ALLEN & OVERY

Les enjeux et défis de la transformation digitale

1. Structurer la transformation digitale

1.1 Sensibilisation interne

Enjeux/Objectifs	Actions
– Sensibiliser **l'entreprise aux opportunités et défis liés à la digitalisation**. – Etre attentif aux évolutions **des pratiques de marché en matière de digitalisation**. – Comprendre les enjeux juridiques **en amont**.	– Constituer une équipe dédiée en interne composée de compétences croisées (juridique, IT, sécurité et commerciale). – Former les employés à l'utilisation d'outils numériques et aux exigences de sécurité sous-jacentes.

1.2 Collaboration externe

Le recours à des formes de collaboration / partenariat dans le cadre de la transformation digitale est devenue incontournable. Plusieurs formes de collaboration sont envisageables en fonction des objectifs poursuivis.

Enjeux/Objectifs	Actions
Externalisation totale ou partielle de la transformation digitale : – Sélectionner un prestataire IT stratégique ; – Etablir un partenariat concernant une solution informatique existante : contrat d'intégration, de licence et de maintenance ; – Construire une solution informatique « sur mesure » : contrat de développement.	– Identifier en amont les besoins et les attentes et les refléter dans la demande de proposition (RFP) ; – Evaluer les capacités et garanties des prestataires envisagés (ie analyse d'impact juridique, opérationnel et technique) ; – Anticiper les points juridiques structurants à couvrir dans le contrat (niveaux de services, droits de propriété intellectuelle, obligation de résultat, responsabilité) ; – Définir précisément dans le contrat les rôles et obligations des parties tant sur le plan juridique qu'opérationnel.
Acquisition d'une entreprise spécialisée ou stratégique : – Pallier l'absence de savoir-faire en interne ; – Maintenir le contrôle et la gouvernance sur la transformation digitale.	– **Conduire un audit** (« due diligence ») pour identifier les risques juridiques et opérationnels éventuels pouvant avoir un impact sur le processus de digitalisation souhaité : invalidité des droits de propriété intellectuelle, systèmes d'information vulnérables, non-conformité au RGPD, litige en cours ; – **Evaluer l'opportunité au regard des risques et refléter les risques dans le prix d'acquisition et la documentation transactionnelle** (ex : garanties, engagements *pré-closing*, indemnités spécifiques).
Constitution d'une entité ad-hoc commune / *joint-venture* : – Créer un véhicule légalement indépendant et aux objectifs communs ; – Partage des ressources humaines, financières et matérielles.	– Comprendre **la culture et les pratiques de chaque entreprise = homogénéisation nécessaire** pour des objectifs communs ; – Déterminer précisément les **rôles opérationnels et responsabilités juridiques de chaque entité dans la documentation contractuelle** ; – A défaut de dispositions contractuelles précises : **conflits d'interprétation sur points clés tels que la gouvernance, le pouvoir de décision, la titularité des droits sur la technologie au cœur de la collaboration**.

2. Comprendre les problématiques liées à la digitalisation

2.1 Cybersécurité

Risques	Actions
– Multiplication des attaques informatiques extérieures **(notamment pendant la période du Covid-19) : accès non-autorisé, vol ou détournement de données, phishing, etc. ;** – Retard **processus de digitalisation** ou systèmes informatiques vulnérables / non-robustes = risque élevé ; – Conséquences critiques pour l'activité de l'entreprise **victime d'une attaque externe** : risque matériel **(ex : interruption des systèmes et des activités critiques, perte de données, atteinte aux secrets des affaires) ;** risque financier **(ex : discontinuité de l'activité, sanction administrative ou règlementaire si niveau de sécurité insuffisant, dommages aux tiers) ;** et risque réputationnel **(ex : perte de confiance / crédibilité vis-à-vis de la clientèle, systèmes informatiques réputés vulnérables et obsolètes).**	– Intégrer les risques dès la conception **d'une technologie et tout au long du processus de digitalisation** (« *secure by design* ») ; – Mettre en place et maintenir des mesures techniques et organisationnelles appropriées **aux risques (contrôle et limitation des accès, ségrégation des systèmes et des données, dispositions contractuelles précises)** ; – Sensibiliser employés / prestataires **ayant accès aux systèmes d'information & imposer contractuellement le respect d'une** politique interne de sécurité des systèmes d'information **(à définir en amont)** ; – Evaluer régulièrement le niveau **de sécurité des systèmes d'information (ex : audit externe)**.

2.2 Utilisation des données

Opportunités liés à l'écosystème *big data* :

– **Valorisation des données** utilisées ou **générées** par l'entreprise ;

– **Monétisation des données** pour générer du **revenu** et développer de nouvelles lignes de produits ou services.

Risques	Actions
– **Traitements illicites de données ;** – **Monétisation non-autorisée ou non-encadrée des données ;** – **Perte de maîtrise de la donnée.**	– **Analyse d'impact en amont pour identifier** les **risques** juridiques et opérationnels ; – **Encadrer contractuellement le partage de données** avec les tiers : de la gouvernance à la réutilisation des données ; – **Veiller à la conformité interne**: conformité du traitement au RGPD (respect des conditions sous-jacentes), **mesures** de sécurité adéquates, sensibilisation, etc.

2.3 Droits de propriété intellectuelle

Instruments clés au service de la stratégie digitale des entreprise, la **protection des technologies doit être strictement encadrée.**

Risques	Actions
– **Conflits de titularité des droits de propriété intellectuelle** sur la technologie cœur du **business** ; – **Articulation complexe entre les différents régimes de protection** : collecte et contrôle de la donnée au sens du RGPD, droits de propriété intellectuelle liés à une solution ou une base de données, etc. ; – **Technologie clé intégrant des composantes « open source » :** obligation de partager les évolutions avec la communauté « open source », risque de non-respect des conditions des licences sous-jacentes.	– **Bien comprendre le périmètre des droits et vérifier régulièrement la bonne utilisation des technologies** en cas de licence de logiciels ou de licence open source ; – **Conduire une analyse sur les risques liés à l'utilisation** de données ; – **En cas de collaboration externe : insister sur la phase de due diligence** pour identifier les risques d'atteintes aux droits de tiers, les risques d'invalidité de droit de propriété intellectuelle ; – **Sécuriser les contrats conclus avec les tiers** (prestataires ou vendeurs) pour couvrir les risques identifiés, obtenir des garanties précises et bien encadrer la cession ou l'utilisation des éléments protégés par le droit de la propriété intellectuelle.

2.4 Ethique

Clients et salariés sont de plus en plus sensibles et sensibilisés à la transparence des informations qu'une entreprise détient sur eux et sur l'usage qui en est fait.

Risques	Actions
– Risques liés à la **non-conformité à la règlementation applicable en matière de protection des données personnelles** notamment ainsi qu'à la **réputation de l'entreprise.**	– **Intégrer les règles d'éthique et de transparence dès la conception** de nouvelles lignes de produits ou services ; – **Définir et communiquer en interne des politiques** / chartes énonçant les principes ; – **Sensibiliser les employés** via des formations dédiées.

3. Cerner les enjeux spécifiques à chaque « domaine » de digitalisation

3.1 Objets connectés et intelligence artificielle

Risques	Actions
– Confidentialité et sécurité **des données collectées et traitées** ; – Conformité de la collecte et du traitement **à la règlementation applicable en matière de protection des données** ; – Biais dans la prise de décision automatisée.	– Conduire une analyse d'impact en amont **pour identifier les risques pour les individus (vie privée, données sensibles et prise de décision automatisée)** ; – Intégrer les enjeux de sécurité dès la conception **de la technologie et permettre aux individus de paramétrer leurs choix à tout moment** ; – Prendre en compte les recommandations et lignes directrices en matière d'algorithmes ; – Mettre en place des procédures opérationnelles internes et des mesures contractuelles efficaces **pour assurer une collecte et un traitement conforme avec les exigences du RGPD** ; – Encadrer les éventuels transferts de données personnelles en dehors de l'Espace Economique Européen (EEA).

3.2 Blockchain

Opportunités liées à la désintermédiation et à la décentralisation des échanges (absence de tiers de confiance, nombre d'intermédiaires limité et autodétermination des règles de la base de données par les acteurs eux-mêmes).

Risques	Actions
La blockchain n'est pas sans risque, elle peut être : – **Source d'insécurité juridique en l'absence d'encadrement légal précis** (ex : validité et opposabilité des opérations réalisées dans le cadre de la blockchain, responsabilité en cas de dysfonctionnement) ; – **La cible de cyberattaques innovantes et sophistiquées** (masquer l'infrastructure malveillante pour intégrer des virus, stocker des données volées ou collectées illicitement) ; – **Le support d'actes liés à la criminalité économique** (ex : blanchiment d'argent, financement du terrorisme, transfert de rançons dans le cadre de cyberattaques permettant de garder secrète l'identité du bénéficiaire).	– **Suivre les évolutions législatives et règlementaires ainsi que les lignes directrices publiées par les autorités compétentes** telles que la CNIL, l'Autorité Nationale de Sécurité des Systèmes d'Information, l'AMF ou l'ACPR ; – **Evaluer au par cas les types et niveaux de risques** en fonction de la nature de la blockchain (privé ou publique) et des finalités recherchées (conservation et partage de données, fonction de transaction digitale, fonction probatoire) ; – Prendre en compte dans l'évaluation l**es problématiques liées à la protection des données personnelles** et les recommandations de la **CNIL** en la matière ; – Considérer les **aspects liés aux droits de propriété intellectuelle et à l'absence de protection légale reconnue à certains composants de la technologie.**

3.3 Cloud

Opportunités : flexibilité, rapidité et adaptabilité permettant aux entreprises de choisir une solution personnalisée.

Risques	Actions
– **Dépendance technique** vis-à-vis d'une solution pouvant s'avérer défaillante (continuité du business et sécurité des données stockées) ; – **Hébergement dans des pays situés en dehors de l'EEA et des exigences strictes en matière de transferts** ; – **Réversibilité et portabilité des données**.	– **Identifier en amont les besoins et les attentes** et les refléter dans la demande de proposition (RFP) ; – **Evaluer les capacités et garanties des prestataires** envisagés (ie analyse d'impact juridique, opérationnel et technique) y compris sur les garanties en matière d'hébergement en dehors de l'EEA et les palliatifs implémentés ; – **Sécuriser les contrats** en (i) intégrant des **obligations de sécurité et d'hébergement** suffisamment robustes pour se conformer aux exigences du RGPD ; (ii) couvrant les étapes de **réversibilité des données** ; et (iii) prévoyant **des niveaux de services et des pénalités suffisamment dissuasives**.

3.4 Signature électronique

Risques	Actions
– **Risques liés à la fiabilité du mécanisme et à la preuve en cas de contestation**.	– **Comprendre les différents types de signature électronique (simple, avancée, renforcée)** reconnus en droit français et à leur force probatoire ; – **Evaluer les enjeux et la complexité de chaque opération concernée** par le recours au processus de signature électronique avant de désigner une forme de signature.

Vos contacts :

Laurie-Anne Ancenys
Head of Tech & Data – Paris
Tel +33 1 40 06 53 42
laurie-anne.ancenys@allenovery.com

Carla Hemery
Associate – Paris
Tel +33 1 40 06 53 48
carla.hemery@allenovery.com

Dalila Korchane
Associate – Paris
Tel + 33 1 40 06 54 82
dalila.korchane@allenovery.com

Juliette Mazilier
Associate – Paris
Tel + 33 1 40 06 51 37
juliette.mazilier@allenovery.com

Présence mondiale

Allen & Overy est une structure internationale d'avocats d'affaires qui compte près de 5800 personnes, dont environ 590 associés, présents dans plus de 40 bureaux à travers le monde. La liste à jour des bureaux d'Allen & Overy est disponible sur www.allenovery.com/global_coverage.

Allen & Overy signifie Allen & Overy LLP et/ou ses entreprises affiliées. Allen & Overy LLP est un limited liability partnership enregistré en Angleterre et au pays de Galles sous le numéro OC306763. Allen & Overy LLP est autorisé et réglementé par la Solicitors Regulation Authority d'Angleterre et du Pays de Galles.

Le terme « associé » désigne un membre d'Allen & Overy LLP ou l'un de ses salariés ou consultants ayant un statut et des qualifications équivalents ou un individu ayant un statut équivalent dans l'une des sociétés affiliées d'Allen & Overy. Une liste des membres d'Allen & Overy LLP et des personnes non-membres ayant la qualité d'associé peut être consultée à notre siège social One Bishops Square, London E1 6AD.

FR
CS2401_CDD-75878_ADD-112551