Chronique du droit des nouvelles technologies - La rubrique mensuelle ICT de Vincent Wellens

Comment choisir son prestataire de services IT ?

Toute entreprise, grande ou petite, dépend de l'informatique, domaine sujet à un renouvellement constant. Ces nouveautés techniques entraînent inévitablement de nouvelles questions juridiques impactant le quotidien des salariés et des employeurs. La présente rubrique, à paraître tous les mois, a pour objectif de couvrir les sujets d'actualité et les évolutions en droit des nouvelles technologies au niveau de la législation luxembourgeoise et européenne.

L'externalisation de la fonction IT par une entreprise est un phénomène de plus en plus fréquent. Elle permet à une organisation de faire d'importantes économies d'argent, tout en obtenant une qualité de service généralement supérieure à ce qu'elle aurait obtenu si elle avait assuré elle-même la fonction. La Chronique du droit des nouvelles technologies a décidé de consacrer trois rubriques mensuelles à la rédaction d'un dossier spécial destiné à guider les entreprises tout au long de ce processus d'externalisation de la fonction IT.

Le présent et premier volet de ce dossier spécial est consacré à la manière de choisir un prestataire de services IT de confiance. Sans prétendre à l'exhaustivité, il met en exergue une série de risques et de points d'attention qu'une entreprise devra nécessairement garder à l'esprit lors du choix de recourir aux services d'un prestataire IT.

Le second volet sera consacré à la négociation et à la rédaction du contrat qui devra nécessairement être conclu avec un prestataire de services IT en cas de sous-traitance.

Finalement, un troisième et dernier volet traitera de l'exécution du contrat, de la fin de la relation contractuelle et de la façon d'assurer une transition efficace entre la situation existante sous l'empire du contrat et la situation post-contractuelle.

Dossier spécial contrats informatiques (Partie 1/3): Comment choisir son prestataire de services IT?

Bien qu'un bon nombre de recommandations soient valables à l'égard de tout contrat de services IT, l'accent sera particulièrement mis sur les services de *cloud computing*. Le choix d'un prestataire IT constitue sans doute la première étape dans la mise en place de votre projet d'externalisation de l'IT. Les conséquences du choix d'un mauvais prestataire IT peuvent être considérables pour une entreprise, et lui faire perdre d'importantes ressources.

Les exemples sont nombreux. La défaillance dans les services IT de l'entreprise peut tout d'abord empêcher les salariés de travailler des heures durant et provoquer pour l'entreprise une réelle perte sèche. Les bogues informatiques incessants peuvent en outre facilement agacer les travailleurs d'une entreprise et faire considérablement baisser leur productivité. Dans le cadre d'une externalisation IT, l'entreprise va en outre confier une grande quantité de données à son prestataire IT.

Les conséquences en cas de pertes ou de fuites de données de l'entreprise par le prestataire IT peuvent également être fortement préjudiciables. Le fait de choisir un mauvais prestataire peut en outre mener à une perte de contrôle effective sur certaines questions cruciales de sécurité. Cela peut également mener à une situation de dépendance vis-à-vis du prestataire IT.

Finalement, le choix d'un mauvais prestataire IT pourrait avoir pour conséquence qu'une entreprise ne soit plus à même de respecter ses obligations légales, de quelque type qu'elles soient, et de se voir imposer de ce fait de lourdes sanctions.

Afin de réduire au maximum les risques susmentionnés, il est crucial de choisir un bon prestataire de services IT. Pour réaliser ce choix, une certaine stratégie doit être respectée par l'entreprise, et certains points d'attention doivent être particulièrement gardés à l'esprit. En voici une liste non-exhaustive. Ceux-ci sont tantôt d'ordre technique, tantôt d'ordre juridique.

La réalisation d'un cahier des charges

Il est vivement recommandé au client de réaliser un cahier des charges détaillant ses propres exigences, d'un point de vue non seulement légal, mais également pratique et technique. Un tel cahier des charges permettra au client de mieux réfléchir à ses propres besoins et exigences, et définira plus clairement l'objet du contrat par la suite. Ceci est d'autant plus important que la tendance est aujourd'hui à la rédaction par le prestataire IT de contrats d'adhésion, ne laissant que peu de marge à la négociation.

En recourant à un cahier des charges, il sera plus aisé pour une entreprise de sélectionner une série de prestataires rencontrant dès le début ses propres exigences pratiques, techniques et juridiques, plutôt que de choisir un prestataire ne respectant *a priori* pas lesdites exigences, et de tâcher de les lui imposer contractuellement par la suite.

Un prestataire permettant d'assurer le respect de la réglementation en matière de protection des données à caractère personnel

Des données à caractère personnel étant généralement traitées au sein des systèmes d'information, une attention toute particulière devra être portée au respect de la législation sur la protection des données à caractère personnel, principalement à la loi modifiée du 2 août 2002 relative à la protection de la personne à l'égard du traitement de données à caractère personnel (ci-après, la «Loi du 2 août 2002 sur la protection des données»).

En règle générale, dès lors qu'elle détermine les moyens et les finalités du traitement des données, le fait pour l'entreprise de sous-traiter en tout ou en partie son IT ne fera pas obstacle à sa qualité de responsable du traitement. Le prestataire IT ne sera en effet dans bien des cas qu'un simple sous-traitant, à savoir qu'il effectuera uniquement un traitement de données au nom et pour le compte de l'entreprise cliente. En d'autres termes, cette dernière restera pleinement responsable du respect correct de la Loi du 2 août 2002 sur la protection des données.

Il est dès lors indispensable de choisir un prestataire IT offrant des garanties certaines en matière de protection des données. Il doit ainsi être particulièrement porté attention à la question du lieu de stockage des données (un transfert transfrontalier de données dans un Etat non-membre de l'Union européenne étant strictement réglementé, notamment par l'article 18 de la Loi du 2 août 2002 sur la protection des données), à la question des mesures de sécurité des données, à la question de la sous-traitance en chaîne, à la question de la notification des violations de données (qui deviendra obligatoire prochainement, en cas d'adoption du règlement européen sur la protection des données à caractère personnel), etc.

Afin d'évaluer le niveau de protection des données à caractère personnel offert par un prestataire de services *cloud*, il peut être intéressant de vérifier la conformité du prestataire concerné avec les nouvelles normes «*ISO 27018:2014 «Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*».

Celles-ci établissent des lignes directrices destinées à tout type d'organisations proposant à d'autres organisations des services de traitement de l'information en tant que sous-traitant via des services de *cloud computing*, avec une attention toute particulière à la question de la protection des données à caractère personnel. A nouveau, le respect par le prestataire IT de ladite norme constitue certes une indication sur le niveau de conformité à la législation en matière de protection des données à caractère personnel, mais ne constitue pas une garantie absolue.

Un prestataire certifié

De manière plus générale, la certification d'un prestataire peut constituer un bon critère de choix. Il existe une multitude de normes et de certifications relatives à la sécurité et au management de services d'information. Le fait pour un prestataire IT de respecter celles-ci permet de prouver qu'il présente *a priori* un certain niveau de fiabilité et de sécurité. Toutes les normes et certifications ne se valent cependant pas, et il faudra faire le tri entre les certifications pertinentes et celles qui le sont moins.

A titre d'exemple, les normes «*ISO/IEC 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*» et «*ISO/IEC 27002:2013, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information*» peuvent être citées. La première garantit le management de la sécurité des informations, notamment des données financières, des documents soumis à la propriété intellectuelle, des informations relatives au personnel ou des données qui sont confiées à une entreprise par des tiers ; tandis que la seconde donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information.

Ces deux normes servent d'ailleurs de base pour la certification des prestataires de services de dématérialisation et/ou de conservation au sens de la future loi sur l'archivage électronique. Cette certification fera bénéficier leurs clients d'une présomption de conformité à l'original de documents conservés électroniquement par les prestataires en question.

La nouvelle norme «*ISO/IEC 27040:2015, Technologies de l'information – Techniques de sécurité – Sécurité de stockage*» est également importante. Elle donne, de manière générale, les règles à suivre afin de gérer efficacement tous les aspects de la sécurité de stockage de données (de la planification à la mise en œuvre), et ainsi réduire les risques de perte ou de violation de données.

Des certifications délivrées par les éditeurs de logiciels, les spécialistes de la sécurité ou encore les fabricants de matériel informatique existent également. Pour s'assurer que le prestataire IT est véritablement certifié, il sera nécessaire de vérifier le portail internet de l'éditeur ou du fabricant concerné par la certification.

Bien que pouvant faciliter l'évaluation de la sécurité et des garanties qu'offre un prestataire déterminé, ces normes ne donnent néanmoins pas de garanties absolues, et il sera nécessaire pour l'entreprise désirant externaliser l'IT d'examiner les conditions exactes d'application de la norme, éventuellement via des rapports d'audit.

Un prestataire assurant le respect de la réglementation CSSF: pour les clients PSF mais également pour les autres?

Dans l'hypothèse où l'entreprise désirant externaliser une fonction IT, est active dans le secteur financier, une couche supplémentaire de règles doit être prise en compte.

Il s'agit du dispositif mis en place par la CSSF, principalement par voie de circulaires. Ainsi, les établissements de crédit, les entreprises d'investissement et les professionnels effectuant des opérations de prêt devront par exemple prêter une attention particulière à la circulaire CSSF 12/552 (telle que modifiée). Celle-ci prévoit un dispositif de règles à respecter, principalement dans le chef de l'entreprise décidant d'externaliser l'IT, mais qui impacte directement le choix du prestataire. La circulaire prévoit, entre autres, que:
- la décision d'externaliser doit être appuyée sur une analyse préalable et approfondie ;
- l'externalisation doit faire l'objet d'un contrat écrit officiel et détaillé (incluant notamment un cahier des charges) ;
- la continuité du service doit être assurée en cas d'événements exceptionnels ou de crise ;
- la réversibilité des services externalisés et la possibilité de transférer de manière adéquate les services vers un autre opérateur ou de les reprendre en gestion propre doivent également être assurés ;
- l'externalisation de services vers un prestataire situé en dehors du Luxembourg n'est possible que dans des situations bien circonscrites ;
- l'accès de la CSSF, du réviseur d'entreprises agréé et des fonctions de contrôle interne de l'établissement aux informations relatives aux activités sous-traitées doit être garanti en vue de leur permettre d'émettre une opinion fondée sur l'adéquation de la sous-traitance.

Même si elle ne relève pas du secteur financier, nous sommes d'avis que toute entreprise envisageant l'externalisation d'une fonction IT devrait garder à l'esprit les exigences principales de la CSSF en considérant celles-ci comme une liste de contrôle des bonnes pratiques en la matière.

Il est finalement à noter que le cadre juridico-réglementaire dans le secteur financier favorise une externalisation vers des PSF de support, lesquels sont également soumis à la surveillance de la CSSF. Ces derniers doivent notamment soumettre un rapport d'analyse de risques (RAR) à la CSSF. Ce rapport est une auto-évaluation des risques directs et indirects pour les clients des PSF de support.

La CSSF a explicitement prévu que ledit rapport pouvait être communiqué aux clients (potentiels) des PSF de support. En d'autres termes, les clients d'un PSF de support ne doivent nullement hésiter à lui demander son RAR.

Conclusion

Choisir le bon prestataire IT n'est pas chose aisée. La multiplication des acteurs sur le marché ne rend pas les choses plus faciles. Sur base de la réalisation par l'entreprise désirant sous-traiter une fonction IT d'un cahier des charges déterminant précisément ses exigences en termes légaux, techniques et pratiques ; et en tenant dûment compte des points d'intérêts énoncés ci-dessus, il sera normalement possible pour l'entreprise de sélectionner les prestataires proposant *a priori* les meilleures garanties de succès. Il restera ensuite à mettre ceux-ci en concurrence, en comparant leurs différentes offres, en tenant néanmoins compte du fait que l'offre la moins onéreuse ne sera pas nécessairement la plus économique pour l'entreprise sur le long terme.

Une fois le prestataire choisi, commencera la seconde étape du processus d'externalisation de l'IT ; à savoir, la négociation du contrat IT. La seconde rubrique de ce dossier spécial «contrat IT» sera consacrée aux points d'attention qu'il faut tenir à l'esprit lors de la négociation d'un tel contrat informatique.

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

Nicolas RASE
Associate chez NautaDutilh Avocats Luxembourg S.à r.l.
nicolas.rase@nautadutilh.com

www.nautadutilh.com

BGL BNP Paribas lance sa solution de paiement mobile

BGL BNP Paribas lance l'application BGL BNP Paribas Digicash, une solution de paiement mobile développée par Digicash Payments et gratuitement téléchargeable sur l'App Store ainsi que sur Google Play. Le client peut désormais effectuer ses paiements en toute simplicité et sécurité via son smartphone, que ce soit sur internet, dans les points de vente partenaires ou chez lui pour le paiement de factures.

L'opération se réalise directement depuis son compte bancaire. Outre un nouveau design qui permet d'optimiser l'expérience utilisateur, l'application est reliée au programme de fidelité Premium Benefits de la banque dédié aux titulaires des cartes haut de gamme MasterCard Gold, Gold Priority, Platinum et Elite.

En effet, l'utilisation par lesdits titulaires de l'App BGL BNP Paribas Digicash pour le paiement de leurs factures et en points de vente partenaires leur permet d'alimenter leur cagnotte Premium Benefits. Le lancement de l'application BGL BNP Paribas Digicash s'inscrit pleinement dans la stratégie de digitalisation et d'innovation de la banque. «En effet, particulièrement engagés dans cette voie, nous avons bâti une offre digitale complète à destination de notre clientèle, en couvrant tous les canaux existants et en les rendant accessibles auprès de n'importe quel type d'appareil (iOS, Android,…).

Après le «multi-channelling», puis le «cross-channelling», l' «omni-channelling» consiste à permettre à l'ensemble de nos clients d'interagir avec la banque par le canal qui leur convient le mieux, et ce avec le moins de restrictions possibles» précise Kik Schneider, membre du Comité de direction de BGL BNP Paribas, responsable Banque de détail et des entreprises à Luxembourg.

Ce lancement constitue une étape supplémentaire dans l'étoffement de l'offre commerciale et mobile de la banque pour répondre aux besoins de l'ensemble de ses clients.