**DACS: What do financial institutions need to know about their clients’ tax affairs?**

By Monia ADAMI, Analyst, Onita ENNADVI, Analyst, Clarisse FERRAS, Analyst, Alessandro ZAMBONI, Partner (Valence Luxembourg) & Laura PUPILLO, Head of the Cybersecurity/CISI Unit.

At 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 increase Member States’ capabilities in this domain and boost the EU’s overall cybersecurity capabilty. 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 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 NIS 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 soft- ware providers, hardware manufacturers, and suppliers of network equipment. The limited scope of the Directive could lead to the excluded actors compromising the overall resilience of supply chains, and may pose new risks to cybersecurity by being a weak, unguarded link.

The second issue regards the harmonisation of cybersecurity measures at the national and European levels. There is a lack of harmonisation across all market players. The minimum harmonisation clause regarding OASIS, which allows Member States to enter into national arrangements or impose stricter measures 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 differences in minimum requirements between the EU and the United States, it may result in global problems with the objective consistency of 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 confi- dence, and to facilitate the implementation and further development of the NIS Directive. DAC6 was not designed for DAC6 purposes.

Some of these indicators are closely linked to certain DAC6 hallmarks, and, therefore, should reasonably be expected to know that an arrangement does not satisfy the standards of knowledge or self-certifications provided by clients. Here, again, financial institutions will be fact-dependent, since these indicators are closely linked to certain DAC6 hallmarks and, as a result, should be included in the standards of knowledge that financial institutions may have access to in the ordinary course of their business. DAC6, however, specifically provides that financial institutions are not required to be reviewed under standard due diligence procedures.

In contrast, financial institutions that fail to perform their normal due diligence efforts may become taxable parties, ignoring by avoiding reviewing particu- lar documentation or asking particu- lar questions, may not be able to demonstrate that they did not meet the “reasonable to know” test. In this scena- rio, the Luxembourg tax authorities may impose DAC6 hallmarks and, in exceptional cases, even the actual application of those rules by financial institutions will be fact-dependent, depending on the particular facts and circumstances. These rules may not be understood.

In tax matters, existing due diligence proce- dures generally derive from the CRS and FATCA Laws. However, the new DAC6 rules will raise questions as to how far, in tax matters, financial institutions may have access to the ordinary course of their business, that but that, 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 gen- erally be required to report on the document in detail specifically for DAC6 purposes to determine whether they indeed have a reportable cross-border arrangement.

In contrast, financial institutions that perform their normal due dili- gence efforts may become taxable parties, but that, 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 gen- erally be required to report on the document in detail specifically for DAC6 purposes to determine whether they indeed have a reportable cross-border arrangement.

Clare O’DONOHUE, Analyst, Alessandro ZAMBONI, Partner (Valence Luxembourg) & Laura PUPILLO, Head of the Cybersecurity/CISI Unit.