

Luxembourg's new IBAN register: increased obligations for entities offering accounts and safe deposit boxes seem straightforward, assuming your data is under control



Michael Schweiger

Partner

michael.schweiger@loyensloeff.com

In line with the requirements of the 5th Anti-Money Laundering Directive, Luxembourg has introduced a centralized IBAN and safe-deposit box register. This creates new obligations for entities providing accounts and safe deposit boxes, such as banks, payment institutions, and electronic money institutions which requires them to collect basic client data.

Simple, right?

That depends on how these institutions manage their data today and whether or not they outsource or are part of a larger, international group structure. The new requirements impose yet another data collection exercise with yet a different data set requirement. For entities which need to comply with Luxembourg's new IBAN register this could mean significant IT and operations involvement to ensure compliance. It will likely also trigger increased data hygiene during client onboarding and require better management of inactive accounts.

The key to managing the potentially burdensome cost of these initiatives is to invest appropriately and manage data intelligently.

What are the new requirements?

The law of 25 March 2020 establishing a centralized electronic data research system with respect to payment accounts and bank accounts identified by an IBAN number as well as safe deposit boxes held by credit institutions in Luxembourg (the Law) introduces a centralised database, to be put in place by the Commission de Surveillance du Secteur Financier (CSSF), allowing the identification of any person that has a payment account, a bank account or a safe deposit box. Although the CSSF has the obligation to create this database, it is for the relevant market players to gather all relevant information and make it available to the CSSF.

The Law applies to “professionals” which are:

- persons established in Luxembourg, including branches of foreign institutions, offering payment accounts or bank accounts identified by an IBAN number (together, Accounts); and
- credit institutions (within the meaning of the Financial Sector Law¹, and including Luxembourg branches of Luxembourg or foreign credit institutions) holding safe deposit boxes in Luxembourg (together, the Professionals).

This covers, for instance, credit institutions, electronic money institutions, and payment institutions.

Professionals must gather information about all their client accounts

Each Professional must put in place a data file allowing the identification of any natural or legal person that holds or controls an Account or a safe deposit box with such Professional (the Data File).

The Data File must contain the following information:

- the data relating to the holder of a client account and of each person acting on behalf of the client, including the name and all other information required to identify a client under the AML Law²;
- the data relating to the ultimate beneficial owner (UBO) of the client Account, including the name and all other information required to identify the UBO under the AML Law;
- the data relating to the Account itself, including the IBAN number and the date of opening and, where relevant, closing of the Account; and
- the data relating to the safe deposit box, including the name of the box holder (lessee), all other information required to identify the client/lessee under the AML Law, and the length of the lease.

Presumably, all Professionals already have all of this data as they are required to collect it for various other purposes under different legal regimes. The challenge for some will be to collect this data in respect of a particular client, which may be stored within multiple files, departments, and IT systems. Similarly, the accuracy of the data will also be an issue.

Different legal requirements mean different data refresh cycles.

The data must be adequate, exact, and kept up to date at all times. Professionals are encouraged to set up a process to feed new account openings and account closures into the Data File, and to update the Data File whenever client data changes – for instance as part of a periodic customer due diligence exercise.

Re-thinking data management

For certain Professionals, this exercise will seem all too familiar. Much of 2019 was spent ensuring compliance with the Luxembourg UBO Register requirements. Before that, 2018 was devoted to ensuring client and counterparty lists were accurate and to mapping all data flows ahead of Europe's data protection regulation: GDPR. All of these regulatory projects require cooperation between various stakeholders, such as the AML department, operations, the data protection team, the IT team, and the compliance function. There is also an impact on clients in terms of the number of requests they receive for different information. Many Professionals seek assistance from consultants to help them reorganise high volumes of data to meet each individual compliance requirement, at a cost.

Given this experience, it is time for institutions in the financial sector to begin to re-think data management if not done so already. Historically, each initiative is funded as an isolated project and it is often difficult to obtain investment for longer-term data management.

Luxembourg's IBAN register is the latest example of why longer-term investment makes sense.

Where client data is stored on multiple systems or within a larger financial group, the previous data collection exercises all confirm that it is critical for client data to be accessible on a legal entity and jurisdictional basis. See "An intelligent approach to client data" below.

It should be noted that according to the Law, the CSSF will define the structure and detail of the data to be included in the Data File. Although this information is not yet available as of the date of this publication, Professionals should start organising their data now.

Professionals must put in place appropriate measures to allow safe access to their Data File by the CSSF

The CSSF must have automated access to the Data File in accordance with a procedure to be

determined by the CSSF. Professionals must ensure the confidentiality of the CSSF's access to the Data File, but may not control the CSSF's access to the data.

Professionals must put in place, at their own cost, all measures required to ensure that the CSSF has permanent, automated and confidential access to the Data File. This includes:

- the acquisition and maintenance of the necessary hardware and infrastructure to ensure confidentiality;
- the maintenance of professional secrecy and protection against unauthorised access;
- the installation of a suitable telecommunication link and the participation in the closed user system; and
- the continued provision of these services via this set-up.

Again, the procedure to be determined by the CSSF should provide additional detail.

These requirements add the need for a potential IT investment on top of the data management and collection exercise required to create the Data File.

Professionals may outsource any or all of their obligations under the Law to a third party

The Law authorises Professionals to outsource the performance of one or more of their obligations to a third party.

Outsourcing may seem appealing, especially for institutions which do not have capacity for another regulatory project, but will not solve the underlying data management issue.

The data required for the Data File will still need to be located and collected from various sources within the organisation.

Such outsourcing requires the signing of a service contract and shall be made in accordance with Article 41(2bis) of the Financial Sector Law or Article 30(2bis) of the Payment Services Law³, as applicable. These two articles are specific to the professional secrecy obligation that Professionals are subject to. Where Professionals choose to outsource certain of their obligations under the Law (for instance the creation of the Data File) to a third party service provider, client data would be transmitted to such service provider, which in principle creates an issue from a professional secrecy perspective. Article 41(2bis) of the Financial Sector Law or Article 30(2bis) of the Payment Services Law however state that the professional secrecy requirement does not apply in an outsourcing scenario if the clients have accepted:

- the outsourcing itself (in accordance with applicable law or in accordance with the information arrangements previously agreed between the parties, which could for instance be outsourcing notification arrangements agreed by clients when signing and accepting a Professional's general terms and conditions)
- the type of information to be transmitted to the service provider and

- the country where the service provider is established (and where the client information would be transferred).
- Professionals should therefore review their existing client consent arrangements or, alternatively, make sure to obtain appropriate consent prior to outsourcing their obligations under the Law. The relevant delegate must either be subject to professional secrecy obligations itself or be bound by a confidentiality agreement to be entered into with the Professional.

Any general outsourcing requirements under applicable laws, regulations and CSSF circulars (such as Circular 12/552 for the banking sector) must also be complied with.

Professionals remain liable for the performance of their obligations under the Law.

Data retention

Data contained in the Data File must be retained in accordance with the provisions of the AML Law, meaning for a period of 5 years following the end of the business relationship with the relevant client. Professionals should build this into their data retention framework.

Supervision and sanctions

The Law gives the CSSF a number of surveillance and investigative powers in order to ensure compliance, which include the right to access any document or data, to request information, to perform on-site inspections and investigations, including at the premises of service providers to which the Professionals have outsourced their obligations, and the right to force Professionals or their delegates to cease any practice that is contrary to the Law and to force Professionals to comply with their obligations to set up the Data File. In cases of non-compliance, the CSSF may order Professionals and their delegates to pay a daily penalty to force them to comply.

The CSSF may also impose administrative penalties, in particular where Professionals do not comply with their obligations to put in place the Data File, to keep the data up to date and accurate, to ensure access for the CSSF or to ensure the confidentiality of the CSSF's access to the Data File. These sanctions include warnings, reprimands, a public declaration specifying the identity of the person(s) responsible for the breach and the nature of the breach, and administrative fines of up to EUR 1,250,000 or twice the amount of the benefit derived from the breach of the Law, where such benefit can be determined. The CSSF may publish the sanction(s) and it is important to bear in mind that the sanctions can be pronounced against the Professionals but also against the members of their management, their de facto managers or any other person responsible for the breach.

An intelligent approach to client data

Depending on how your data is structured and your operating context, it may be worthwhile to

conduct a data-mapping exercise in order to visualise at which points in your organisation data is being collected and where it is being channelled and stored. This is often only done in the context of specific regulatory projects (such as the IBAN register) by compliance teams and the findings are not shown to those who innovate commercial strategies. Professionals should consider the potential value in understanding the data.

In parallel, Professionals should document which types of data they collect, for which purpose and how it is documented, together with the associated legal basis, as well as the relevant data retention periods applicable to each data set (which may vary as different legal requirements impose different retention requirements) and the applicable or self-imposed refresh cycles (for instance, different periodicities may apply for the updating of KYC data depending on the risk profile assigned to any particular client).

There is potential to transform these tasks from mere regulatory compliance exercises to a powerful data tool which supports new products and services.

There is an opportunity to engage with clients about core priorities, instead of validating data sets with them.

If you are interested in understanding how to comply with Luxembourg's new IBAN register requirements or learn more about how to better manage data for this and other similar regulatory projects, please do not hesitate to contact us.

1Law of 5 April 1993 on the financial sector, as amended

2Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended

3Law of 10 November 2009 on payment services, as amended