant client). They will organise their AML in a way which will be intimately linked to all transactions and thereby be inevitably tracking their clients' behaviour. Such "regular and systematic monitoring" is, however, not applicable to investment funds, which do not constantly monitor their investors – they may indeed have to perform several KYC/AML checks during their relationship, but only upon the occurrence of specific triggering events. Moreover, investment funds do not check the origin of the funds each and every time their investors are sending money to them as it may be sufficient to check the origin of the fortune of an investor at the time when the professional relationship starts. This "constant vigilance" or "ongoing monitoring" required by KYC/AML laws is clearly different from a "regular and systematic monitoring" or to monitoring at all in the meaning of the GDPR.

KYC/AML checks *per se* can thus, in our opinion, not be considered as intrinsically falling in the definition of "monitoring" since :

- Their purpose is not to assess the behaviour of an individual. In fact, for KYC, the information collected will very often be a copy of a passport and of a utility bill for the sole purpose of checking the identity and address of an individual. This processing is not done for the purpose of analysing or predicting behaviours, preferences or attitudes of the individual but just to check his/her identity and address. Regarding AML, the purpose is to check the origin of the funds used by the investor for a given transaction. Here again, the purpose is not to track any behaviour, preference or attitude of an individual, but to check the source of the money they are using.
- They are "one shot" operations only, even if they are performed repeatedly during the relationship between the investment funds and their investors (e.g. every 1, 2 or 3 years depending on the particular context and level of risk). KYC/AML checks are indeed performed by the investment funds at the beginning of the relationship with their investors, and eventually upon the occurrence of a specific triggering event. There is, therefore, no tracking and hence no regular monitoring.

Also, unlike the checks that can be done in relation to the transfers of money made into and from a bank account (which may reveal a whole lot of information about data subjects lives', consumption habits, locations, etc., in other words their day-to-day behaviour), checks done in the context of KYC/AML by investment funds only give a limited view on data subjects' behaviour from both a quality and quantity standpoint.

We further discuss below whether such processing forms part of the core activities of investment funds (please see point 2.2).

2.2. Question 2 : Does the data processing analysed in Question 1 form part of the core activities of investment funds ?

In its FAQs on the designation of a DPO[8], the 29WP specifies that :

"*'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, processing health data, such as patient's health records, should be considered as one of any hospital's core activities and hospitals must therefore designate DPOs.*

On the other hand, all organisations carry out certain supporting activities for example, paying their employees or having standard IT support activities. These are necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity."

According to the Data Protection Commission of Ireland, a private security company which carries out surveillance of private shopping centres and/or public spaces using CCTV would be required to appoint a DPO as surveillance is a core activity of the company[9].

In its online Q&A, the Belgian *Association pour la Protection des Données* (APD) provides that "*each time the processing forms an integral part of the activity of the controller or of the processor, it is deemed a core activity*" whereas "*although they are necessary for such activity, supporting activities (salary payment, data relating to career management) will be generally deemed as ancillary activities.*" The APD provides examples of core activities, as follows :

8. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf.

9. http://gdprandyou.ie/data-protection-officer.

- *"processing of health data in the context of health care services provided by a hospital ;*
- *processing of data in the context of the provision of insurances products by insurance companies ;*
- *processing of data by interim agencies relating to the interim workers they staff ;*
- *processing of data by schooling institutions in relation to their students ;*
- *processing of data by fiduciary services companies in relation to the workers of their clients.*[10]"

The common theme of all these examples is that the entity concerned must process the personal data at stake to provide its services or, in other words, to carry on its business activities. Business units that contribute significantly to the realisation of the company's business strategy, and are not just routine administrative and conservation tasks, form part of the core activities of the company. Data processing must be indispensable for the business purpose of the controller or processor and not an end in itself[11]. The processing forms an inextricable part of the service itself. For example, it would not be possible for a hospital to provide health care services without processing data about the health of the patients. Insurance companies need to monitor their clients' behaviour such as their health or their real property to assess the risk they are covering before providing a health or home insurance product respectively. Beyond the core activities listed by the APD, it can be added that monitoring the client's behaviour is also a core activity of banks since such monitoring is inextricable from their function as a depositary and lender of money. Indeed, such monitoring is required for the banks to avoid anti-money laundering and to enable, for example, the lending of money to their customers which require it to establish a risk profile of the future borrowers. In other words, performing anti-money-laundering checks is a task that is required for a bank to protect itself against risks which are directly linked to its banking activities.

An investment fund is "*a company or fund that gathers capital from a number of investors to create a pool of money that is then re-invested into stocks, bonds and other assets*"[12]. Investment funds thus provide collective investment opportunities. To provide such services, they do not intrinsically need to know the source of the wealth of the investors who become their shareholders. In fact, investment funds structures do not need to know who those shareholders are to provide their investment advisory and portfolio management services (other than for collecting funds and paying dividends as appropriate). The situation is not different from other shareholders, such as those holding stocks of listed companies. Those companies do most often not know their shareholders.

As such, even though most of the EU-based investment funds structures are required to perform KYC/AML checks on their investors (which might not be the case in other jurisdictions), it is reasonable to argue that such activity does not form an inextricable part of their activity. Although they need certain information about their shareholders to collect funds and pay dividends (mainly their bank account number), investment funds do not intrinsically need a copy of a passport, utility bill, or similar evidence of identity and address of their shareholders.

Service providers such as central administration agents, transfer agents or domiciliary agents who regularly or largely provide KYC/AML checking services on remuneration regarding investment fund structures as part of their main business/service offering, eventually should separately assess whether such activity forms part of their core activity.

Finally, the fact that KYC/AML checks are mandated by law does not automatically mean that the personal data processing activities related to such legal obligations should be regarded as a core activity of the entity carrying out such checks. Preventing the misuse of the financial markets and combating money laundering and terrorism financing does not form part of the core activity of investment funds. They are not set up for that purpose or for collecting and processing personal data for that purpose. Carrying out KYC/AML checks does not add any value to investment funds products and is more often seen as a burden rather than an element that would be promoting them. It's a legal requirement and merely an administrative task to be performed on top of the core activity of investment funds. The ensuing processing of personal data (e.g. asking for a copy of the shareholders' passport) can, therefore, not be seen as an inextricable part of investment funds' activities.

There are a number of examples of legal obligations that controllers and processors must comply with which cannot be considered as their core activities, such as the ob-

10. https://www.autoriteprotectiondonnees.be/faq-themas/quand-d%C3%A9signer-un-d%C3%A9l%C3%A9gu%C3%A9-%C3%A0-la-protection-des-donn%C3%A9es.

11. „Kerntätigkeiten sind Geschäftsbereiche, die entscheidend zur Realisierung der Geschäftsstrategie des Unternehmens beitragen und nicht nur routinemäßige Verwaltungs- und Erhaltungsaufgaben darstellen. Datenverarbeitungen müssen also zur Geschäftszweckerreichung des Verantwortlichen oder Auftragsverarbeiters unerlässlich, aber nicht die einzige Tätigkeit als Selbstzweck sein." See von dem Bussche in: Plath, DSGVO/BDSG, 3rd edition 2018, Article 37 DSGVO, point 19.

12. http://lexicon.ft.com/Term?term=investment-company-or-investment-fund.

ligation to keep any documents relating to accounting or for tax reasons, the obligation to process (special categories of) personal data of employees in an employment context, the new obligation to process personal data of beneficial owners and communicate such data to the Beneficial Owner Register (in view of their publication).

Based on the above, there are solid arguments to say that the processing of personal data by investment funds in the context of KYC/AML does not form part of their core activities.

2.3. Question 3 : Is the data processing analysed in Question 1 conducted on a large scale ?

The GDPR does not define what constitutes "large scale" processing but guidelines about the interpretation of the GDPR recommend that the following factors be considered when determining whether the processing is carried out on a large scale[13] :

- The number of people concerned, as a particular figure or as a proportion of the applicable population.
- The volume of data and/or the range of different items of information items being processed.
- The duration, or permanence, of their information processing.
- The geographical extent of the processing activity.

Some individual EU data protection authorities have provided guidance in terms of large scale thresholds as a number of data subjects[14]. In general, such numbers amount to between 4 % and 6 % of the total concerned population, giving a good indication of what more general thresholds might be. For processing, activities that relate to the Luxembourg market and population, the threshold for large scale data processing could therefore be a database exceeding around 30.500 data subjects[15]. One could also compare the total population of the countries where the investment fund operates against the number of investors from such countries. One could finally take into consideration the median number of investors per type of investment product considered and compare it with the number of investors in a specific fund active in that segment.

This criterion of "large scale" seems, therefore, to be met for large international funds (such as UCITS funds for example), important funds with a large geographical extent since they may bring together a large number of investors and more generally a large number of data subjects. On the contrary, for funds with one or few investors, this criterion is unlikely to be met.

3. CONCLUSION

Taking the above analysis into consideration, one can come to the conclusion that, in relation to KYC/AML activities carried out by investment funds :

- Should investment funds assess their KYC/AML activities as not carried out on a large scale, then such analysis is sufficient to determine that they are not obliged to appoint a DPO in relation to such KYC/AML activities.
- Processing of special categories of personal data or personal data relating to criminal convictions and offences is incidental and, most of the time, occasional only and not necessary as such for investment funds to carry out their core activity.
- AML/KYC activities should not be considered as falling within the definition of "monitoring" since their purpose is not to assess the behaviour of an individual but rather checking the identity and address of an individual and the source of the money in relation to a particular transaction.
- Even though it would be considered that investment funds are monitoring the behaviour of investors, *quod non*, the processing of personal data for KYC/AML as mandated by law should not be considered as part of the core activities of investment funds which are to provide collective investment opportunities. To provide the latter services, investment funds do not intrinsically need to know the source of the wealth of the investors or to obtain proof of identity of their shareholders. This applies even more so for listed companies that do not necessarily know their shareholders.
- Based on the above, the designation of a DPO by investment funds should not be required for processing personal data arising out of mandatory KYC/AML activities.
- It is undebatable, however, that services providers such as central administration agents, transfer agents or domiciliary agents who provide KYC/AML checking services to investment funds structures as part of their main service offering, eventually against remuneration, should consider such activities as being part of their core activities. Consequently, these entities should check if all the other conditions are met in which case they would be obliged to appoint a DPO.

13. *Op. cit.* n° 1.

14. For example Estonian authority: https://www.linkedin.com/feed/update/urn:li:activity:6404572629235220480; Dutch authority: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg; German federal authority: https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/ListeVerarbeitungsvorgaenge.html.

15. I.e. 5 % of a 610,000 total population.