# DAC6: What do financial institutions need to know about their clients' tax affairs?

*By Eric CENTI, Partner Tax & Nenad ILIC, Director Tax, Deloitte*

**DAC6 is the name commonly given to EU Directive 2018/822/EU of 25 May 2018 and refers to the most recent amendment to the EU directive on administrative cooperation in the field of taxation. It was implemented in Luxembourg by the Law of 25 March 2020 and, once in force, will impose new disclosure obligations on intermediaries (and potentially taxpayers) regarding reportable cross-border tax arrangements that contain certain predefined hallmarks.**

The definition of an intermediary is broad, encompassing not only lawyers and advisers but also banks, insurance companies, asset managers and investment funds, trust companies, and other financial sector professionals. More specifically, it covers any person or entity that designs, markets, organizes, or makes available or manages the implementation of a reportable cross-border arrangement.

The definition goes on to designate intermediaries as any person or entity that—having regard to the relevant facts and circumstances and based on available information and the relevant expertise and understanding required to provide such services—knows (or could be reasonably expected to know) that they have undertaken to provide (directly or through other persons) aid, assistance or advice for designing, marketing, organizing, and making available for implementation or managing the implementation of a reportable cross-border arrangement.

In simpler terms, DAC6 defines intermediaries as any person or entity that

knows or is presumed to know that they have aided or advised on a reportable cross-border arrangement entered into by their clients. For financial institutions, this translates into performing specific due diligence procedures on their clients and their clients' transactions to assess whether they contain one or several hallmarks that would make them reportable. This, in turn, raises questions as to how far should a financial institution go with such due diligence. In other words, what is a financial institution expected to know about its clients' tax affairs when assessing DAC6 hallmarks?

In this respect, the Law of 25 March 2020, the explanatory memorandum to the draft law and the interpretation guidelines issued by the Luxembourg tax authorities on 13 May 2020 provide useful clarifications.

According to the Law of 25 March 2020, a person or entity can provide evidence that they did not know and could not reasonably be expected to know that they were involved in a reportable cross-border arrangement. This evidence should be based on all relevant facts and circumstances, as well as available information and their relevant expertise and understanding required to provide the services.

This is an important limitation to the definition of an intermediary, as often financial institutions may only be involved in a particular part of a wider arrangement (such as a bank providing finance) and may not have a full understanding of all the arrangement's facts and implications, including its potential for containing DAC6 hallmarks.

Furthermore, financial institutions may not always possess the required level of expertise for a thorough assessment of an arrangement that their clients designed and achieved, especially when these arrangements involve sophisticated cross-jurisdictional structures, complex financial instruments and transactions, etc. In these cases, a financial institution would reasonably be able to conclude that it would not be expected to report under DAC6, because it did not know, and could not reasonably be expected to know, that it was involved in a reportable arrangement.

In addition, the explanatory memorandum to the draft law as well as the interpretation guidelines specify that intermediaries can rely on existing professional obligations (including, for example, existing due diligence procedures) and that they must not actively search for information that they do not normally collect as part of those obligations. If after applying those obligations it appears that an arrangement does not qualify under DAC6, financial institutions would reasonably be able to conclude that no DAC6 reporting is necessary.

In tax matters, existing due diligence procedures generally derive from the CSSF Circular 17/650 from 17 February 2017 on aggravated tax fraud and tax swindle (which itself transposes the revised FATF standard of 2012/2013 and the Fourth AML Directive), the Law of 24 July 2015 implementing the Foreign Account Tax Compliance Act (FATCA) in Luxembourg and the Law of 18 December 2015 implementing the Common Reporting Standard (CRS) in Luxembourg. Annex I of the CSSF Circular 17/650 provides a list of 21 indicators of tax fraud and tax swindle that financial institutions need to monitor on an ongoing basis as part of their AML/KYC procedures.

Some of these indicators are closely linked to certain DAC6 hallmarks and, therefore, should reasonably form part of financial institutions' standards of knowledge for DAC6 purposes. Furthermore, the CRS and FATCA Laws obligate financial institutions to perform reasonableness checks on self-certifications provided by clients. Here again, information collected from these self-certifications and reasonableness checks is relevant for certain DAC6 hallmarks and, as a result, should be included in the standards of knowledge for DAC6 purposes.

Therefore, a key question is how to treat information and documentation that financial institutions may have access to in the ordinary course of their business but that do not, strictly speaking, need to be read or examined as part of their AML/KYC and CRS due diligence procedures.

For example, financial institutions may come across a tax opinion, an email, or any other documents that could potentially contain elements relevant under DAC6, but that are not required to be reviewed under standard due diligence procedures. In such a case, financial institutions would generally not be required to review the document in detail specifically for DAC6 purposes to determine whether it relates to a reportable cross-border arrangement.

In contrast, financial institutions that fail to perform their normal due diligence, or find ways to be deliberately ignorant by avoiding reviewing particular documentation or asking particular questions, may not be able to demonstrate that they do not meet the "reasonable-to-know" test. In this scenario, the Luxembourg tax authorities would likely maintain that the financial institution should reasonably be expected to know that the arrangement was reportable.

While the clarifications provided in the Law of 25 March 2020 and the interpretation guidelines issued by the Luxembourg tax authorities do provide useful guidance to assess DAC6 hallmarks, the actual application of those rules by financial institutions will be fact-dependent and most likely subjective rather than objective. Therefore, one could expect significant disparity in the standards of knowledge across different financial institutions.

To avoid any potential consequences of non-compliance, it may be of particular interest for financial institutions to establish comprehensive yet meaningful standards of knowledge to support and justify the actions and decisions made, and to demonstrate a considerate business behavior and good faith effort to comply with their DAC6 obligations.

# Shaping Europe's digital future with the upcoming review of the NIS Directive

*By Monica ADAMI, Analyst, Ghita ENNADIF, Analyst, Clare O'DONOHOE, Analyst, Alessandro ZAMBONI, Partner (Wavestone Luxembourg) & Lorenzo PUPILLO, Head of the Cybersecurity@CEPS Initiative*

**On the 27th of May 2020, the European Commission adopted a proposal for a major EU recovery plan in the wake of economic damage brought about by the global outbreak of Covid-19. As part of this recovery plan, large investments will be made in cybersecurity in order to increase Member States' capabilities in this domain and boost the EU's overall cybersecurity capability. This will be accompanied by a review of the Directive on security of network and information systems ("NIS Directive" or "Directive"), which is the first piece of EU-wide legislation on cybersecurity.**

The NIS Directive was born from the overarching need to ensure Member States' preparedness and cooperation regarding cyber risks and set cybersecurity requirements for key private and public organisations. Network and information systems are indeed essential to facilitate the functioning of cross-border movements of goods, people and services within the European Union (EU) and to create a trusty environment for the digital single market to flourish.

Proposed in February 2013 by the European Commission, the NIS Directive entered into force in August 2016, after three years of discussions between the European Parliament, co-legislators, and the European Commission. The final text included several compromised amendments, such as updated selection criteria for essential services (OESs) and digital service providers (DSPs) at the request of the Parliament and the Council, and the establishment of national single point of contacts, a Computer Security Incident Response Team (CSIRT), the CSIRT network and the Cooperation Group. While, the NIS Directive allows Member States to impose stricter requirements than the minimum harmonisation measures stipulated in the Directive itself to protect society and the economy from any disruption to their essential services, while imposing maximum harmonisation with regards to DSPs.

As DSPs are cross-border by nature, with headquarters in different countries and acting under varying national legislation, it was decided to make their notification requirements less strict. Under the principle of maximum harmonisation, Member States are not allowed to adopt stricter measures than those set out in the Directive in relation to DSPs and are simply mandated to apply the stated requirements of the NIS Directive.

After reviewing the amendments, the Commission stated that the Council's and Parliament's proposed compromise endorses the objectives of the initial proposal, namely, to ensure a high common level of security in network and information systems, and thus, the changes regarding how to achieve this goal were welcomed.

Luxembourg's Prime Minister and President of Council at that time, Xavier Better, stated that "This was an important step towards a more coordinated approach in cybersecurity across Europe. All actors, public and private, will have to step up their efforts, in particular by increased cooperation between Member States and enhanced security requirements for infrastructure operators and digital services", following the approval of the final text of the Directive.

Following the adoption and implementation of the NIS Directive, some challenges have emerged in the transposition process in the Member States. First, the scope of the NIS Directive excludes software providers, hardware manufacturers, and SMEs from its provisions. The limited scope of the Directive could lead to the excluded actors compromising the overall resilience of supply chains, exposing them to cyberattacks by being the weakest, unregulated link.

The second issue regards the harmonisation of cybersecurity measures at the national and European level, which, if not aligned, could damage all market players. The minimum harmonisation clause regarding OESs, which allows Member States to adopt measures that may be stricter than those set forth in the Directive, coupled with the diverse cyber maturity of Member States and their reluctance to publicly acknowledge cyber preparedness, bears the risk of legal fragmentation in the EU.

The issue of harmonisation may have far-reaching international consequences. For instance, if there are significant differences in regulatory regimes between the EU and the United States, it may result in global problems with harmonisation, consistency and collaboration, especially when it comes to multinational organisations operating under multiple jurisdictional regimes.

Third, with respect to incidents' notification requirements, risks related to potential reputational damage and the resulting consumers' loss of confidence should be better addressed in order to avoid lacklustre implementation of the obligations of the Directive by affected companies. Criticism has also been raised as the Directive does not specify obligations to notify citizens of data security breaches. While market operators are obliged to notify attacks, there is no obligation to make data breaches public. The Directive should better specify under which circumstances does the notification of data breaches to the public constitute public interest under Article 16(7). Similar to this issue, the lack of a vulnerability equity process has been signalled as disincentivising intelligence and law enforcement agencies to disclose zero-day vulnerabilities. Under the current NIS Directive, lessons learned from incident-root causes analyses are limited to OES and DSP organisations. Today, however, cybersecurity is characterised by growing cross-sectorial risks and circular dependencies among critical sectors. More focus is required within the NIS Directive on improving cross-sector resilience and understanding dependencies. Sharing lessons learned across both public and private sectors should be incentivised. Similarly, possible avenues for boosting information-sharing on relevant information other than lessons learned, such vulnerabilities and threat intelligence, should be more thoroughly explored.

These issues will be discussed and analysed during the review of the NIS Directive, which will take place in the fourth quarter of 2020, as outlined in the European Commission Work Programme 2020 and the EU recovery plan. The review will entail the assessment of the Directive's legal and policy framework, and an evaluation of new policy measures with the aim to further strengthen cybersecurity in the Union.

For the review of the NIS Directive, the European Institutions, Member States and stakeholders are called once again to step up their efforts to ensure a high common level of security of network and information systems, and in light of the changes to societal, political, technological and market conditions over the past five years, to welcome the appropriate changes regarding how to achieve this goal.

Nevertheless, many questions remain. What will the review of the NIS Directive entail? Will the scope of the Directive be broadened to make more resilient the European cyber ecosystem? Will the selection and regulation of DSPs and OESs be revisited? Will the incident notification process be optimised? Indeed, these questions must be addressed during the evaluation of the Directive and the identification of new policy concepts in order to increase the cybersecurity maturity level and capabilities of Member States, break information silos, and build more harmonised response actions towards cybersecurity threats.