What legal framework for your APIs in the financial sector?

Application programming interfaces (APIs) already exist for years. Until recently, financial institutions however rarely published APIs for consumption by third parties. Things are however changing. The 2nd Payment Services Directive (PSD2) as well as neo-banks and FinTechs turned APIs into a must have. Technical and business aspects come first in mind when designing an API implementation project. Legal aspects should nevertheless not be forgotten, these tools being a showcase of your company.

Application Programming Interface

APIs can be defined as "*the calls, subroutines, or software interrupts that comprise a documented interface so that an application program can use the services and functions of another application, operating system, network operating system, driver, or other lower-level software program*" (Shnier, 1996). APIs are blocks which may be assembled by developers to build and enrich applications by extending their potential to be integrated in or to work with other ones. As an example, a crowdfunding website which has to perform onboarding measures on a very large number of investors, can decide to use a character recognition API to extract the data from the identification documents uploaded in order to speed up the process and reduce the risk of error. Once the data extracted, the crowdfunding website can perform checks on the investor's data based on sanctions screening or Politically Exposed Persons (PEP) APIs.

When the API provider intends (or has) to publicly promote its APIs, the latter are usually published on dedicated portals and identified by a logo which is either the company's sign or a product dedicated logo. To ease the use and the integration of the API, documentation is published containing information such as how authentication is performed or providing example responses. Developers can usually test the API in a so-called "Sandbox" environment before being granted access to production environment. Once access to production is granted, developers can access to the requested information which might contain different kind of data, including personal data.

Each of the steps of the API product implementation project, from the idea, its realization to its promotion imply to consider the applicable legal framework from the start, in particular for financial institutions.

Applicable legal framework

APIs traditionally have been perceived in the IT sector as a tool of collaboration and interoperability so that the question as to the IP (and, more particularly, copyright) protection rather relates to the interfaced software applications and focusses much less on the APIs which enable such interface. The famous Oracle / Google case in the US about the use of Oracle's Java APIs in the earlier versions of the Android running on smartphones which has been launched in 2010 and is still pending, has renewed the interest in the question.

In the EU, the Court of justice of the EU (CJEU) had the opportunity to shed its light on the question in 2012 in relation to the SAS programming language, which is used in SAS APIs and intended to enable users to write and run applications on the basis of the SAS System which is famous for statistical analysis. WPL, another software company, created an alternative API using the same SAS language and format but did not copy any (source) code lines of SAS' API. Indeed, generally speaking, an API comprises a list of commands that an application A can use to access functionality in an application B. It includes the specific format in which the first application should give those commands to the second one and also is built on a specific programming language (after all if two applications should «talk» to each other, they have to speak the same language).

The CJEU held that the special copyright that is foreseen under EU law for computer programmes only covers the concrete expression of a functionality under the form of «code», it being understood that such expression is «original» in the sense that it is the author's own intellectual creation (which must be proven by the author or the right holder). The functionality itself as well as the format or programming language (which often consists of very common and simple words) fall together with the underpinning idea of the computer programme and do not enjoy protection as such. Accompanying logos and manuals, however, can nevertheless enjoy protection under general copyright law (and thus not under the specific protection for computer programmes). In the SAS case WPL did not take over any source code so that there was no copyright infringement with exception to the copying of parts of the SAS' manual.

This being said and contrary to the impression that may exist following the SAS case, APIs also do contain lines of code. In fact, in principle they contain so-called «libraries», i.e., prewritten code implementing a series of related functions on the basis of well-defined inputs, and on the basis of the above SAS judgment of the CJEU, those are in fact likely to be copyright protected so that the rights holders have the exclusive right to determine if they can be deployed and under which licensing terms. These will depend of course on the API monetization model (see below).

Now that APIs are copyright protected, the question arises as to whether API benefit from some exception. There is no general «API» defence available under EU and Luxembourg copyright law and the «interoperability» exception under EU copyright law will often not apply neither. The latter exception allows to reproduce code without the consent of the rights' holder if that is indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program A with a program B which requires that the latter program B is duly licensed to the person seeking the interoperability and the information necessary to achieve interoperability has not been readily available (in the case of APIs such information is often readily available).

In addition to the protection of the API itself, the API might comprise personal data flows triggering the application of personal data protection rules and, in the financial sector, professional secrecy rules. The use of APIs gives, in some use cases, access to databases the content of which may be protected by *sui generis* database protection.

In addition to this "general" framework, specific rules (will) frame the use of APIs in the financial sector. The 2nd Payment Services Directive (PSD2) has indeed been opening the door of "Open Banking" whereby financial institutions providing access to payment accounts online are obliged by law to enable so-called third-party providers (TPPs) to retrieve payment account information and/or initiate payments through APIs for those customers that have consented thereto. PSD2 was a first step and the European Commission is currently working on its revision as well as on the extension of its scope to other categories of data and eventually also to other financial institutions such as insurance companies or investment firms (cf. Agefi December 2020, A European Open Finance Framework by 2024). In that particular context (PSD2), it is clear that the relevant financial institutions, even when they could enjoy IP protection, are not entitled to implement licensing and other terms that would qualify as an obstacle. There is thus a protective and supportive legal framework in place to foster the development of APIs and the value they deliver and thus enabling the development of a large variety of use cases.

API products business models and use cases

There exist three main categories of APIs when it comes to their publicity: the first are "public APIs", the second are "partner APIs" and the third are "private" ones. Our focus will be on the two first categories as they involve the consumption of the API by a third party and thus a higher risk from a legal point of view. In the case of public APIs, consumers may be everyone whereas for partner APIs the existence of a prior relationship / approval and usually a specific contract are necessary.

To illustrate these categories in the financial sector, one may for instance mention currency exchange rate, IBAN validation or branch location APIs which are usually provided as "public APIs", whereas loan, insurance quote or customer identity verification APIs are usually "partner APIs". The decision to publish an API as "public" or "partner" is intrinsically linked to the underlying product business model. For instance, where the consumption of the API helps the provider promoting its services whatever the channel (i.e. the API consumer), the API provider will make the choice of having a public API. When the API is published with the same purpose but the provider wishes to select who may promote its services, for reputation or commercial reasons, a partner API will be more appropriate.

The determination of the targeted API consumers also raises the question of the API monetization. Depending on the service at stake, providers may indeed decide to provide access to their API(s) for free (e.g. branch location), against a fee per (type of) call (e.g. sanctions or PEP screening, identity verification) or against a fee covering a larger set of services (e.g. a KYC service provider offering the API as one of tools put at the disposal of the end client). The monetization chosen by the API provider has to be transparent towards the API consumer and will need to be reflected in the applicable contractual framework. These developments show that APIs are more and more seen as a product, with a dedicated strategy, rather than a sole technical tool. In addition to the applicable legal framework, API providers have to contractually frame their relationships in order to protect these assets.

Contractual framework

APIs will often be embedded in a larger service offering, e.g., the access to the database, so that the use of any APIs must be addressed in that framework. As APIs (at least the lines of code) are most likely copyright protected, any IP licensing clauses should also cover the APIs in addition to the use of/access to any other IP protected elements, such as *sui generis* database rights which may cover the content of databases that are accessed via APIs. In the context of a «public API», normally the users consuming the APIs do not conclude a specific agreement but the API provider will publish terms and conditions that will set forth any restrictions in relation to the use of the APIs. Where the service provided through the API qualifies as a (material) outsourcing in the financial sector, the financial institution consuming APIs shall ensure that the T&Cs, respectively the agreement, entered into complies with the Luxembourg and EU supervisors' requirements.

As indicated above, very often an API will facilitate the access to data in a particular application and lead to a transfer of data towards another application (and, as the case may be, vice versa). In some cases this may include a transfer of *personal* data in which event such transfer must abide with applicable data protection rules and the conclusion of a data transfer agreement may be a useful tool. The service provider offering an API to access its service, e.g., a database, must therefore have informed the persons concerned whose details figure in the database, and also have a basis to lawfully transfer those data. Financial institutions providing TPPs access to their customers' accounts must do so by law, so that «compliance with a legal obligation» will be the basis of such processing.

Some service providers offering APIs can also do it in the context of a service for which they would qualify as a «data processor», processing personal data on instruction and behalf of a data controller (for example, the APIs made available by Amazon for its cloud data storage and retrieval platform, S3, are part of that service where Amazon typically acts as data processor). If so, a data processing agreement must be concluded between the service provider and the client consuming the API. This agreement must also set forth in more detail the security measures implemented by the service provider, including the security measures in the context of the deployment of the API.

Anne-Sophie MORVAN
LUXHUB
Business Development Manager

Vincent WELLENS
NautaDutilh Avocats Luxembourg S.à r.l.
Partner, Avocat à la Cour (Luxembourg) / Avocat (Bruxelles)