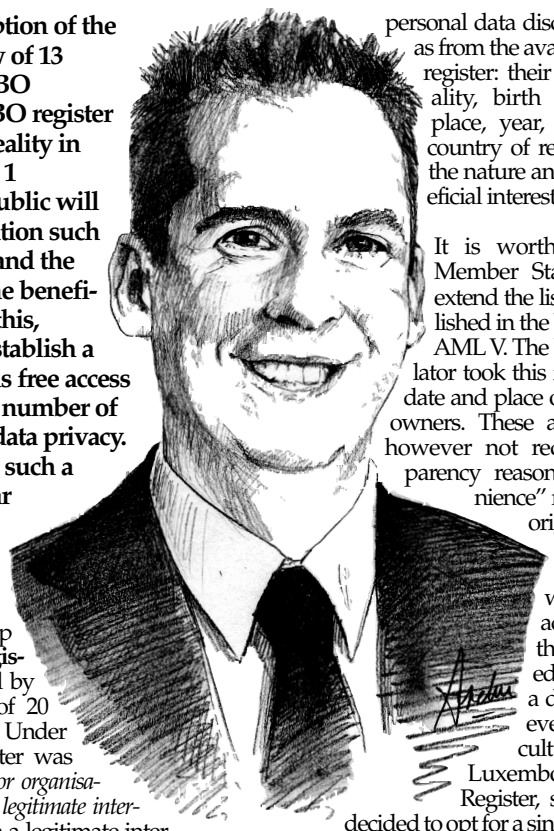
UBO register: a data privacy no man's land?

Further to the adoption of the Luxembourg Law of 13 January 2019 ("UBO Register Law"), the UBO register is about to become a reality in Luxembourg. As from 1 September 2019, the public will have access to information such as the UBOs' identity and the nature and extent of the beneficial interest held, and this, without necessity to establish a legitimate interest. This free access to private data raises a number of questions in terms of data privacy. The proportionality of such a measure is in particular very debated.



Legislative context

The beneficial ownership central register ("**UBO register**") has been introduced by the Directive 2015/849 of 20 May 2015 ("**AML IV**"). Under AML IV, the UBO register was accessible to "*any person or organisation that can demonstrate a legitimate interest*". The necessity of such a legitimate interest did however disappear in Directive 2018/843 of 30 May 2018 ("**AML V**").

When the Ministry of Justice introduced the UBO register bill of law on 16 January 2018 (i.e. more than 6 months after the AML IV transposition deadline), AML V was not yet adopted. No mention of a general public access was thus contained in the bill. Six months later, when AML V entered into force, the bill of law was still under discussion in the Luxembourg parliament. Hence, the Ministry of Justice decided to kill two birds with one stone and amended the bill of law to reflect the new AML V UBO register access rules.

The "public" data

As from 1 September 2019, the public shall have free access to a certain number of information concerning the beneficial owners of entities registered with the Luxembourg Trade and Companies Register. As a reminder, the beneficial owner is any natural person who ultimately owns or controls the customer or any natural person on whose behalf a transaction or activity is being conducted.

In the case of corporate entities, the threshold of 25% shareholding / ownership interest held by a natural person is an indication of direct ownership. These beneficial owners will see several of their personal data disclosed to the public as from the availability of the UBO register: their (sur)name, nationality, birth information (incl. place, year, month and date), country of residence, as well as the nature and extent of the beneficial interest held.

It is worth noting that the Member States had room to extend the list of data to be published in the UBO register under AML V. The Luxem-bourg legislator took this freedom to add the date and place of birth of beneficial owners. These additional data are however not requested for transparency reasons but for "convenience" reasons. Indeed, the original version of the bill of law provided obliged entities with a broader access to UBO's data than the access granted to the public. Such a difference was however technically difficult to handle for the Luxembourg Business Register, so that it has been decided to opt for a single set of data accessible by both the obliged entities and the public, regardless of the fact that non-necessary information would be disclosed to the public.

Such an approach raises more generally the question of proportionality of the measures at stake.

The (questionable) necessity of an access by the public at large

The public disclosure of UBO's personal data constitutes a limitation of the UBO's right to data privacy. Such a limitation shall comply with the proportionality principle, i.e. be necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

In order to comply with this principle, the AML V's recitals put forward several justifications. Hence, the public disclosure of UBO's information would in particular (i) allow "*greater scrutiny of information by civil society, including by the press or civil society organisations*", (ii) contribute "*to preserving trust in the integrity of business transactions and of the financial system*" and (iii) contribute "*to combating the misuse of corporate and other legal entities and legal arrangements for the purposes of money laundering or terrorist financing, both by helping investigations and through reputational effects, given that anyone who could enter into transactions is aware of the identity of the beneficial owners*".

These justifications of the European legislator are thus mainly relating to the confidence from investors and the general public in financial markets on the one hand, and the better performance of measures to fight against money laundering and terrorist financing on the other hand.

The European Court of Justice (ECJ) considers that the fight against international terrorism and serious crime constitutes an objective of general interest. However, the measures implemented should not exceed the limits of what is appropriate and necessary to achieve this objective. In the case *Digital Rights Ireland* for instance, the ECJ annulled Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, due to the lack of proportionality of the measures at stake. The main concerns of the ECJ were the generality of the data retention measure (which was even applicable to persons without any link with a serious crime or persons subject to professional secrecy) and the lack of safeguards to ensure the effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data.

In the light of this *Digital Rights Ireland* case, it is interesting to note that the disclosure of UBO data in the public applies to any beneficial owner, regardless of any identified risk (whereas the AML systematic is based on a risk-based-approach). Such disclosure is motivated by the intention of the EU legislator to come to a greater transparency generally speaking, which goes well beyond the fight against anti-money laundering and terrorist financing. Therefore, it very questionable whether the public disclosure of UBO data is still in line with and limited to the purpose of the AML directives.

This impression is further reinforced by the fact that AML V requires the persons who wish to access the UBO information of trusts and similar legal arrangements to establish the existence of a legitimate interest. Therefore, it does not seem clear from a data privacy perspective why such a legitimate interest would be less necessary within the context of the UBO register.

Furthermore, in order to limit the impact of this measure, the legislator must in any event implement adequate safeguards.

The (insufficient) safeguards

AML V enables the Member States to provide for an exemption from such a public access to all or part of the information on the beneficial ownership. The Luxembourg legislator has implemented this exemption in the UBO Register Law. It is hence possible for registered entities and beneficial owners, on a case-by-case basis and in exceptional circumstances, to request a limitation of the public access to the information. In order to have the information exclusively available to national authorities, credit institutions, financial institutions, bailiffs (*huissiers*) and notaries acting in their public officer capacity, it shall be established that a public access would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable.

This safeguard is welcomed, however it does not seem sufficient as it may only be requested in "*exceptional circumstances*".

As additional mitigating measures, the Luxembourg Data Protection Commission (CNPD) *inter alia* suggested to subject access to the UBO register to the fulfilment of security measures, to an online registration as well as to the payment of a fee. In addition thereto, the CNPD recommended the implementation of a system enabling the tracking of the persons consulting the register. The Luxembourg legislator did however not follow these suggestions in the UBO Register Law.

In its opinion on the project of Grand-Ducal Regulation implementing the UBO Register Law, the CNPD reiterated the importance of such measures and pointed out the risk of lack of compliance of the Luxembourg UBO register with the GDPR. The CNPD hence considers that, in its current version, the UBO register is not limited to what is strictly appropriate and necessary for the purposes at stake and does thus not accurately transpose AML IV as amended by AML V.

The Grand-Ducal Regulation implementing the UBO Register Law will thus play a key role. In the event the Ministry of Justice does not take this last opportunity to implement additional safeguards, any beneficial owner whose personal data are publicly disclose in the UBO register could challenge the legal validity of the UBO Register Law in the light of the GDPR and has chances to succeed.

If you want to learn more on the data protection rules applied to the AML, we will give a presentation on the topic "GDPR & AML" at the Anti-Money Laundering event organised by CREO on 28 February 2019 (https://creobis.eu/).

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

Anne-Sophie MORVAN
NautaDutilh Avocats Luxembourg S.à r.l.
Senior Associate
Avocate à la Cour (Paris & Luxembourg)

2019 sera l'année de la résilience digitale

Selon les dernières prédictions de Riverbed, les talents en data sciences vont rester rares en 2019 et la demande en spécialistes de la discipline comme en analytique des données va continuer à s'accentuer. Alors que les Data Lakes deviennent toujours plus volumineux, la difficulté à gérer et exploiter ces énormes quantités de données va devenir stratégique dans les opérations des entreprises au point de devenir la principale préoccupation dans le développement et la planification de l'activité.

Au cours de l'année à venir, les entreprises vont prendre pleinement conscience de l'impact des données sur leur réussite d'ensemble et sur la compréhension de leurs clients. Des technologies telles que l'intelligence artificielle (IA) et le Machine Learning (ML) seront capables d'apporter des informations exploitables, alors que l'analytique jouera un rôle capital pour les entreprises à la recherche d'un avantage concurrentiel sur un marché compétitif et attachées à répondre à des clients digitaux aux exigences accrues. La faculté à tirer parti de ces informations et à analyser les données va devenir inestimable.

Ces nouvelles technologies soulèvent un autre défi pour les managers : comment éduquer l'entreprise à l'analytique des données. Au-delà des compétences techniques nécessaires, il faut des compétences métier pour comprendre les implications en termes de technologie requise dans les opérations, ce qu'elle peut faire et comment l'implémenter pour atteindre une performance maximale.

Pour se doter de telles expertises, les entreprises peuvent faire monter en compétence leurs employés à condition que le retour sur investissement soit vraiment prometteur. Il est toutefois plus simple pour les entreprises de recruter à l'extérieur, aussi la bataille de l'analytique des données a de grandes chances de s'intensifier l'année prochaine.

Suivi de la performance

Les entreprises commencent seulement à cerner combien il est important de comprendre l'empreinte digitale de leurs clients et de leurs prospects. Aussi, en 2019, les data sciences et l'analytique des données vont devenir les principaux moteurs de la réussite avec les clients. Les cas d'usage de l'IA et du ML vont se multiplier et rassembler un volume conséquent de données qui va exiger une compréhension fine de ces applications. La compréhension superficielle que l'on constate pour le moment empêche les entreprises d'offrir à leurs clients une expérience vraiment cohérente et optimale. Ce ne sera plus le cas l'année prochaine : les techniques de data science et l'analytique prédictive vont davantage se généraliser afin de mettre pleinement à profit les technologies en essor comme le ML.

Des entreprises tournées vers leurs clients

Au départ, la transformation digitale se concentrait sur l'adoption de solutions de nouvelle technologie. Toutefois, dans l'année à venir, les choses vont commencer à évoluer. Alors que les data sciences et l'analytique des données se développent, les clients se mettent à demander et à attendre des services toujours plus personnalisés. De l'offre packagée d'un opérateur de télécoms à un crédit, des vêtements ou de simples articles d'épicerie, les clients digitaux exigent que les biens et les services soient taillés sur-mesure en fonction de leurs goûts et de leur expérience personnelle. L'année prochaine, les entreprises capables de proposer à leurs clients une expérience sur-mesure en utilisant l'analytique avancée des données, l'IA et le ML en tireront d'importants bénéfices. L'usage de nouvelles technologies comme la blockchain va également aider à élever le niveau de personnalisation.

Internet des objets

L'année qui arrive verra des changements considérables de l'IoT, car les fabricants vont continuer à améliorer la sécurité intégrée tant attendue qu'ils ont auparavant sacrifiée pour maintenir des coûts de production bas. Le grand public n'ayant pas pleinement conscience des risques de sécurité associés aux objets connectés, l'adoption de l'IoT ne va pas massivement diminuer, même si les nouvelles mesures de sécurité de l'Internet des objets fait grimper les prix. En parallèle, les fuites de données très médiatisées et l'implémentation du RGPD continueront à créer un changement d'attitude envers l'IoT. Comme un coup de semonce, il va y avoir une prise de conscience qu'aucune solution rapide ne peut combler les brèches de sécurité. En comprenant qu'éviter ces brèches au niveau de l'IoT est un impératif de taille et que le poids des preuves exigées par le RGPD repose sur leurs épaules, la plupart des entreprises vont tenter de limiter le nombre d'amendes potentielles.

D'un point de vue positif, les défis de l'Internet des objets nécessitent des solutions innovantes et peuvent aboutir à de nouveaux développements qui aideront à lutter contre de futures menaces et donneront un coup d'accélérateur à d'autres technologies telles que le Machine Lerning.

Incidents et résilience digitale

Les pannes continueront de sévir dans tous les secteurs, en particulier dans la finance et la vente au détail. Les entreprises ont besoin d'avoir davantage de visibilité. En effet, elles vont vouloir une seule source d'informations fiables sur toute leur architecture logicielle. Les outils de visibilité digitale peuvent livrer l'équivalent d'un diagnostic IRM de tout ou partie de l'architecture logicielle et détecter potentiellement les vulnérabilités avant qu'un incident ne survienne. Une fois leur visibilité d'ensemble améliorée, les entreprises pourront prendre des mesures plus pertinentes pour renforcer leur résilience de manière proactive et s'assurer que les clients pâtiront moins de pannes informatiques l'année prochaine qu'en 2018.

Secteur financier : prise de distance avec les systèmes hérités

Le secteur financier a connu des temps difficiles avec sa transformation digitale. En 2018, les institutions financières se sont retrouvées noyées dans les différentes couches logicielles héritées, si bien qu'apporter des changements à leur infrastructure relevait de l'opération délicate et onéreuse, rarement sans risque. Les entreprises de la finance doivent s'émanciper de leurs anciens systèmes et adopter une infrastructure plus agile par le biais de partenariats avec des startups de la fintech.

En 2019, les banques et les institutions financières vont doubler leurs services digitaux et tenter de gagner en compétitivité grâce à des technologies financières très agiles. Il sera capital qu'elles offrent à leurs clients une expérience satisfaisante, sans heurt. Pour y parvenir, il leur faudra une visibilité et une performance améliorées, y compris à la périphérie du réseau. Le secteur des services financiers va devoir adopter le SD-WAN et des solutions de visibilité pour faire le suivi de la performance, commercialiser rapidement les produits et adapter les services pour absorber la transition de systèmes hérités à l'agilité.

Collaboration entre les DAF et les équipes digitales de la finance

Les équipes de la finance vont devoir faire des changements drastiques et s'adapter dans l'année qui vient. Face à l'attrait grandissant des entreprises de technologie financière auprès des clients et des talents, il faudra que les banques traditionnelles s'adaptent et gagnent en agilité. Dans ce contexte, les équipes de la finance devront développer des compétences plus pointues en analyse des données. Les data scientists vont devenir des acteurs-clés dans les équipes de la finance et l'analyse prédictive, alors que les profils spécialisés dans l'IA et le ML seront toujours plus indispensables dans ce secteur.De plus, l'adaptation des équipes de la finance restera de mise l'année qui vient et dans toutes les entreprises, les DAF s'appuieront davantage sur les données et sur les analystes au sein de leurs équipes. Par conséquent, les CIO et les DAF vont collaborer plus étroitement que jamais et les entreprises qui se seront débarrassées des données en silos remporteront les plus belles réussites.

Source : Riverbed