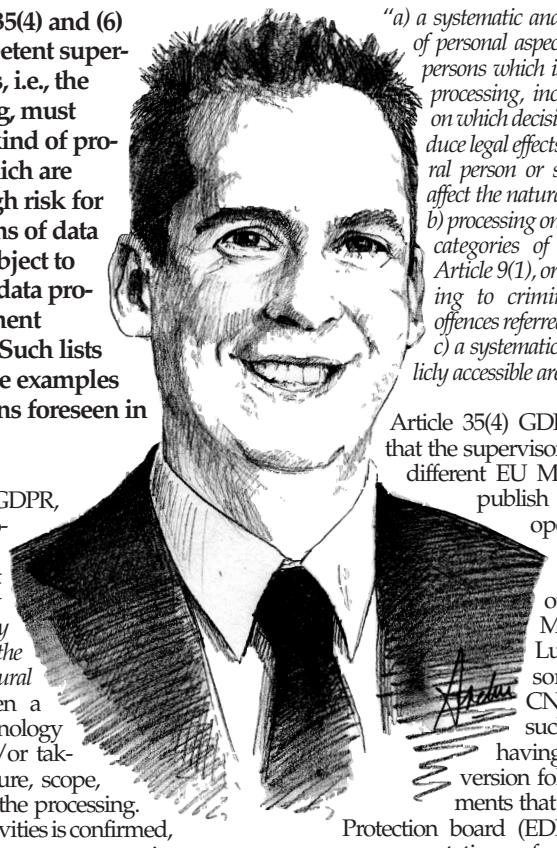
GDPR: the CNPD has released its black list of processing operations subject to a data protection impact assessment (DPIA)

Further to Article 35(4) and (6) GDPR, the competent supervisory authorities, i.e., the CNPD in Luxembourg, must establish a list of the kind of processing operations which are likely to result in a high risk for the rights and freedoms of data subject and, hence, subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). Such lists come in addition to the examples of «high risk» situations foreseen in Article 35(3) GDPR.



According to Article 35 GDPR, the carrying out of a so-called data protection impact assessment (DPIA) is mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*", especially when a new data processing technology is being introduced and/or taking into account the nature, scope, context and purposes of the processing. If the high risk of such activities is confirmed, the relevant data controller must engage in a consultation with the supervisory authority.

Article 35(3) GDPR provides some examples when a processing operation is "*likely to result in high risks*", i.e., when:

"a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 1013; or
c) a systematic monitoring of a publicly accessible area on a large scale".

Article 35(4) GDPR further foresees that the supervisory authorities in the different EU Member States must publish a list of processing operations that are subject to the requirement carry out a DPIA. On 11 March 2019, the Luxembourg supervisory authority, the CNPD, has published such a «black list» after having amended its initial version following some comments that the European Data Protection board (EDPB, a body which regroups representatives of all EU supervisory authorities) had made on 4 December 2018.

The following processing activities are included in this list :
1. The processing of genetic data if one further criterion of the 2017 EDPB DPIA guidelines is met (unless the processing is carried out by a healthcare professional in the context of healthcare services).
2. The processing of biometric data for identification purposes if one further criterion of the EDPB DPIA guidelines is met.
3. The combination, correspondence or comparison of data that were collected for different purposes if this has a legal effect or a significant impact on the data subject. This type of processing reminds us a bit of the Luxembourg 2002 Data Protection Act (*Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*) that was abolished in the context of the entry into force of the GDPR. This law provided for an obligation to request a prior authorisation for the interconnection of datasets.
4. A regular and systematic control of employee activities if this has a legal effect or a similar significant impact on the data subject. The possibility that employee monitoring could subject to a DPIA, was already underscored in the Luxembourg 2018 GDPR Act (*Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du RGPD*), which implements and complements the GDPR.
5. The processing of files which are likely to contain data of the whole population, unless a more general impact assessment already has been carried out in the context of a legislative measure on the basis of which such processing takes place.
6. The processing for scientific or historical research, or for statistical purposes within the meaning of Articles 63 to 65 of the 2018 GDPR Act. Article 65 of the 2018 GDPR Act stipulates that data controllers must for these processing activities implement several measures amongst which the appointment of a DPO, the carrying out of a DPIA, etc., it being understood that this legal provision foresees the possibility for the controller to document, justify and to request an exemption to the obligation to implement one or more of these measures. Now that the CNPD has included this type of processing in its «black list», it seems not to be possible any more for controllers in this area to request such an exemption to their obligation to carry out a DPIA.
7. Systematic geolocalisation.
8. The processing of indirectly collected data if one further criterion of the EDPB DPIA guidelines is met. In its initial proposal, the CNPD suggested that a DPIA would be required if such processing is based on indirectly collected data but only «*when it is not possible / feasible to guarantee the right of information*». That last requirement has not been withheld in the final version.

It is worth noting that the 2017 DPIA guidelines of the EDPB also contain a list of «high risk» criteria, it being understood that according to these guidelines a DPIA is required if a processing meets two of these criteria. These guidelines are not legally binding but have a high authoritative power as soft law and have an EU wide reach. Furthermore, with the adoption of the CNPD «black» list these EDPB also have a more binding character as some of the of the «black listed» processing activities require that in addition to the listed processing operations one of the EDPB 2017 DPIA criteria is met.

In any event, now that the CNPD has issued its black list and the 2017 DPIA guidelines of the EDPB gain authority, Luxembourg based data controllers have a little more certainty in which situations they have to carry out a DPIA.

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

Les banques européennes aveugles face à l'impact des FinTechs

Par Euan DAVIS, European Lead for the Center for the Future of Work, Cognizant

Au sein du secteur bancaire européen, le simple passage au numérique ne suffit plus. Les décideurs des banques en traditionnelles doivent en effet être mesure de déceler les principales menaces qui pèsent sur leur secteur (évolution réglementaire, paysage politique, concurrence nouvelle et technologies émergentes). Ils doivent par ailleurs comprendre dans quelle mesure ces menaces sont susceptibles de réduire, déplacer, court-circuiter ou même détruire leur activité au cours des cinq prochaines années.

Les réformes liées à la Directive révisée concernant les services de paiement (PSD2) et à l'open banking préparent actuellement le terrain à l'arrivée de «nouveaux» entrants. De fait, un récent rapport sur le nouveau génome bancaire révèle que plus de la moitié (55%) des nouvelles banques digital first et 61% des FinTech sont davantage confiance dans leur capacité à concourir face aux établissements bancaires existants. Toutefois, il est inquiétant de constater que les banques en place semblent ne pas avoir conscience de cette situation ; seul un tiers d'entre elles (36%) perçoivent les menaces de ce nouveau paysage.

Ce rapport présente les résultats de recherches menées auprès de plus de 300 cadres du secteur bancaire européen. Il souligne que les nouvelles réformes bancaires ne constituent pas un pensum supplémentaire lié à un bouleversement réglementaire, mais plutôt le début d'une nouvelle dynamique au sein du secteur.

Les licornes du numérique font vaciller les banques

Outre les inquiétudes liées aux nouvelles banques et aux FinTechs, l'étude constate que les banques en place considèrent les géants de la technologie comme Amazon, Google et Facebook comme une menace majeure. Plus d'un quart d'entre elles (28%) estiment en effet que ces mastodontes du numérique constitueront les principaux concurrents des établissements bancaires au cours des trois prochaines années. Si la majorité des banques en place considèrent qu'elles sont en mesure de conserver un avantage compétitif sur les FinTechs et les nouvelles banques dans leurs domaines de prestations actuels, 45% d'entre elles craignent de perdre un atout stratégique dans le secteur des prêts aux particuliers non sécurisés avec l'essor des prêts peer-to-peer.

Une autre menace importante concerne la capacité des FinTechs qui s'appuient sur la blockchain à perturber les banques traditionnelles à différents niveaux de la chaîne de valeur bancaire. Les FinTechs remportent actuellement la bataille, 34% d'entre elles recourant déjà à la blockchain, contre 17% seulement des banques en place.

D'après le rapport, tout acteur du secteur qui considérerait que la blockchain n'est pas en mesure de court-circuiter les banques dans les cinq à dix prochaines années ferait preuve d'un manque total de clairvoyance. Pourtant, la majorité des cadres du secteur bancaire interrogés (77%) conviennent que l'accès aux données consommateurs dont disposent les banques en place reste pour elles un atout par rapport aux FinTechs et aux nouvelles banques.

Les nouvelles règles bancaires se concrétisent

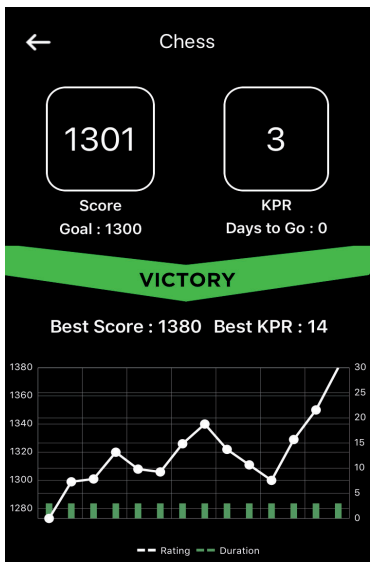
Face aux menaces des banques «challengers», des FinTechs et des géants de la technologie, une catégorie de banques traditionnelles apparaît progressivement : les «banques résilientes». Ces établissements ont engagé l'automatisation avancée du traitement des données au niveau du front office, intégré l'analyse des données en temps réel pour soutenir les principaux services du middle et du back office, et adopté des solutions de cloud public. Ils s'attachent bien plus que les autres à améliorer la culture interne et l'expérience client numérique, et travaillent en partenariat plus étroit avec des tiers opérant à la fois à l'intérieur et à l'extérieur du secteur bancaire.

Le rapport définit le Nouveau Génome Bancaire et met l'accent sur cinq étapes que les banques en place doivent suivre pour devenir des «banques résilientes» :
- **Placer les clients au cœur des modèles opérationnels** : recadrer les données et les processus autour des clients. Débuter en simplifiant les systèmes hérités et en engageant l'automatisation. Puis diriger prioritairement les investissements vers l'expérience numérique et le data analytics.
- **Adopter le modèle du marché** : l'open banking n'en est encore qu'à ses balbutiements, mais il a le pouvoir de développer l'innovation. Étudier les possibilités des prestations de FinTechs en marque blanche, en nouant voire en créant un partenariat avec des incubateurs/accélérateurs de FinTechs.
- **Profiter du bouleversement réglementaire à venir comme d'un catalyseur du changement** : la PSD2 est susceptible de mettre en évidence les défaillances des banques en place en matière de technologie, de culture et de services clients. Mais les changements réglementaires devraient être envisagés comme un catalyseur encourageant des actions en termes d'optimisation, d'innovation et de transformation.
- **La culture de l'innovation doit venir d'en haut** : cette culture doit également constituer l'axe autour duquel tourne l'objectif stratégique prioritaire. Assurer une communication régulière à ce sujet en encourageant les collaborateurs à donner leur avis sur les actions stratégiques.
- **Ne pas oublier la blockchain** : les répercussions de la blockchain seront profondes à tous les stades ou presque de la chaîne de valeur bancaire. Identifier ces risques potentiels, procéder à des tests puis se renforcer pour rester résilients.

Alors que les organismes réglementaires nivellent le secteur et que la technologie contribue à faire tomber les barrières à l'entrée de cette industrie, en en modifiant la dynamique, les banques européennes sont tenues de faire preuve d'une résilience de plus en plus grande. Elles doivent redéfinir leur modèles opérationnels et économiques afin de faire face à un nouvel environnement concurrentiel, accélérer rapidement leurs cycles d'adoption des nouvelles technologies et accroître de façon massive leur capacité de réponse aux changement géopolitiques. Cette nouvelle approche des "banques résilientes" devrait constituer un antidote contre les FinTechs, et aider ainsi les banques traditionnelles à adapter et redéfinir leurs modèles pour rester compétitives, quels que soient les nouveaux entrants auxquels elles seront confrontées.

App #TheGameofNumbers : les clefs de la performance

Réussir tient souvent à peu de chose : se fixer un objectif à sa porter, sur une courte durée et garder une trace de sa performance. L'application «TheGameofNumbers» a pour vocation de partager, d'encourager et de révéler le potentiel de chacun. Focus sur l'application TheGameofNumbers avec Jérôme BLOCH, PDG de 36OCrossmedia.



Pourquoi avoir développé l'application «TheGameofNumbers» ?

D'un jour à l'autre, les performances de chacun peuvent varier en fonction de divers facteurs comme la déshydratation, le manque de sommeil, le stress… Il est parfois difficile d'avoir du recul sur son efficacité, ainsi avoir un outil permettant d'analyser ces fluctuations aide à mieux appréhender et gérer sa performance. Le développement de l'application TheGameofNumbers est le résultat de cette réflexion. Elle permet de définir des objectifs, d'avoir un suivi régulier sur une durée déterminée et d'obtenir une récompense : une médaille pour chaque exploit accompli. Cela renforce la confiance, la motivation et l'estime de soi de chacun. Comme je le décris dans mon livre «The Game of Numbers», les nombres ont une importance dans les prises de décisions et les performances.

Comment vous permet-elle d'être plus performant ?

Avoir des routines permet dans un premier temps d'améliorer une compétence en particulier et dans un second temps d'avoir une idée sur son état d'esprit. Se fixer pendant une durée déterminée un objectif demande de s'investir pleinement dans l'accomplissement de cette mission. J'ai instauré un rituel autour de la résolution quotidienne de «situations» sur l'application Chess24, me permettant de résoudre 5 défis par jour.

Un rang est attribué en fonction de mes résultats. Je demande à mes collaborateurs d'en faire autant. Cette routine permet de garder une certaine continuité, de chercher l'excellence et d'être au meilleur de sa performance. Cela se ressent dans le travail et dans l'exécution des missions. Mesurer son efficacité favorise la régularité, l'assiduité et la persévérance. S'astreindre à une routine quotidienne et exigeante implique de l'être au travail.

Pour qui est-elle destinée ?

Tout le monde peut l'utiliser. L'application «TheGameofNumbers» est téléchargeable gratuitement dans l'App Store et très prochainement dans Google Play Store. Il suffit de créer un compte avec une adresse mail afin de lancer ses propres défis. Cela va des performances sportives à l'utilisation des réseaux sociaux, en passant par le bien-être. La beauté de l'outil est de pouvoir reporter, garder une trace et avoir une preuve de l'accomplissement de son objectif. Elle permet ainsi d'avoir un suivi sur les KPR (Key Performance Revelator), c'est-à-dire, le nombre de jours sur lequel l'objectif a été tenu. Par exemple, si le défi est d'augmenter le nombre de connexions sur LinkedIn sur 2 semaines, le KPR sera de quatorze jours, sinon, il retombera à 1.