Note de synthèse IDC

Parrainée par : **Brother**

Auteur :

Jacqui Hendriks

Mars 2018

Assurer la confidentialité des données : l'évolution du défi de gestion de l'impression et des documents

De nombreuses sociétés ne parviendront pas à se conformer à la nouvelle législation en matière de sécurité et de confidentialité des données, car elles auront négligé les éventuels facteurs de vulnérabilité liés à l'impression. Un environnement d'impression non sécurisé est un environnement informatique non sécurisé.

Cette note de synthèse IDC présente la nouvelle législation sur la confidentialité des données, les initiatives nécessaires pour s'y conformer, et les mesures spécifiques nécessaires à la conformité des processus de gestion de l'impression et des documents.

Sécuriser les données des clients

Sous l'impulsion de l'innovation technologique, la façon dont les entreprises de toutes tailles reçoivent, traitent, utilisent et diffusent de l'information a considérablement évolué. Les entreprises reçoivent des quantités d'information exponentielles en version imprimée et dans des formats électroniques. Selon la recherche IDC, d'ici 2025, la quantité des données créées, saisies et reproduites s'élèvera à 163 zettaoctets (Zo), ou 163 000 milliards de gigaoctets (Go) - soit dix fois plus que les 16,12 Zo de données générées en 2016[1]. Pourtant, la législation sur la protection des données ne suit pas l'évolution de ces pratiques dans les milieux professionnels.

La capacité à exploiter ces données peut à la fois permettre d'attirer et de fidéliser les clients en améliorant leur expérience[2]. Cependant, en raison de l'inefficacité de la gestion de l'information, les entreprises ont souvent du mal à la retrouver[3]. Pire encore, si l'information n'est pas gérée correctement, le risque de voir des données sensibles tomber entre de mauvaises mains augmente. Cette situation peut entraîner des failles de sécurité qui exposent les données personnelles du public et des clients à des risques.

Les points de vulnérabilité incluent :

- La mauvaise utilisation des périphériques d'impression et des documents imprimés
- Les données conservées sur la mémoire interne d'un périphérique
- Les violations potentielles à partir des ports du périphérique
- Les documents non récupérés

La loi sur la protection des données est en cours d'actualisation pour tenir compte des nouvelles pratiques et des valeurs, y compris l'utilisation des

réseaux sociaux et autres services en ligne. La Directive européenne de 1995 sur la protection des données (95/46/CE) a vu le jour avant l'existence des nombreux modèles actuels de gestion en ligne, et bien avant l'avènement de du cloud et des réseaux sociaux. La nouvelle législation va imposer des sanctions considérables aux entreprises qui ne produisent pas un effort concerté pour atténuer les risques.

Actuellement, il est beaucoup question du Règlement général sur la protection des données (RGPD) de l'Union européenne (UE), mais de nombreuse autres réglementations européennes sont en préparation en matière de confidentialité, par exemple[4] :

Actuellement, il est beaucoup question du Règlement général 2016/679 sur la protection des données (RGPD) de l'Union européenne (UE), mais de nombreux autres éléments de législation européenne sont en préparation en matière de confidentialité dans l'UE.

- **La directive 2016/680** Va de pair avec le RGPD et s'intéresse au traitement des données personnelles, le but de cette directive est la prévention, la détection, la poursuite et la sanction d'infractions pénales. Il s'agissait précédemment d'une directive européenne, mais à partir du 6 mai 2018, elle sera transposée dans la législation nationale dans l'ensemble des 28 États membres de l'UE.
- **La directive relative à la sécurité des réseaux et des systèmes d'information (directive SRI) -** Elle a été adoptée par l'UE afin d'introduire une approche cohérente contre les cyberattaques visant les services essentiels tels que l'énergie, les transports, les banques, les infrastructures des marchés financiers, la santé, l'approvisionnement en eau potable, l'infrastructure numérique et les services numériques.
- **Le Règlement sur la vie privée** - Avec le RGPD, la directive « vie privée et communications électroniques » constitue le cadre juridique de la protection de la vie privée dans les communications électroniques pour les citoyens de l'UE, et concerne les communications sur les réseaux publics. Cette directive remonte à 2002, mais elle est en cours de révision pour intégrer les dernières avancées technologiques.
- **La directive sur les dossiers des passagers (données PNR) -** Cette directive concerne la pratique courante de collecte des données des passagers avant d'embarquer dans un avion. Les États membres doivent transposer la directive dans leur législation nationale au plus tard le 24 mai 2018. Les données personnelles recueillies dans le cadre des données PNR doivent être stockées pendant six mois, puis elles doivent être anonymisées et conservées pendant encore quatre ans et demi.

Bien qu'une partie de la nouvelle législation soit relativement générique ou spécifique à un secteur donné, elle aura dans son ensemble un impact sur la façon dont les entreprises gèrent les documents imprimés et les flux de documents à l'avenir.

Confidentialité et sécurité des données

Le RGPD 2016/679 définit une violation de données comme une « destruction accidentelle ou illicite, une perte, une modification, une divulgation non autorisée d'accès à des données à caractère personnel transmises, stockées ou

traitées d'une autre manière ». Cela représente un changement fondamental pour les lois de l'UE régissant les données personnelles et la vie privée de ses citoyens. Les sociétés internationales situées à l'extérieur de l'UE, y compris les sociétés britanniques après le Brexit, seront également visées si elles gèrent des données de citoyens de l'UE.

La logique du RGPD répond à deux objectifs principaux. Le premier concerne la mise à jour des lois sur la protection des données, et le second vise à harmoniser les règles européennes de protection des données sous une loi unique. Il s'appuie sur les principes suivants :

- Les sociétés ne sont pas propriétaires des données personnelles. La dernière législation conforte le droit des personnes à savoir si leurs données sont bien gérées et leur droit d'être informées en cas de perte, de vol, ou d'autres usages inappropriés ou lorsqu'une telle violation présente un risque élevé pour ces personnes (notifications obligatoires en cas de violation).
- Les entreprises doivent respecter le « droit à l'oubli » des personnes. Pour ce faire, les entreprises ont besoin de savoir où se trouvent les données de chaque personne dont elles collectent les données, dans quelle application ou dans quel équipement matériel. Cette législation exige également que toutes les informations soient établies de façon

uniforme dans tous les recueils de données sur l'ensemble des systèmes/plates-formes/équipements.

Plusieurs de ses exigences ainsi que celles d'autres législations imminentes sont potentiellement beaucoup plus strictes que les lois qu'elles remplacent. Les amendes pour non-conformité sont délibérément sévères ; elles se veulent « efficaces, proportionnées et dissuasives » d'après le texte du RGPD, mais l'objectif sous-jacent est de faciliter et de clarifier la mise en conformité pour tous les intéressés. La preuve des intentions et des efforts de l'entreprise pour se conformer revêtira beaucoup d'importance si l'autorité compétente doit enquêter sur une violation de sécurité.

La non-conformité peut avoir un impact négatif majeur sur la réputation d'une entreprise. En fait, le risque de réputation lié à la non-conformité est l'une des principales préoccupations par rapport au RGPD[5].

Pour répondre aux exigences de conformité, les entreprises ont quatre priorités principales en matière d'investissement[6] :

- Identifier les applications qui utilisent des données relatives à chaque réglementation
- Cartographier les données : l'évaluation et la classification des données
- Établir des processus de documentation
- Examiner et améliorer la gestion des identités et des accès

Le RGPD met l'accent sur la relation entre la sécurité des documents imprimés et la confidentialité des données. Il exige que certaines conditions soient respectées pour tous les documents imprimés et les flux de travail électroniques. Le RGDP exige un journal d'audit, que l'accès et le traitement doivent faire l'objet d'une autorisation, et que l'information doit être sécurisée, y compris les données conservées sur des périphériques d'impression. Le RGDP exige également que les processus soient correctement documentés dans des registres adéquats, que les journaux d'audit aident à atténuer les violations de sécurité ; mais en cas de violation, cela prouve que des mesures adéquates ont été mises en place pour l'éviter.

Le RGPD met l'accent sur la relation entre la sécurité des documents imprimés et la confidentialité des données. Il exige que certaines conditions soient respectées pour tous les documents imprimés et les flux de travail électroniques. Le RGDP exige un journal d'audit, que l'accès et le traitement fassent l'objet d'une autorisation, et que l'information soit sécurisée, y compris les données conservées sur des périphériques d'impression. Le RGDP exige également que les processus soient correctement documentés dans des registres adéquats, que les journaux d'audit aident à atténuer les violations de sécurité ; en cas de violation, cela prouve que des mesures adéquates ont été mises en place pour l'éviter

Les prestataires d'impression et de gestion des documents sont eux-mêmes obligé de se conformer à la réglementation sur la confidentialité des données et sont bien placés pour servir leurs clients. Cependant, la responsabilité du respect de la législation incombe en dernier ressort à chaque entreprise.

À ce jour, les entreprises ne semblent pas répondre aux exigences de conformité en termes d'impression, par méconnaissance de la législation, de son impact et des délais associés[7]:

- Il est surprenant que malgré l'entrée en vigueur prévue des amendes en 2018, au début de 2017, seulement 40 % des acheteurs de services d'impressions ignoraient ce qu'était le GRPD, tandis que 19 % en avaient connaissance mais ignoraient les délais. Les entreprises qui étaient au courant étaient sereines quant à l'atteinte de la conformité.

- De manière encore plus surprenante, parmi les acheteurs de services d'impressions au fait du RGDP, 51 % ne comprenaient pas qu'il y avait un impact majeur sur l''impression de document.

L'assurance que vos processus de gestion de l'impression et des documents soient conformes à la loi

Parmi les acheteurs de services d'impressions au fait du RGDP, 51 % ne comprenaient pas qu'il y avait un impact majeur sur l''impression de documents.

La sécurité organisationnelle est une grande priorité pour toutes les entreprises, des commerçants de détails aux grandes multinationales. Les trois principaux points sensibles à aborder en matière de sécurité sont les suivants[7] :

1. Planifier la continuité des activités et la reprise après sinistre.
2. Conserver de l'avance sur les attaques de plus en plus sophistiquées.
3. Rester en conformité et respecter les règlements.

En dépit de l'augmentation des incidents liés aux fuites de données personnelles et professionnelles, les entreprises prêtent peu attention aux obligations de conformité à la législation[7] :

- Les investissements en sécurité d'impression sont faibles ; plus de la moitié des entreprises consacrent moins de 3 % de leur budget de sécurité informatique à la sécurité de l'impression.
- En termes de projets d'avenir, les deux tiers des entreprises n'ont pas l'intention d'augmenter cette dépense au cours des 12 prochains mois, et seulement un tiers d'entre elles incluent la sécurité de l'impression dans leurs appels d'offres.

Du côté de l'offre, des solutions ont déjà été élaborées et visent à améliorer l'efficacité de gestion de l'impression et des documents des entreprises et à relever le défi de la conformité relative à la protection des données :

- Les entreprises ont indiqué qu'elles étaient très intéressées par l'acquisition de fonctionnalités de sécurité de l'impression - comme l'impression à distance et les solutions d'authentification et d'autorisation de l'utilisateur final - intégrées à leurs imprimantes multifonctions[3]. Ainsi, les entreprises peuvent limiter l'accès des employés à des informations spécifiques, en fonction du rôle et des responsabilités des employés. Il s'agit d'une mesure de conformité crédible visant à réduire le risque.
- La demande croissante de numérisation d'informations en vue de leur intégration aux flux de documents électroniques a donné lieu à une augmentation de l'utilisation des scanners. Selon une enquête IDC de 2017 sur le format imprimé en Europe, les numérisations vers les e-mails, vers les dossiers réseau et vers les solutions utilisée (par exemple, ERP, CRM) représentent toutes désormais un grand intérêt pour les entreprises. En outre, il y a une demande accrue concernant les imprimantes multifonctions intelligentes qui proposent des fonctionnalités de numérisation et un accès direct aux données stockées[3].

Les fournisseurs de solutions d'imagerie et d'impression n'ont pas négligé l'efficacité ni la sécurité de la gestion de l'impression et des documents. Ils offrent un éventail de solutions qui aident les entreprises à optimiser leur façon de gérer le processus de conformité.

Les fournisseurs de solutions d'imagerie et d'impression n'ont pas négligé l'efficacité et la sécurité de la gestion de l'impression et des documents. Ils offrent un éventail de solutions qui aident les entreprises à optimiser leur façon de gérer le processus de conformité, sans besoins de mobiliser des ressources supplémentaires, les aidant ainsi à se concentrer sur leur métier:

- **Solutions de gestion et de surveillance de l'impression -** Ces outils se sont avérés efficaces pour le suivi et les rapports sur l'utilisation des périphériques dans le cadre de l'évaluation de l'environnement d'impression lors des négociations d'achats/de contrats. Pour cette raison, plus de la moitié des entreprises (53 %) ont déployé ces solutions[8]. Ces solutions présentent également l'avantage de créer un journal d'audit pour identifier les documents imprimés et traités, où et par qui. Cette capacité à conserver un journal d'audit est un élément essentiel dans la prévention contre les principales violations de sécurité.
- **La sécurité d'accès et d'authentification -** 46 % des entreprises requièrent une authentification des employés avant d'utiliser un périphérique d'impression[8], par un code PIN ou par une carte d'accès à technologie NFC. Cette fonctionnalité est souvent obligatoire pour les services qui traitent principalement de sujets sensibles tels que les ressources humaines, les services juridiques ou financiers.
- **Sécuriser l'accès à l'impression à l'aide d'Active Directory :** Cette solution offre encore plus de sécurité grâce au verrouillage des fonctionnalités du périphérique physique, tout en permettant une plus grande souplesse, comme la définition d'une limite de temps pour collecter les travaux d'impression. Les documents non récupérés au niveau du périphérique peuvent poser un risque s'ils tombent dans de mauvaises mains.
- **Sécurité des périphériques d'impression -** Les entreprises sont de plus en plus préoccupées par le fait que des informations confidentiels stockés sur des réseaux de périphériques, puissent accidentellement se retrouver dans le domaine public[8]. Certains fabricants d'imprimantes veillent à ce que les utilisateurs ne puissent pas stocker des informations dans les périphériques, mais leurs donnent la possibilité de récupérer des documents à partir d'un serveur sécurisé ou d'un service de stockage dans le cloud. Les entreprises ont donc l'assurance que des documents ne peuvent pas être récupérés d'un périphérique, au cas où il y a un accès physique non autorisé.
- **Numérisation sécurisée -** Les mesures de sécurité ne sont pas seulement limitées à la sortie par impression. Les documents numérisés peuvent également être sécurisés sous forme de fichier PDF avec un code d'accès PIN ou en utilisant un protocole FTP sécurisé pour créer un flux de données sécurisé. Pour 20 % des entreprises l'accès des employés à des documents numérisés[9] est une source de préoccupation en matière de sécurité.
- **La sécurité de la communication des données -** Les périphériques utilisés pour l'impression, la numérisation ou d'autres tâches de

gestion des documents doivent être sécurisés par le suivis de normes de sécurité reconnues dans le secteur, comme Internet Protocol Security (IPsec) et TLS (Transport Layer Security). Ces fonctionnalités garantissent que les communications vers et depuis le périphérique sont authentifiées, confidentielles et sûres.

- **Menaces du réseau de périphérique d'impression -** Les entreprises doivent s'assurer que le périphérique d'impression n'est pas un point de vulnérabilité en appliquant le même niveau de sécurité qu'aux autres équipements informatiques tels que les ordinateurs portables et les tablettes.

Les entreprises devraient voir la mise en conformité comme une opportunité d'améliorer leurs processus, plutôt que de l'envisager comme une contrainte.

Des flux de travail simplifiés aideront les entreprises non seulement à respecter la réglementation, mais aussi de manière générale à traiter l'information plus efficacement au quotidien. En outre, les réductions de coûts peuvent aller de pair avec l'amélioration des processus pour répondre à la conformité.

Les réductions de coûts peuvent aller de pair avec l'amélioration des processus pour répondre à la conformité.

Quelques mesures à suivre pour assurer la conformité de la gestion de l'impression et des documents

Dans le cadre des initiatives qu'une entreprise doit suivre pour s'assurer de la sécurité de son activité et de sa conformité aux lois sur la confidentialité des données, voici une liste de 10 mesures pour aider à la mise en conformité :

- ☑ Auditez les politiques de sécurité et de confidentialité en cours, et adaptez-les aux exigences du RGPD, en veillant à ce que l'infrastructure d'impression fasse partie intégrante de cet audit.
- ☑ Identifiez au sein du personnel interne les compétences pertinentes ainsi que d'éventuelles lacunes en termes de sécurité et de confidentialité.
- ☑ Songez à demander à votre fournisseur de périphériques d'impression quelles ressources le service informatique peut exploiter afin de soutenir les initiatives de conformité.
- ☑ Sécurisez le réseau auquel vos imprimantes sont connectées.
- ☑ Protégez toutes les informations sensibles qui sont envoyées vers le ou les périphériques d'impression/de numérisation, ou qui y sont traitées.
- ☑ Assurez-vous que vos imprimantes ne soient pas sensibles aux logiciels malveillants et autres cyberattaques.
- ☑ Assurez-vous que des renseignements pouvant être confidentiels ne soient pas stockés sur des périphériques tels que les imprimantes.
- ☑ Mettez en œuvre un outil de gestion du parc de périphériques dans le cadre d'une gestion centrale permanente et de la surveillance des périphériques d'impression et de numérisation.
- ☑ Adoptez l'authentification des utilisateurs (y compris pour l'impression à distance) et l'autorisation au niveau du périphérique pour garantir une récupération sécurisée des documents confidentiels.
- ☑ Élaborez un plan permanent visant à surveiller, faire remonter, corriger et faire respecter les politiques présentes et futures relatives à la sécurité et la confidentialité.

Sources :

1. *Data Age 2025: The Evolution of Data to Life-Critical, Don't Focus on Big Data; Focus on the Data That's Big*, Livre blanc IDC, avril 2017
2. *What are the Top Priorities of LOBs and Industries in Western Europe?* IDC #EMEA43168117, octobre 2017
3. *Content Management Opportunity: Integrated Solutions vs Outsourcing*, IDC #EMEA43165417, octobre 2017
4. *An Overview of Incoming EU Privacy and Data Security Legislation*, IDC #EMEA42911917, août 2017
5. Sondage RGPD IDC EMEA, mars 2017
6. *IDC PlanScape: EU General Data Protection Regulation Compliance*, IDC #US42574817, juin 2017
7. *Low Investment in Print Security and Increasing Compliance Challenges Leave European Companies at Risk*, IDC #EMEA42819617, juin 2017
8. *Still Significant Opportunity to Address Print Infrastructure /Management Challenges*, IDC #EMEA43059617, septembre 2017
9. *Workplace Dynamics Drive Print and Document Management,* IDC #EMEA41529116, juin 2016

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
Londres
W5 5TH, Royaume-Uni
44.208.987.7100
Twitter : @IDC
idc-community.com
www.idc.com

Siège mondial : 5 Speen Street, Framingham, MA 01701, États-Unis Tél. : +1 508 872 8200
Fax : +1 508 935 4015
www.idc.com

A propos d'IDC

International Data Corporation (IDC) est le principal fournisseur mondial en matière d'information commerciale, de services de conseils et d'événements sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels de l'IT, les chefs d'entreprise et les membres de la communauté financière à prendre des décisions basées sur des données factuelles pour leurs achats de produits et services technologiques et leurs stratégies business. Plus de 1 100 analystes d'IDC partagent leur expertise mondiale, régionale et locale de la technologie, des possibilités et des tendances de l'industrie dans plus de 110 pays. Depuis 50 ans, IDC formule des conseils stratégiques pour aider ses clients à atteindre leurs principaux objectifs opérationnels. IDC est une filiale d'IDG, leader mondial du marché de l'information, de la recherche et de l'organisation d'événements consacrés aux technologies de l'information.