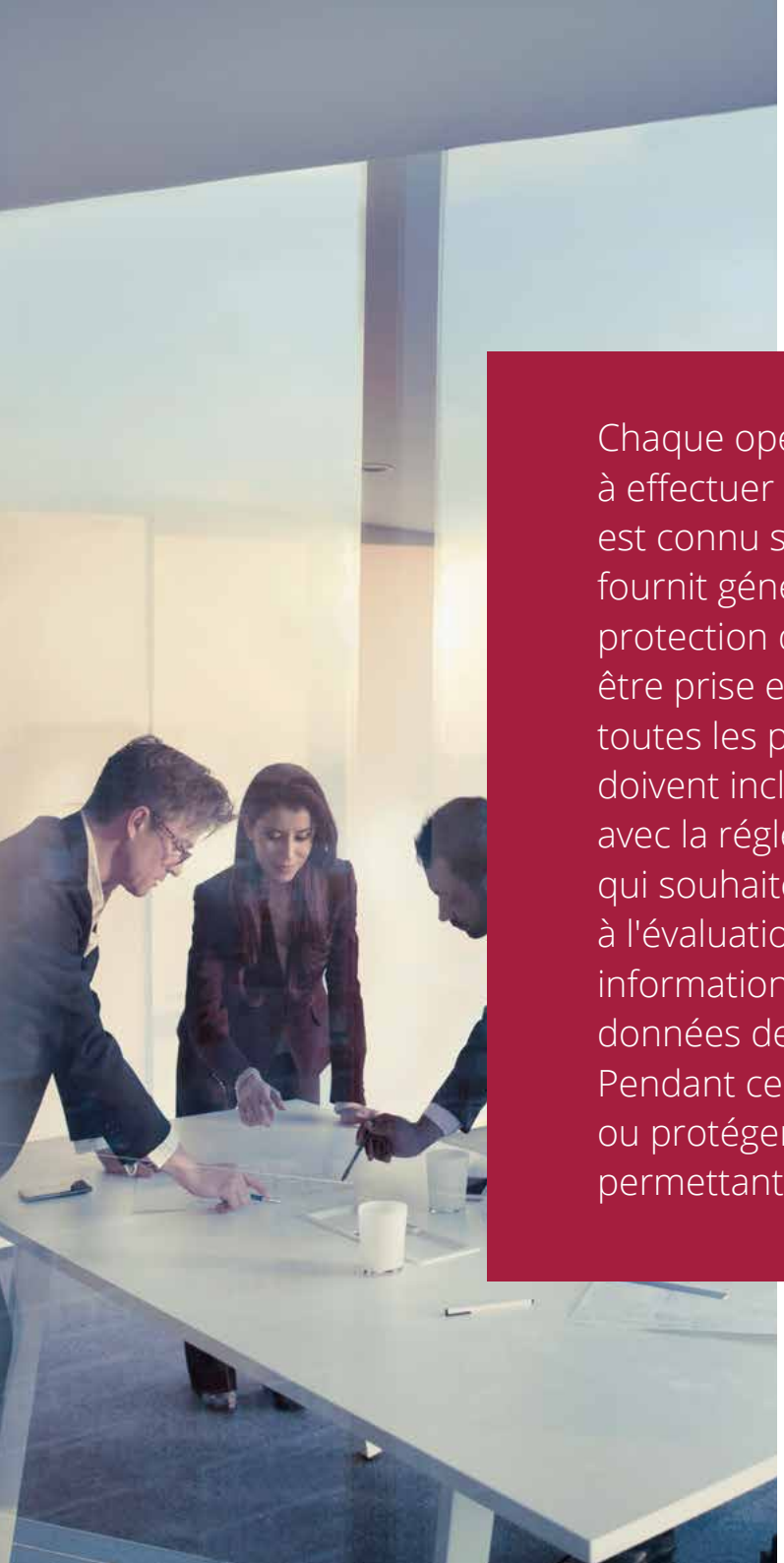
GGV Avocats . Rechtsanwälte

Drooms

DROOMS LIVRE BLANC

Gestion de la sécurité et de la confidentialité des données dans les opérations de due diligence

drooms.com



Chaque opération de fusion-acquisition inclut une étape essentielle qui consiste à effectuer une analyse juridique et financière de la société cible. Ce processus est connu sous le nom de due diligence. Pendant cette étape, la société cible fournit généralement à l'acheteur potentiel un large volume d'informations. La protection des données, y compris notamment, les données personnelles, doit être prise en compte à plusieurs égards et constitue une priorité élevée pour toutes les parties concernées. Tout d'abord, le ou les acheteurs potentiels doivent inclure dans leur analyse un audit de la conformité de la société cible avec la réglementation sur la protection des données. D'autre part, le vendeur, qui souhaite fournir aux acheteurs potentiels toutes les informations nécessaires à l'évaluation du prix et du risque, devra leur fournir des documents et des informations contenant des données personnelles ou, plus généralement, des données de nature confidentielle et/ou couvertes par le secret des affaires. Pendant ce processus complexe, comment respecter les contraintes légales et/ou protéger les droits des tiers et/ou les intérêts de la société cible, tout en permettant aux acheteurs potentiels d'en avoir une vision claire et exhaustive ?

Toutes les questions importantes

Plusieurs questions doivent être prises en compte, notamment :

1. Pour qualifier les données et déterminer leur criticité : les données fournies entrent-elles dans le champ d'application des réglementations sur les données personnelles, telle que le RGPD ? Les informations partagées sont-elles couvertes par le secret des affaires ou une obligation de confidentialité (intrinsèquement ou liées à un accord de confidentialité) ?

2. Quelles mesures techniques et organisationnelles seront mises en œuvre afin de garantir la sécurité et la confidentialité des données (sur la base de l'Article 5 (f), Article 24(1) et Article 32 du RGPD, de la réglementation sur le secret des affaires ou en vertu d'un accord de confidentialité auquel la société cible est partie) ? Entre aussi en jeu :

- Le choix du prestataire d'hébergement et sa conformité aux éventuelles exigences légales (notamment l'Article 28 du RGPD) ;
- L'anonymisation ou la pseudonymisation des données
- La sécurisation et la limitation de l'accès aux données et informations à un groupe de personnes ou groupes de personnes dûment autorisées dans des conditions strictement définies (gestion des droits d'accès, conclusion d'accords de confidentialité assortis de sanctions en cas de violation, etc.)

Quelles données doivent être considérées comme « confidentielles » et donc bénéficier d'une attention et d'une protection particulières ?

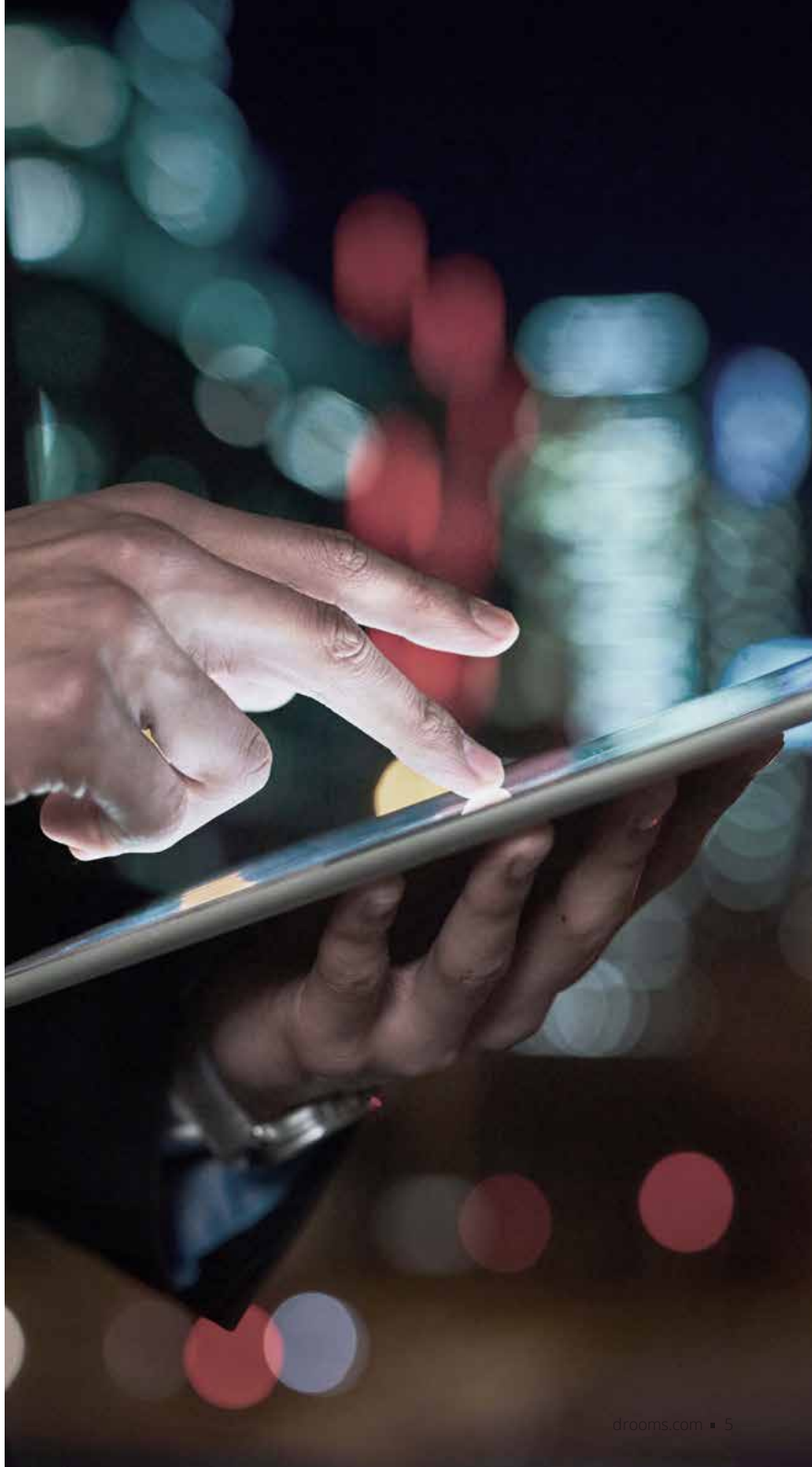
Pour les processus de due diligence, la société cible fournit généralement différents types de documents et d'informations. Certains de ces documents contiennent des informations sensibles juridiquement et confidentielles , ou parce qu'elles ont été classées comme telles. Les données fournies peuvent être classées dans différentes catégories :

a. Données couvertes par le RGPD

Ce règlement accorde un statut de protection élevé aux données à caractère personnel.

D'après le RGPD, toute information relative à une personne physique identifiée ou identifiable doit être traitée comme une donnée à caractère personnel. Le règlement européen précise qu'une personne physique identifiable est « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (Article 4 (a) du RGPD).

Dans le cadre d'un processus de due diligence, les informations suivantes peuvent être partagées avec des acheteurs potentiels : données sur les employés, les organes de représentation des employés, les informations relatives à l'équipe de direction, les informations relatives aux clients (et plus particulièrement si la cible est une entreprise B2C), etc.



Conformément à la législation européenne, dès lors que des informations peuvent être qualifiées de données personnelles, leur traitement est soumis à certaines obligations (et notamment leur stockage dans le cloud, leur communication sur une plateforme de partage, leur téléchargement, etc.).

› **Déterminer la base juridique du traitement des données :** selon le RGPD, le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est satisfaite (Article 6 §1 du RGPD) :

- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Dans le cadre des données mises à disposition des acheteurs potentiels, le traitement de ces données sera le plus souvent fondé sur les intérêts légitimes poursuivis par le responsable du traitement, c'est-à-dire la société cible, un tel intérêt légitime consistant, par exemple, à fournir des informations complètes à un acheteur potentiel. Toutefois, il appartient au responsable du traitement d'évaluer au cas par cas la licéité du traitement des données.

- **Respecter le principe de minimisation des données :** le responsable du traitement ne traite les données que de manière adéquate, pertinente et limitée à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (Article 5 du RGPD). Par conséquent, les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens (voir Raison 39 du RGPD).

Dans le contexte d'un processus de due diligence, cela implique que seules les données strictement nécessaires sont communiquées et que les données ne peuvent être stockées et communiquées que si elles sont destinées à permettre aux acheteurs potentiels de se faire une image fidèle de la société cible. En revanche, lorsque ces informations peuvent également être fournies sans données personnelles (par exemple, par anonymisation préalable des données), cette solution est privilégiée.

- **Intégrité et sécurité des données :** les données personnelles sont traitées d'une manière qui leur apporte un niveau de sécurité approprié, incluant la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) (Article 5 du RGPD). DSGVO).

Dans le cadre d'un processus de due diligence, cette obligation impose notamment à la société cible de ne sélectionner qu'un prestataire fiable en termes de sécurité. En outre, il appartient à la société cible de s'assurer que les informations ne soient communiquées qu'à un groupe restreint de personnes conscientes de la nécessité de protéger les données. Enfin, il est nécessaire de mettre en place une politique de conservation des données qui garantit leur suppression lorsqu'elles ne sont plus nécessaires.

Ces obligations seront supportées à la fois par la société cible et par le repreneur potentiel qui les traitera une fois les documents en ligne (par exemple en les téléchargeant et en les stockant, en les transmettant aux employés et/ou aux conseils en charge de l'audit, en les analysant, etc.). En outre, chaque activité de traitement exige le respect de conditions spécifiques.

b. Données et informations couvertes par le secret des affaires

Afin de préserver l'innovation et les informations stratégiques, une directive européenne sur la protection du secret des affaires a été adoptée en 2016. L'objectif de cette directive européenne est la protection du savoir-faire et des informations commerciales non divulguées (secrets des affaires) contre l'obtention, l'utilisation et la divulgation illicites.

Le 8 juin 2016, la directive 2016/943/UE sur la protection du secret des affaires a été transposée en France à l'Article L151 du Code de Commerce. Cet article définit la notion de secret des affaires ainsi que les conditions dans lesquelles les informations relevant de cette définition sont protégeables :

- « Est protégée au titre du secret des affaires toute information répondant aux critères suivants :

  1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ;

  2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ;

  3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret »

Toute information correspondant à cette définition est protégeable, ce qui signifie notamment que le propriétaire de cette information peut empêcher ou limiter sa diffusion ou son utilisation par des tiers et poursuivre les contrevenants.

Par exception au régime de protection, la loi française transposant la directive européenne, permet aux autorités judiciaires ou administratives de demander l'accès à des informations couvertes par le secret des affaires.

En revanche, le secret des affaires ne peut pas non plus être invoqué lorsque la divulgation de l'information sert à « révéler une activité illégale, une faute ou un comportement répréhensible dans le but de protéger l'intérêt général et de bonne foi ».

En outre, les informations couvertes par le secret peuvent avoir été obtenues conformément au droit à l'information et à la consultation des travailleurs ou de leurs représentants.

Les informations couvertes par le régime de protection peuvent comprendre, entre autres, le savoir-faire, les connaissances technologiques ou techniques ou les données commerciales.

Pour les processus de due diligence, la partie qui détient des informations dans le champ d'application des règles juridiques susmentionnées peut évaluer si leur partage avec un acheteur potentiel est essentiel et si des « mesures de protection raisonnables » doivent être adoptées pour qu'elles ne sortent pas du champ d'application de l'Article L151-1 du Code de Commerce français.

En juin 2016 en Allemagne, la directive européenne 2016/943/UE a été transposée dans la Loi sur la protection du secret des affaires (« Gesetz zum Schutz von Geschäftsgeheimnissen - GeschGehG »), ce qui nécessite une approche proactive de la part du titulaire légal afin de bénéficier de la protection juridique. Contrairement à la situation juridique antérieure, la simple intention de protéger le secret des affaires ne suffit plus. En effet, une information n'entrera dans le champ d'application de la Loi sur le secret des affaires et ne bénéficiera donc de la protection accordée par cette loi que si, et seulement si, elle fait l'objet de mesures proportionnées pour empêcher sa divulgation.

Si de telles mesures ne sont pas correctement adoptées par le détenteur, les informations à protéger seront non seulement accessibles en dehors du groupe des personnes autorisées,

mais elles ne seront plus protégées en tant que secret des affaires. Pour cette raison, il est fortement recommandé de mettre en place un concept de classification des secrets des affaires pendant les processus de due diligence. Répondant à ces nouvelles exigences, un mécanisme protège le cédant, qui peut avoir un intérêt direct à ne pas divulguer facilement des informations contenant des secrets des affaires potentiels de la société cible, d'une part, et l'acquéreur potentiel, d'autre part, de sa responsabilité pour divulgation d'informations.

Pour éviter que cela ne se produise, les listes de clients, les idées novatrices, les dessins techniques et autres secrets commerciaux ne devraient être disponibles dans une dataroom qu'en cas de nécessité et, le cas échéant, uniquement accessibles par un groupe limité de personnes. Les données pertinentes doivent être spécifiquement identifiées comme confidentielles et, si nécessaire, être protégées par chiffrement.

En outre, pour permettre au détenteur du secret de documenter les mesures proactives prises pour protéger les informations, les différents participants au processus de due diligence devraient signer un accord de non-divulgation. Seul un groupe restreint de personnes devrait avoir accès aux informations concernées.

c. Données et informations couvertes par un accord de confidentialité auquel la société cible est partie.

La société cible peut, dans le cadre de ses activités, avoir obtenu des informations de sociétés tierces et s'être engagée à assurer un certain niveau de confidentialité pour ces sociétés tierces.

En vertu de ces accords de confidentialité, qui peuvent être unilatéraux ou bilatéraux, les parties s'engagent généralement à traiter de manière confidentielle les informations que les parties apportent dans le cadre de l'accord. Cela implique généralement que les informations concernées ne peuvent être divulguées à des tiers sans l'accord exprès de l'autre partie.

Dans la plupart des systèmes juridiques, le non-respect des obligations/interdictions contractuelles peut être sanctionné par des dommages et intérêts.

C'est pourquoi, dans le cadre d'un processus d'acquisition, la société cible doit, avant de divulguer toute information, vérifier si les données sont librement communicables ou couvertes par un accord de confidentialité.

d. Toutes les autres données et informations détenues par la société cible, et qui sont protégées d'une autre manière (par exemple, dans le domaine des relations de travail, des droits de propriété intellectuelle et industrielle, etc.)

Certaines données peuvent être confidentielles par nature sans être classées comme secret des affaires. Par exemple, tel est le cas des informations fournies au Comité d'entreprise pour la recherche d'un repreneur lorsque la fermeture d'un établissement est envisagée (Article L1233-57-15 du Code du travail).

Ce type d'information peut également être divulgué pendant les processus de due diligence.

La menace croissante des violations de données

Très peu d'entreprises sont préparées à un incident de sécurité jusqu'à ce qu'il soit trop tard et que les systèmes et/ou les données soient compromis. Selon les dernières statistiques publiées par IT Governance, principal fournisseur mondial de solutions de gestion des cyber-risques et de la confidentialité, 729 incidents de sécurité ont eu lieu entre janvier et juin 2021, affectant 3 947 030 094 enregistrements dans le monde. Comment ces chiffres se situent par rapport à ceux des années précédentes ?

Les données montrent que, même si le nombre de violations peut augmenter, le nombre d'individus impactés diminue. Au premier semestre 2021, 118,6 millions de personnes ont été touchées par un incident de sécurité, soit nettement moins que les 2,5 milliards de victimes impactées en 2016. Selon le Centre de ressources sur le vol d'identité (ITRC) aux États-Unis, cette évolution peut provenir du changement d'orientation des cybercriminels, qui cherchent à obtenir des paiements de rançongiciel plus importants en ciblant des entreprises dépourvues de défenses suffisantes. L'industrie manufacturière et les services professionnels ont enregistré la plus forte augmentation de cybermenaces, tandis que le secteur du commerce de détail, par exemple, a enregistré une baisse des incidences.

Le Centre de ressources sur le vol d'identité et le Ministère américain de la Santé et des Services sociaux ont constaté que plus de 98,2 millions de personnes ont été affectées par les 10 principaux incidents de violation de données pendant le seul premier semestre 2021.

En décembre 2020, un accès non autorisé aux serveurs de la société Infinity Insurance Company a affecté les dossiers de 5,72 millions de personnes, incluant ceux des employés anciens et actuels. Des données incluant des numéros de permis de conduire et des informations de sécurité sociale, ainsi que des antécédents médicaux du personnel, ont été volées.

Jetfit, l'une des applis les plus appréciées dans le secteur du fitness, a été victime d'une violation de données en mars 2021. Elle a touché plus de 9 millions de comptes créés avant

septembre 2020. Les informations personnelles illégalement accédées comprenaient des adresses électroniques et IP ainsi que des mots de passe.

ParkMobile, une entreprise spécialiste des solutions de stationnement électroniques et numériques, a subi une violation provenant d'un logiciel tiers utilisé en interne. Signalé en mars 2021, l'incident a touché 21 millions de personnes. Des informations personnelles ont été consultées sans autorisation, telles que numéros de téléphone, adresses électroniques et informations relatives aux plaques d'immatriculation.

Nous savons maintenant qu'indépendamment de leur taille, toute entreprise est une cible potentielle, et même les géants de la technologie. Facebook a été victime d'un autre incident malgré les efforts déployés pour rectifier une violation subie au troisième trimestre 2019. Un nombre colossal de 533 millions d'utilisateurs dans 106 pays ont été affectés. Dans la majorité des cas, les vols incluaient numéros de téléphone, identifiants d'utilisateur, dates de création de comptes, biographies, dates de naissance, noms complets, localisations actuelles et antérieures, et statuts relationnels.

En avril 2021, Apple a également été visé. L'attaque par rançongiciel avec un paiement exigé de 50 millions de dollars aurait été menée par le groupe de pirates russes REvil, basé sur des plans d'ingénierie et de fabrication volés à son partenaire Quanta, dont certains ont déjà été publiés en ligne.

Les utilisateurs de Klarna, une société privée du secteur fintech, ont signalé en mai 2021 qu'ils étaient déconnectés de leurs comptes et reconnectés à d'autres, ce qui leur permettait d'accéder à des informations privées d'autres clients, notamment des informations sur des cartes bancaires et des adresses postales. Le nombre réel de clients touchés reste inconnu.

Le 14 mai 2021, des pirates ont volé 700 Mo de données concernant des patients à une agence gouvernementale irlandaise (The Health Service Executive – HSE), dont certaines ont été publiées en ligne. Les cybercriminels ont depuis exigé plus de 20 millions de dollars pour ne pas publier d'autres dossiers médicaux en ligne. L'agence doit maintenant faire face à des amendes réglementaires et à d'éventuelles poursuites judiciaires lancées par les personnes concernées.

Touchant les entreprises de tous les secteurs, et indépendamment de leur taille, le piratage de Microsoft Exchange semblait, à première vue, cibler des entreprises et des organismes publics. Selon Volexity, la société de sécurité qui a découvert le problème, l'attaque s'est très vite propagée, touchant principalement des petites et moyennes entreprises mal préparées.

Morgan Stanley, une banque d'investissement multinationale américaine et de services financiers, a été impliquée dans un incident de violation de sécurité en mai 2021, qui a impacté des fichiers clients sous la responsabilité de Guidehouse,

fournisseur de services de gestion de comptes. Des informations personnelles telles que des adresses, des noms, des numéros de sécurité sociale et des dates de naissance ont été volées.

En juin 2021, les données de 92 % des utilisateurs de LinkedIn ont été mises en vente. Selon Privacy Sharks, un site web de classement de solutions VPN, 700 millions d'enregistrements ont été retrouvés sur un forum de hackers. Des noms, des adresses électroniques et des numéros de téléphone ont été volés, bien que contestés par ce service en ligne axé sur l'emploi.

Volkswagen Group of America est l'un des grands noms victimes d'une violation de sécurité qui a affecté 3,3 millions de personnes aux États-Unis et au Canada. Selon des informations divulguées par ce groupe en juin 2021, une entité tierce a acquis des informations, destinées à des activités de vente et de marketing, par l'intermédiaire d'un fournisseur utilisé par d'autres constructeurs et concessionnaires automobiles, dont Audi. Parmi les clients et prospects affectés, les données sensibles de 90 000 individus ont été compromises, incluant leur numéro de permis de conduire. Les données d'autres personnes ont été exposées, telles que noms, adresses électroniques, adresses postales, numéros de téléphone, dates de naissance, numéros de sécurité sociale ou d'assurance sociale, numéros de compte ou de prêt, numéros d'identification fiscale et informations sur leur véhicule.

Manque de préparation des entreprises

Selon une étude publiée par FireEye, fournisseur de solutions de cybersécurité, plus de la moitié des entreprises dans le monde ne sont pas préparées pour répondre à un incident de sécurité. Cyber Trendscape a interrogé 800 RSSI et cadres supérieurs en Europe, en Amérique du Nord et en Asie. D'après son rapport 2020, 50 % des dirigeants interrogés estiment que leur entreprise est mal équipée pour faire face aux cybermenaces. En outre, 29 % des entreprises ont révélé l'absence de tests complets, avec des lacunes importantes dans leurs défenses.

Un grand nombre des personnes interrogées estiment que les cybermenaces continueront de progresser en fréquence et en gravité au fil du temps. Le rapport annuel Cost of a Data Breach 2021, publié par le Ponemon Institute et IBM Security, fait état d'une augmentation significative du coût total moyen de chaque violation de données au cours des derniers mois, en partie en raison des directives sur le télétravail rendu nécessaire par la pandémie du COVID-19.

Quels sont les facteurs à l'origine de ces violations de données ? Au-delà des vulnérabilités des systèmes informatiques, le facteur humain joue souvent un rôle déterminant.

Des risques importants

Une seule attaque de cybersécurité peut entraîner des conséquences majeures à long terme pour les entreprises. Le préjudice réputationnel résultant d'un manque de confiance peut inciter les clients à se tourner vers d'autres entreprises, réduire les possibilités d'attirer de nouveaux clients, perturber la chaîne d'approvisionnement si des partenaires se retirent, affaiblir la confiance des investisseurs et, enfin, avoir un impact négatif sur les marges bénéficiaires et le cours des actions.

Un rapport analytique d'Aon et Pentland sur le risque réputationnel à l'ère de la cybernétique a montré à quel point les retombées peuvent être considérables, certaines entreprises faisant état d'une baisse de leur valeur sur le marché de 25 % en 12 mois après une attaque. Yahoo a été victime d'une violation en 2013, qui a eu un impact considérable sur le cours de son action et sa valorisation trois ans plus tard, lorsqu'elle a été rachetée par Verizon au prix réduit de 4,48 milliards de dollars.

Le géant de l'audit et de l'assurance PricewaterhouseCoopers (PwC) a fait état d'un manque de confiance persistant parmi les consommateurs interrogés. 69 % d'entre eux pensent que les entreprises qu'ils utilisent ne sont actuellement pas capables de se protéger contre des cyberattaques. Selon leur enquête, 87 % des consommateurs se tourneront vers un concurrent en cas d'incident de sécurité.

L'entreprise de télécommunications TalkTalk en a eu un avant-goût lorsqu'une attaque a impacté 150 000 de ses clients et lui a fait perdre plus d'un tiers de sa valeur et 100 000 utilisateurs en 2016.

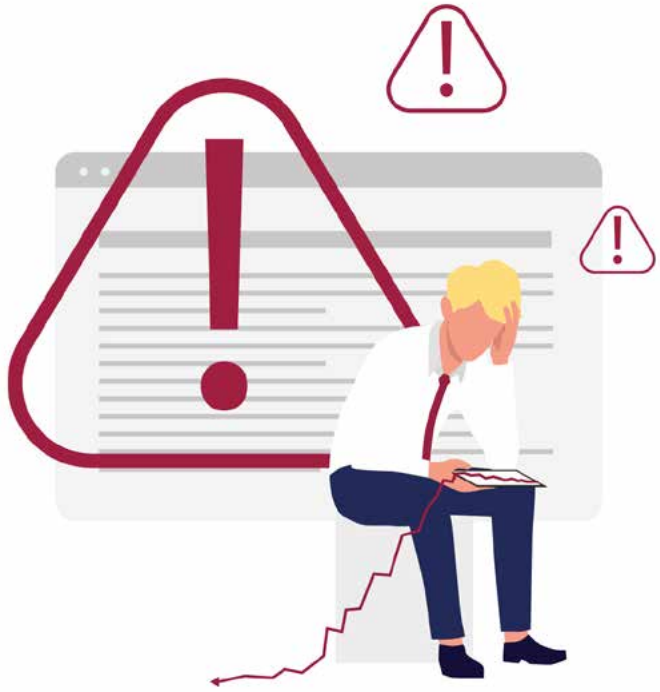
Les pertes financières dues aux systèmes d'indemnisation des clients, aux efforts de protection, aux investissements dans des contre-mesures, aux enquêtes, aux temps d'arrêt opérationnels et aux perturbations du commerce constituent également un risque majeur pour les entreprises qui subissent une violation ou un piratage.

En outre, personne ne peut se permettre de sous-estimer les pénalités et amendes réglementaires infligées pour non-conformité au règlement général sur la protection des données (RGPD), qui peuvent représenter 4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros (le montant le plus élevé étant retenu).

En hausse par rapport aux 3 000 milliards de dollars de 2015, les coûts mondiaux liés à la cybercriminalité augmenteront de 15 % par an au cours des cinq prochaines années, pour atteindre 10 500 milliards de dollars par an d'ici 2025, d'après les prévisions de Cybersecurity Ventures.

Les actions en justice intentées par des personnes affectées par une attaque de cybersécurité et cherchant à obtenir une indemnisation constituent un autre risque pour la survie de l'entreprise concernée. Une augmentation du nombre de recours collectifs générée par les pertes de données personnelles a été constatée aux États-Unis et au Royaume-Uni en particulier. Il est peu probable qu'elle se ralentisse, puisque la gravité des cas augmente. 145 millions de personnes dans le monde ont été touchées par la violation de données d'Equifax en 2017, qui a vu l'agence d'évaluation du crédit verser plus de 700 millions de dollars d'indemnités aux seuls clients américains concernés.

Enfin, les pertes d'informations personnelles très sensibles causées par une violation de la sécurité peuvent être encore plus préjudiciables que les atteintes financières et réputationnelles. Les données biométriques et génétiques, qui peuvent servir à identifier un individu, n'ont pas de prix pour les cybercriminels. Les dossiers médicaux, s'ils sont supprimés, peuvent avoir de graves répercussions sur le traitement médical d'un patient, voire sur sa vie.



Quelles mesures devraient être adoptées pour répondre aux exigences de confidentialité et de sécurité des données ?

En ce qui concerne les données personnelles, l'Article 32 du RGPD exige que les responsables du traitement prennent « toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

Des mesures similaires doivent/peuvent être adoptées pour protéger d'autres données sensibles et/ou confidentielles détenues par la société cible.

Choix du fournisseur de services dans le cloud

Si la technologie du « cloud computing » ou informatique dématérialisée peut être exploitée de diverses manières, le stockage dans le cloud reste l'une de ses applications les plus utilisées par les entreprises. Contrairement aux méthodes traditionnelles, le stockage dans le cloud repose sur le stockage virtuel des informations sur des serveurs distants. Il est basé sur un modèle informatique à la demande avec une connexion Internet pour partager et supporter l'accès aux données. Lorsque les données sont stockées dans le cloud, c'est-à-dire sur un serveur tiers, elles sont accessibles par plusieurs appareils, partout dans le monde, avec une connexion Internet stable, permettant aux entreprises de fonctionner plus rapidement et plus efficacement.

Son succès est dû en grande partie à une multitude d'avantages, notamment une sécurité accrue par rapport aux équipements sur place, qui sont sujets à des risques de détérioration et de destruction.

Cependant, les services de cloud computing ne sont pas tous égaux. Les risques liés à une mauvaise configuration de l'infrastructure restent un problème majeur. Le processus de due diligence prend donc une importance cruciale. En matière de gestion de documents, les plateformes de datarooms virtuelles (VDR) prennent le dessus sur les services génériques de partage de fichiers. Alors que les fournisseurs de services de partage de fichiers génériques ont tendance à se concentrer sur la facilité de partage des fichiers et leur protection pour les transferts initiaux des données, les VDR protègent également contre la modification, le traitement ou la perte de données à long terme. Elles intègrent en général toute une série de mesures de sécurité. Pour ne citer qu'un exemple, en 2016, Dropbox a dû admettre une fuite de mots de passe et d'adresses électroniques concernant plus de 68 millions de ses utilisateurs. Comme les datarooms virtuelles se concentrent sur la sécurité pendant et après le téléchargement, les violations de données sont nettement moins probables.

Les environnements de datarooms virtuelles bénéficient de systèmes de connexion sécurisés qui incluent ou proposent l'authentification multifacteur. En outre, ils offrent souvent une sauvegarde et une reprise après sinistre rapides, ce qui réduit les risques de temps d'arrêt coûteux. Pour les utilisateurs les avantages incluent :

- **Surveillance continue des données** – Alerte instantanée en cas d'activité inhabituelle, provenant d'une source externe ou interne.
- **Chiffrement avancé** – Protection des fichiers par chiffrement à haute sécurité, les données étant beaucoup plus difficiles à pirater et à lire.
- **Une meilleure conformité** – Stockage conforme à la législation la plus récente, notamment le règlement général sur la protection des données (RGPD).

L'infrastructure répond à une grande variété de besoins et peut être configurée et personnalisée en conséquence. Outre la prise en charge de fonctions telles que le partage et le stockage sécurisés, les processus de due diligence et les communications avec la direction, les VDR sont devenues une plateforme réputée pour l'efficacité de la gestion des portefeuilles. En proposant une solution tout au long du cycle de vie de leurs actifs, les utilisateurs peuvent résoudre les problèmes liés aux lacunes des données et aux différents formats de fichiers.

Comment Drooms traite-t-il les informations transmises via sa plateforme avec conformité au RGPD ?

› **En préservant la confidentialité et la sécurité des données, avec une infrastructure adaptée pour répondre aux exigences réglementaires.**

Depuis l'entrée en vigueur du règlement général de l'UE sur la protection des données, les exigences de la conformité sont de plus en plus critiques. Par exemple, les responsables du traitement des données doivent contrôler leurs fournisseurs actuels et n'engager que des partenaires fiables pour assurer les activités de traitement des données. En tant que fournisseur européen entièrement conforme au RGPD, dont le siège social est situé en Allemagne, Drooms n'a jamais eu besoin de recourir à des mesures de protection supplémentaires risquées telles que les clauses types. Drooms réalise ses activités et fonctions principales, incluant la facturation, l'informatique, les services à la clientèle et l'hébergement au sein de l'UE afin de minimiser les risques. L'hébergement, la facturation et/ou l'assistance informatique ne sont pas confiés à des tiers ou à des sous-traitants, qui ont tendance à être le principal domaine d'exposition au risque. Toutes les données sont stockées sur des serveurs propriétaires, certifiés ISO, en Allemagne ou en Suisse. Ils sont uniquement accessibles par les employés dédiés de Drooms pour effectuer des opérations de maintenance. Toutes les activités de traitement des données ont lieu exclusivement en Allemagne. Pour les clients suisses, un stockage spécial en Suisse est proposé.

Drooms effectue des analyses de vulnérabilité et des tests de pénétration internes. En cas d'urgence, son plan de reprise après désastre garantit l'intégrité des données. Drooms assure la confidentialité, la sécurité et la haute disponibilité des données grâce au concept N+1, au chiffrement des données au repos et à une architecture de sécurité multi-niveau.

Pour Drooms, la protection de la confidentialité de ses clients est une priorité essentielle. Par conséquent, aucune datarom ne conserve ni n'analyse des données personnelles à des fins de recherche et de réutilisation futures. Même en ce qui concerne la facturation, Drooms ne conserve que les informations minimales nécessaires au traitement des paiements dans sa base de données. Afin d'accroître la résilience face aux cyberattaques, une formation continue de sensibilisation à la sécurité est obligatoire pour l'ensemble du personnel.

Comment Drooms traite-t-il les informations transmises via sa plateforme avec conformité au RGPD ?

La fourniture d'outils administratifs pour gérer l'accès aux données et aux informations (y compris la définition des droits d'accès, la mise en œuvre d'une politique de suppression des données, etc.)

Conçue fondamentalement pour répondre aux exigences de sécurité et de résilience, l'architecture Drooms offre une série d'outils pour gérer l'accès contrôlé aux données. Parmi ses fonctions qui renforcent la sécurisation des processus de travail, citons seulement :

- Filtrage IP : limitation des accès à la dataroom au niveau du groupe et uniquement avec des appareils/ adresses IP spécifiques.
- L'authentification multifacteur : connexion à la plateforme Drooms grâce à un code de sécurité supplémentaire envoyé par SMS.
- Chiffrement haut de gamme : pour une sécurité optimale, les transferts de données ne sont possibles que via des connexions TLS avec les derniers protocoles et codes de chiffrement.
- Contrôle des droits et des autorisations des utilisateurs : attribution d'autorisations individuelles de révision, d'impression et/ou de stockage au niveau de l'utilisateur et du document, ainsi qu'un filigrane dynamique.
- Rapports détaillés : Drooms offre un reporting complet sur les activités de tous les utilisateurs de la dataroom.

Drooms utilise l'intelligence artificielle (IA) pour automatiser les flux de travail et améliorer l'efficacité. Pour garantir un niveau élevé de sécurité et de fiabilité, Drooms a développé et intégré sa technologie en interne, au lieu de dépendre de produits tiers. Drooms intègre les exigences de la confidentialité et de la gouvernance des données, ainsi que de la supervision humaine. Cela signifie que la boucle opérationnelle inclut toujours une personne compétente qui confirme les suggestions générées par l'intelligence artificielle, assurant ainsi la responsabilité et la qualité des résultats. De même, Drooms tient compte des principes directeurs pour concevoir des solutions intelligentes, visant la responsabilité, l'explicabilité, l'exactitude, l'auditabilité et l'équité.

Anonymisation ou pseudonymisation des données

Le RGPD n'exige pas des responsables du traitement des données qu'ils anonymisent les données, mais stipule expressément la nécessité d'assurer leur sécurité, avec notamment le chiffrement ou la pseudonymisation (Article 32). Avec la pseudonymisation, les données (personnelles) ne peuvent plus être attribuées à une personne concernée spécifique sans recourir à des informations supplémentaires, alors que dans le processus d'anonymisation, elles ne peuvent plus être liées à un individu.

Ces deux techniques, qui sont souvent difficiles à distinguer, peuvent donc être différenciées par le caractère irréversible du traitement appliqué aux données. Par conséquent, si elle est correctement mise en œuvre, l'anonymisation préserve les droits de la personne concernée, puisqu'elle fait perdre aux données leur caractère personnel.

Toutefois, avant d'envisager l'une ou l'autre technique, il est nécessaire de déterminer si le processus doit être irréversible ou non, ce qui dépend de la nature et de la sensibilité de ces données.

Sécuriser les accès tiers aux données par des accords de confidentialité

Les accords de confidentialité sont généralement signés par la partie divulgatrice et la partie destinataire. L'accès à la dataroom peut également être soumis à l'acceptation d'un accord de confidentialité.

Les accords de confidentialité incluent généralement les clauses suivantes :

- Définition : la clause stipule la portée de la confidentialité applicable dans le cadre du projet envisagé par les parties.

- Portée : la clause définit les droits et obligations de chaque partie en ce qui concerne les informations confidentielles. Les parties s'engagent généralement à respecter la confidentialité pour toutes les parties impliquées dans le projet (y compris leurs employés, consultants, agents).

- Exclusions : sont généralement exclues du champ d'application de accord de confidentialité les informations (i) qui sont dans le domaine public au moment de la divulgation, ou tombent dans le domaine public après la divulgation autrement que par un acte ou une omission du destinataire ; (ii) le destinataire peut prouver qu'elles étaient légalement en sa possession au moment de la divulgation et qu'elles n'ont pas été acquises directement ou indirectement auprès de la partie divulgatrice ; (iii) elles ont été obtenues légalement auprès de tiers autorisés à les divulguer ; (iv) elles ont été développées indépendamment par les employés du destinataire sans référence ni utilisation de ces informations ; (v) leur publication a été autorisée par un accord écrit de la partie divulgatrice ; ou (vi) la divulgation est requise par une loi ou en vertu d'une demande, d'une exigence ou d'une injonction gouvernementale ou judiciaire valide.

- Durée : si l'accord de confidentialité ne définit aucune durée, le contrat peut être considéré comme offrant une durée indéterminée et l'une ou l'autre des parties peut le résilier à tout moment sans compensation.

- Fin du contrat : engagement des parties à ne plus utiliser les données et à les restituer (délais et modalités à définir).

- Pas de transfert de droits de propriété : l'accord de confidentialité précise généralement que les informations confidentielles restent la propriété de chaque partie.

- Pas d'engagement ultérieur : l'accord de confidentialité précise généralement que la communication d'informations confidentielles ne constitue pas un engagement d'exécution du projet, qui fait l'objet d'un contrat spécifique.

- Clause de pénalité : la violation d'un accord de confidentialité fait généralement l'objet d'une indemnisation. Cependant, c'est à la victime de prouver le préjudice et son montant, ce qui peut soulever quelques difficultés. Parfois, les accords de confidentialité anticipent ce type de problème avec une clause de pénalité qui fixe le montant de l'indemnisation en cas de violation des dispositions.

- Loi applicable et juridiction : cette clause est importante lorsque les parties de l'accord de confidentialité sont de nationalités différentes.

Outre sa fonction principale, l'accord de confidentialité de chaque utilisateur peut également avoir une fonction de sensibilisation des utilisateurs à la confidentialité et/ou à la valeur de protection de certaines données.

Une fois l'accord de confidentialité signé, il incombe au destinataire des données de s'assurer que les engagements stipulés dans cet accord de confidentialité sont respectés par les employés et les consultants externes. Cela nécessite des clauses de confidentialité spécifiques insérées dans les contrats de travail ou de service. En outre, des mesures opérationnelles et techniques doivent assurer la sécurité des données. Lorsque les données sont personnelles, et que leur traitement est effectué avec des sous-traitants au sens de l'Article 28 du RGPD, un accord de traitement des données approprié doit être conclu avec le prestataire de services.

Pour toutes ces questions, il est utile de faire appel à un avocat, lui-même soumis à une obligation de confidentialité en vertu du code de déontologie applicable à la profession et passible de sanctions pénales.

GGV Avocats - Rechtsanwälte est un cabinet d'avocats parisien spécialisé dans les opérations transfrontalières.

Avec 20 avocats et 7 domaines d'expertise (M&A-droit des sociétés, droit du travail, fiscalité, immobilier, droit des affaires, contentieux, protection des données-IT-IP), GGV Avocats - Rechtsanwälte vous accompagne dans toutes les étapes de votre transaction : conduite de l'audit côté acheteur , la sélection des documents nécessaires au sein de la dataroom, la mise en place et la structure du contenu de la dataroom, les Q&R, la rédaction et la révision des accords de confidentialité, la rédaction des accords pertinents (SPA, transfert d'actifs, fusion, accord d'investissement, garanties et déclarations, management packages, pactes d'actionnaires...) et le processus de négociation jusqu'aux étapes de closing et de finalisation de la transaction.

Contributeurs GGV

Catherine Stary est avocate au barreau de Paris, certifiée CIPP-E et Conseil chez GGV Avocats. Catherine Stary est responsable du département protection des données et IP/IT chez GGV Avocats. À ce titre, elle conseille et assiste également diverses entreprises allemandes ayant des activités en France en qualité que DPO externe.

Caroline Blondel est avocate au Barreau de Paris et associée du cabinet GGV Avocats. Caroline Blondel conseille des entreprises internationales sur des questions de fusions et acquisitions, de droit des sociétés et de droit commercial concernant leurs filiales françaises.