The forthcoming EU legal framework on Digital Operational Resilience in the financial sector:

DORA the EU Regulation

The Luxembourg rules on the use of information and communication technology ("ICT") in the finance sector, once very country-specific, will soon change significantly as the result of an EU-led initiative aimed at harmonising rules across the region.

DORA stands for "Digital Operational Resilience Act". This Act consists in an EU Regulation proposed by the European Commission in September 2020[1] as part of its digital finance package.

DORA's main objective is to provide for a single set of reinforced and overarching rules for financial entities concerning the use of ICT, particularly ICT risk management, security and business continuity, digital operation resilience testing, and contracts with ICT service providers.

A provisional agreement on DORA was reached in May 2022. The finalised text was published in June 2022.[2] At the time of writing, DORA still needs to pass two votes in the European Parliament and the European Council in order to become law. The final adoption of the regulation is expected before the end of this year.

A quick historical recap

For many years, the Luxembourg rules applicable to how regulated professionals (i.e. the Luxembourg-based financial sector professionals ("FSPs"), insurance and payment services professionals) organised and ran their IT function arguably revolved around the principles of banking secrecy[3], central administration and internal governance. This created a somewhat unique ecosystem of Luxembourg-based financial institutions having to use local ICT service providers supervised by the CSSF (referred to as "Support FSPs") for most ICT projects that required access to readable client data by the service provider.

Since 2018, a number of regulatory changes[4] have relaxed restrictions dictated by banking secrecy while at the same time reinforcing the principles of central administration and internal governance to increase the regulated professionals' business resilience. Luxembourg regulated professionals can now, subject to conditions, outsource a wide range of activities to providers located abroad, whether these providers belong to the same corporate group as the regulated professional or not. A specific regulatory framework is even in place to allow regulated professionals to outsource services using cloud-based technologies.

Another noticeable trend has been the progressive (but as yet incomplete) convergence of rules on ICT outsourcing between the Luxembourg banking, insurance and fund management industries.[5] With the entry into force of DORA, we will witness a harmonisation of the rules applicable to ICT outsourcing not only across banking, insurance and fund management but across the entire EU region. Moreover, ICT outsourcing is merely one of the areas that DORA will shake up.

DORA's extremely broad scope

DORA has an extremely broad scope. It will apply to most entities engaged in financial services, including (but not limited to) credit institutions, payment and electronic money institutions, investment firms, most insurance and reinsurance undertakings, most managers of alternative investment funds and management companies as well as ICT third-party service providers (which will include providers of cloud computing services, software, data analytics services, and data centre services) ("financial entities").[6]

DORA will apply to the use and provision of ICT services in a broad sense[7] and is not limited to outsourcing arrangements. A wide range of technology-related contracts will therefore be impacted.

Most importantly, ICT third-party service providers that are considered critical for financial entities – most likely including big tech companies providing cloud services as well as data analytics firms – will fall within the scope of DORA and its supervisory framework. These critical providers will have a number of direct legal obligations. For instance, those based in a third country that provide services to financial entities in the EU will be required to establish a subsidiary in the EU so that proper oversight can be ensured.

How DORA will fit into the existing regulatory framework

The proposed regulation seeks to codify many requirements (e.g. the reporting of major ICT-related incidents) that are currently covered, for the most part, by guidelines issued by EU and national authorities, such as the EBA or the CSSF in Luxembourg. According to some sources, the European Commission has confirmed that some guidelines will need to be amended or possibly repealed in order to reflect the requirements of DORA once its provisions enter into force.

Main changes that DORA will bring

1. Changes regarding third-party risk management

A general principle of proportionality will apply with respect to ICT third-party risk management, taking into account the scale, complexity and importance of ICT-related dependencies and risks that arise from the contractual arrangements in place with ICT third-party service providers. Financial entities will also have to:
- adopt and regularly review an ICT third-party risk strategy and maintain a register of information relating to all ICT third-party supply contracts;
- make assessments when entering into new contractual arrangements and only exclusively enter into contracts with ICT third-party service providers that comply with high, appropriate and the latest information security standards; and
- comply with various reporting obligations regarding arrangements with ICT third-party service providers.

DORA will regulate the contents of contractual arrangements concluded between ICT third-party service providers and financial entities. An additional layer of contractual provisions will be required when these arrangements relate to critical or important functions of a financial entity. Topics that will have to be addressed in the contracts include oversight of sub-outsourcing, data requirements, audit rights, termination and exit strategies.

As already mentioned, DORA's remit is significantly broader than just the outsourcing arrangements of financial entities. The latter will indeed have to review not only their outsourcing arrangements but also any other contracts in the context of which they receive digital and data services through ICT systems on an ongoing basis. As the intragroup provision of ICT services will also be covered by DORA, contracts with group entities providing ICT services to financial entities located in the EU will have to be reviewed and updated where necessary.

2. Changes in other areas

DORA is not only about dealing with ICT third-party service providers. It also:
- includes requirements on **governance and ICT risk management**. This will require financial entities to review their internal organisation to ensure that ICT risks are addressed quickly, efficiently and comprehensively. A sound and comprehensive ICT risk management framework incorporating a digital operational resilience strategy will need to be documented;
- introduces a number of rules on how to manage, classify and report **ICT-related incidents**. Financial entities will have to carefully assess how to integrate these rules into the many existing reporting requirements, which notably ensue from the General Data Protection Regulation and, for some critical regulated professionals, from the Luxembourg Act of 28 May 2019 transposing the so-called "NIS" EU Directive;
- requires most financial entities to establish, maintain and review a **digital operational resilience testing programme** under which independent parties (internal or external to the financial entities) will test ICT tools and systems. The most significant financial entities will be required to carry out advanced testing by means of threat-led penetrating testing, which will effectively mimic real life cyber-attacks; and
- sets a framework in which financial entities may **exchange cyber threat information and intelligence among themselves**.

Entry into force and action required

The current text specifies that the regulation's provisions will start to apply two years after it enters into force, which will most likely be sometime in 2024 if DORA is adopted before the end of this year. In the meantime, a draft bill complementing DORA's provisions (in particular to establish the level of fines for breaches of the regulation) should be submitted to the Luxembourg parliament.

Luxembourg regulated professionals operating in the banking, insurance and fund management industries, including Support FSPs, need to ascertain whether DORA applies to them and, if so, will have to start preparing for its implementation without undue delay.

We stress that the two-year period granted by the regulation before its provisions enter into force will not be excessive to start, run and finalise internal "DORA compliance" projects in good conditions, especially given the need to involve multiple teams (at least, the IT security, legal, compliance, risk management teams and management) and external counterparties.

Vincent WELLENS (portrait)
Avocat à la Cour (Luxembourg) / Avocat (Bruxelles)
Partner NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Lindsay KORYTKO
Avocat à la Cour / Inscrit au Barreau de Luxembourg
Senior Associate NautaDutilh Avocats Luxembourg S.à r.l.
Lindsay.Korytko@nautadutilh.com

1) Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 24 September 2020.
2) Available at https://data.consilium.europa.eu/doc/document/ST-10581-2022-INIT/en/pdf.
3) Although investment funds, management companies and alternative investment fund managers are not subject to a strict duty of professional secrecy (as opposed to some of their service providers, such as registrars and professional depositaries of financial instruments), they are nonetheless subject to a duty to keep data secure and confidential.
4) The Luxembourg Act dated 27 February 2018 implementing Regulation 2015/751/EU, the guidelines on outsourcing arrangements by the European Banking Authority ("EBA") of February 2019 (the "EBA Outsourcing Guidelines of 2019") and the recent CSSF Circular 22/806 on outsourcing arrangements (the "CSSF Outsourcing Circular").
5) The CSSF Outsourcing Circular is one example of this trend, as it extended the scope of the EBA Outsourcing Guidelines of 2019 to cover most entities in the banking industry as well as entities active in the fund management industry.
6) DORA defines "ICT third-party service providers" as undertakings providing ICT services. See Article 2 of the proposed regulation for an exhaustive list of covered financial entities.
7) DORA defines "ICT services" as "*digital and data services provided through the ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which include technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services*" (Art. 3(16)).

IMD Digital Competitiveness Ranking :

Le Grand-Duché chute

L'International Institute for Management Development (IMD) vient de publier la 6ème édition de son classement des économies les plus compétitives sur le plan digital, 3 mois après la parution de son célèbre classement de la compétitivité. Les années se suivent et ne se ressemblent pas pour le Luxembourg.

Avec un score de 76,47, en recul de 1 point par rapport à l'an passé, le pays dégringole de 8 positions cette année pour figurer à la 30ème position du classement, soit sa plus mauvaise place jamais enregistrée.

L'attribution du score global de chaque pays repose sur des critères quasi similaires aux années précédentes, à savoir une évaluation autour de 3 piliers : «Knowledge», construit autour d'indicateurs axés sur la qualité du capital humain, «Technology» pour évaluer le contexte général favorable au développement des technologies numériques et «Future Readiness», qui mesure le degré d'adoption des technologies par les gouvernements, les entreprises et la société en général. 3 piliers eux-mêmes divisés en 9 sous-facteurs comprenant 54 critères. Cette année, ce sont 63 pays qui ont été passés à la loupe.

Petit séisme parmi les premières places où l'hégémonie des Etats-Unis (2e) prend fin après 4 années. Le Danemark, non content de se hisser au sommet du célèbre classement de compétitivité de l'Institut en juin dernier récidive, devenant par la même le premier pays européen à atteindre la première place. La Suède, au 3e rang, vient compléter le podium.

La comparaison est peu flatteuse pour le Luxembourg, qui se situe dans le dernier tiers des pays dont le PIB par habitant est supérieur à 20.000€, au 20ème rang européen et seulement au 13ème rang des pays de l'Union européenne.

Les pays limitrophes, Allemagne, France et Belgique sont respectivement 19ème, 22ème et 23ème. Marqueur de compétitivité de plus en plus affirmé, il n'est pas surprenant que 8 pays du top 10 de ce World Digital Competitiveness Ranking se trouvent également dans celui du World Competitiveness Yearbook.

Le Luxembourg régresse cette année sur l'ensemble des 3 facteurs du classement. Il perd respectivement 6 et 5 places sur les piliers «Knowledge» et «Technology». Le pays chute de 11 places sur le pilier «Futur readiness», reculant à la 35ème position. Le Grand-Duché continue de disposer d'atouts importants. Le pays figure à la 7ème position sur l'aspect «main-d'œuvre étrangère hautement qualifiée», à la 10ème place pour la réussite dans l'enseignement supérieur, et se situe parmi les meilleurs quant au ratio élèves par enseignants (9ème rang). Grâce à sa place financière importante, le Luxembourg profite d'un environnement favorable aux fintechs. Il se situe en haut du classement (2ème) concernant la capitalisation boursière dans le secteur des technologies et des médias.

Après avoir été classé 8ème internet le plus rapide au monde par le site britannique Cable.co, le Luxembourg se retrouve 6ème concernant la vitesse de la bande passante internet, confirmant ainsi sa bonne position sur ce segment extrêmement important pour les usagers et les entreprises.

Le Luxembourg capitalise également sur ses forces habituelles, à savoir sa notation AAA (1ère place), le nombre d'usagers internet (5ème place) ou encore la protection des logiciels contre le piratage (4ème place). A noter la progression fulgurante du classement du pays sur la crainte de l'échec des entrepreneurs, les empêchant de développer une entreprise. Le Luxembourg fait un bond de 20 places sur ce sujet, passant de la 40ème à la 20ème place sur cet indicateur. Néanmoins, de nombreuses et fortes insuffisances empêchent le Luxembourg d'achever son projet de «Digital nation». Parmi les plus importantes, il convient de relever un investissement dans les télécommunications en pourcentage du PIB encore trop faible, situant le pays en pénultième position de ce classement, des abonnés au haut-débit mobile encore trop peu nombreux, matérialisant la critique des auteurs du rapport DESI, regrettant que la couverture 5G au Grand-Duché représente uniquement 13% du réseau (contre 66% en moyenne à l'échelle de l'UE). L'interaction en ligne entre les citoyens et le gouvernement est encore trop peu utilisée au Luxembourg (52ème place), et le pays souffre d'un manque de publications scientifiques en rapport avec le montant investi en R&D (60ème position).

Le Centre mondial de la compétitivité, centre de recherche attaché à IMD conseille aux gouvernements et au secteur privé d'investir dans les talents, la formation, l'éducation, mais aussi en R&D afin de protéger leurs infrastructures digitales contre les cyberattaques et de développer des services d'e-administration, clés pour devenir une économie digitale compétitive.

Si l'Amérique du Nord, l'Est de l'Asie présentent un haut niveau de cybersécurité, l'Europe mais aussi l'Amérique du Sud ou encore l'Asie centrale accusent un écart important entre le développement des services administratifs en ligne et leur capacité en matière de cybersécurité. Cet écart risque de rendre ces régions particulièrement vulnérables aux cyberattaques.

Rapport : https://www.cc.lu/fileadmin/user_upload/tx_ccnews/digital-ranking-2022_IMD_PDF.pdf

Source : Chambre de Commerce