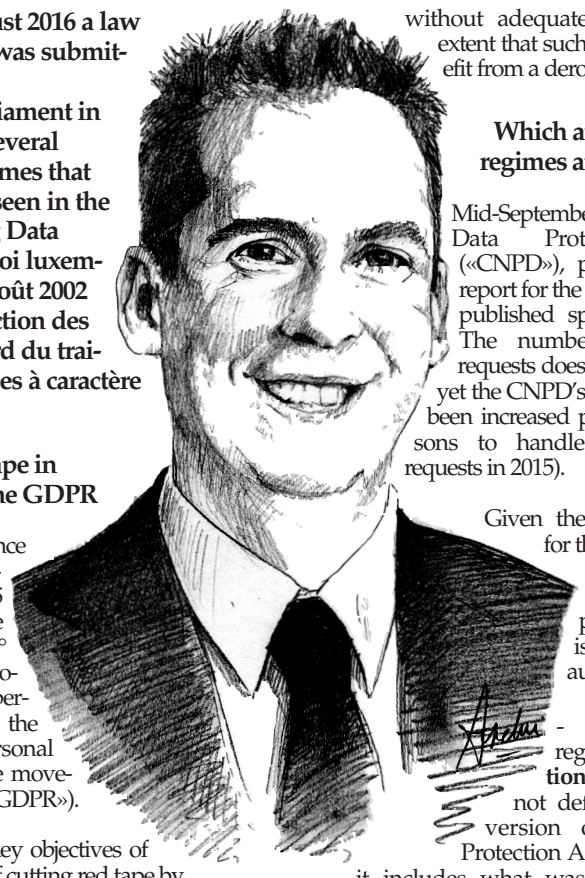
Luxembourg anticipates the GDPR:

Abolition of authorisation for several critical data processing activities and for SCC based data transfers outside the EEA/EU

On 31 August 2016 a law proposal was submitted to the Luxembourg Parliament in order to abolish several authorisation regimes that are currently foreseen in the 2002 Luxembourg Data Protection Act («Loi luxembourgeoise du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel»).



Cutting red tape in anticipation of the GDPR

This law proposal, once adopted, will anticipate the as from 25 May 2018 applicable Regulation (EU) n° 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data («GDPR»).

Indeed, one of the key objectives of the GDPR consists of cutting red tape by, amongst others, abolishing the several authorisation regimes that EU Member States are allowed to adopt under the current Data Protection Directive 95/46/EC for critical data processing activities and for data transfers to countries outside the EU/EEA without adequate protection (to the extent that such transfers do not benefit from a derogation).

Which authorisation regimes are concerned?

Mid-September, the Luxem-bourg Data Protection Authority («CNPD»), published its annual report for the year 2015. The figures published speak for themselves. The number of authorisation requests does not cease to increase, yet the CNPD's staff number has not been increased proportionally (2 persons to handle 969 authorisation requests in 2015).

Given the resulting workload for the CNPD, the competent minister decided to submit a law proposal in order to abolish the following authorisation regimes:

- The authorisation regime for **interconnection**: 'interconnection' is not defined in the current version of the 2002 Data Protection Act, but it is clear that it includes what was understood under 'interconnection' within the meaning of the initial version of the same act, *i.e.*, the correlation of data that are processed for a given purpose with data processed for another purpose and/or by another controller.

Even when the law proposal intends to abolish the authorisation requirement, interconnection of personal data remains subject to some specific rules of the 2002 Data Protection Act.

- The authorisation regime for **supervision in general and in the workplace**. 'Supervision' is defined as «*any activity which, carried out using technical instruments, consists of observing, collecting or recording in a non-occasional manner the personal data of one or more persons, concerning behaviour, movements, communications or the use of electronic computerised instruments*».

Even though the GDPR exceptionally allows EU Member States to adopt stricter data protection rules in the context of an employment relationship and thus enables Luxembourg to uphold the authorisation regime for supervision in the workplace, the authorisation requirement for this type of processing is likely to disappear in the near future.

Nonetheless, the 2002 Data Protection Act will still contain restrictions for supervision in general and the Luxembourg Labour Code for supervision in the workplace in particular (specific information requirement vis-à-vis staff delegation and individual employees, etc.).

- The authorisation regime for **credit and solvency related personal data** processing carried out by controllers which are not financial or insurance service providers. The abolition of this authorisation regime will be welcomed by those undertakings that acquire distressed consumer debt from foreign banks via Luxembourg special purpose vehicles and which are likely to be subject to the said authorisation regime in the current state of things.

- Finally, save in some exceptional circumstances foreseen by the Luxembourg 2002 Data Protection Act (e.g. data subject consent, transfer necessary for the performance of a contract, etc.), **the transfer of data to non-EU/EEA countries** without an adequate level of data protection is prohibited unless adequate safeguards (such as the use of the so-called standard contractual clauses («SCC») issued by the European Commission) are provided and the CNPD has authorised the transfer. The law proposal, if adopted, will not subject transfers to non-EU/EEA countries to an authorisation anymore if they are based on SCCs.

The processing activities concerned are not subject to authorisation but will prior to 25 May 2018 still need to be notified

The initiative to cut red tape by abolishing some authorisation regimes, whose effectiveness was regularly called into doubt, must be welcomed and is fully in line with one of the principal GDPR objectives.

However, it is very likely that most of these types of data processing will nevertheless remain subject to a prior notification to the CNPD, so that the undertakings concerned will still have to deal with paperwork. On a positive note, this notification requirement will in any event disappear on 25 May 2018, the date of application of the GDPR.

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

Anne-Sophie MORVAN
Avocat au Barreau de Paris (Liste IV)
Associate NautaDutilh Avocats Luxembourg S.à r.l.
annesophie.morvan@nautadutilh.com

Conférence SESAMm

« Gestion d'actifs & Big Data : nouveaux moteurs de performance »

SESAMm, jeune start-up Fintech des écosystèmes français et luxembourgeois, a réussi son pari : réunir au Luxembourg des acteurs influents et connus du monde de la finance. C'est dans le cadre du lancement officiel de ses activités au Luxembourg que la start-up a organisé cette grande conférence, premier événement d'envergure pour SESAMm. Son but ? Réussir le challenge de réunir des décisionnaires autour d'une même thématique qui devient de plus en plus centrale pour les acteurs de la finance : «Gestion d'actifs & Big Data : nouveaux moteurs de performance».

137 invités soigneusement sélectionnés, provenant d'un panel varié de l'Europe et d'outre Atlantique, ont pu assister à cette conférence. Celle-ci s'est déroulée au siège de la BGL BNP PARIBAS, situé dans le quartier d'affaire au Kirchberg dans la ville de Luxembourg.

L'objectif de la conférence était de sensibiliser les acteurs de la finance et plus particulièrement ceux de la gestion d'actif. La problématique centrale était focalisée sur l'utilisation de nouvelles solutions innovantes apportées par le Big Data et l'intelligence artificielle au service de la finance de marché, plus précisément dans le domaine du trading systématique. Face aux au caractère novateur et précurseur des possibilités offertes par le Big Data, ses applications pour les acteurs de la finance ne sont pas toujours évidentes à comprendre. Les enjeux principaux du Big Data résident ici dans la détermination des besoins, des nouvelles opportunités et surtout des applications concrètes pour les besoins des professionnels du monde de la finance. L'objectif était donc de lever ces interrogations à travers l'étude de cas concrets. Par l'intervention d'experts de renom, le public a pu observer les enjeux stratégiques communs d'IBM et de SESAMm dans leurs thématiques respectives de recherche et développement avec pour vocation de développer de nouveaux outils «Smart Big Data». Parmi ces experts se trouvait Erick Brethenoux, directeur mondial de la stratégie au sein d'IBM Watson Analytics, le programme informatique d'intelligence artificielle conçu par IBM. Erick Brethenoux occupe également le poste de professeur à l'Illinois Institute of Technology.

Tout spécialement venu de Chicago pour participer à cette conférence, celui-ci a démontré au public son engouement profond et sa passion pour les enjeux du Big Data et de l'intelligence artificielle. Durant sa présentation, monsieur Brethenoux a démontré la complémentarité qui existe entre institutions financières classiques et Fintechs. Ces dernières peuvent être des relais d'innovation génératrices de performance et de croissance. Pour preuve, des alliances stratégiques sont en cours et existent déjà.

Sur le sujet de l'émergence de l'intelligence artificielle, il a su notamment apaiser certaines craintes sur l'émergence de cette technologie vis-à-vis d'un éventuel remplacement de l'homme par la machine. Il a souligné le fait que l'intelligence artificielle ne vise pas à remplacer l'humain mais à l'assister et lui simplifier les tâches les plus complexes, ainsi qu'à réduire les biais susceptibles d'altérer nos prises de décision.

Après le succès de cette première conférence, SESAMm prévoit de faire de cet événement annuel un rendez-vous incontournable pour les acteurs financiers et de les aider à adopter ces technologies.

Les plus grandes menaces de l'entreprise numérique en 2016

Le vol de données en interne et les logiciels malveillants sont les principales sources d'inquiétude des responsables de la sécurité des entreprises, selon un nouveau rapport publié par Accenture et HfS Research. La majorité des personnes interrogées (69%) déclarent avoir été victimes d'une tentative de vol ou d'altération de données menée en interne sur les 12 derniers mois. Les sociétés du secteur des médias et des hautes technologies sont les plus touchées (77%).

Le risque interne pourrait s'aggraver, les professionnels interrogés estimant le vol de données d'entreprise devoir augmenter des deux tiers dans les 12 à 18 mois. Par ailleurs, l'étude montre que la faiblesse des budgets dédiés au renforcement des compétences freine la capacité des entreprises à lutter contre ces attaques. Cette étude, intitulée «The State of Cybersecurity and Digital Trust 2016», (État de la cybersécurité et de la confiance numérique en 2016) a été réalisée par HfS Research pour le compte d'Accenture auprès de plus de 200 cadres supérieurs chargés de la sécurité de leurs entreprises et d'autres spécialistes en informatique sur plusieurs zones géographiques et secteurs.

«Notre étude dresse un portrait contrasté. Les responsables de la sécurité voient les menaces s'intensifier avec le temps, limitant ainsi leur capacité à protéger les données sensibles et à alimenter la confiance numérique» explique Stéphane Geyres, directeur de l'activité conseil en Cyber Sécurité d'Accenture Strategy en France.

«Alors que les entreprises souhaitent investir dans des cyber technologies, des budgets de recrutement et de formation limités font obstacle à un plein usage de ces technologies. Régler ces problèmes de sécurité va exiger des entreprises de collaborer avec l'ensemble de leur écosystème – leurs unités commerciales, leurs partenaires et leurs utilisateurs – pour pérenniser un environnement de confiance numérique.»

Ce rapport identifie cinq points de vigilance pour les entreprises :
- **RH** : Pour 31% des sondés, l'insuffisance des budgets de formation ou de recrutement est le principal frein à la lutte contre les attaques.
- **Technologie** : Les pare-feu et le chiffrement sont les technologies au cœur de la cyberdéfense, mais les entreprises se focalisent sur l'informatique cognitive et l'intelligence artificielle (31%), ainsi que sur l'anonymisation des données (25%).
- **Parité** : La sécurité d'une entreprise est celle du maillon le plus faible de son écosystème, or seules 35 à 57% des participants déclarent vérifier la sécurité et la résilience de leurs partenaires. Les prestataires de gestion déléguée sont les moins contrôlés, et les prestataires de crédit les plus contrôlés.
- **Budget** : A 70%, les sondés soulignent le manque d'investissements dans les talents et compétences en technologies de cybersécurité.
- **Direction** : Alors que 54% des interrogés s'accordent sur une cybersécurité qui favorise la confiance des consommateurs dans le numérique, 36% pensent que leur directions générales y voient un coût injustifié.

«Si les lacunes identifiées peuvent être surmontées, elles soulignent toutefois le besoin d'une approche fondamentalement différente, avec une gestion des risques métiers plus robuste et le développement de la confiance numérique» explique Stéphane Geyres, directeur de l'activité conseil en Cyber Sécurité d'Accenture Strategy.

«C'est l'occasion de repenser la manière dont confiance et sécurité viennent systématiquement s'intégrer au cœur même de l'entreprise, par exemple via des solutions d'automatisation ou d'intelligence artificielle, ou par des partenariats et des externalisations.»