PRÉPAREZ-VOUS À LA LOI EUROPÉENNE DE PROTECTION DES DONNÉES

Organisez les données personnelles de votre entreprise et pérennisez votre plan de conservation des archives

IRON MOUNTAIN®

LIVRE BLANC

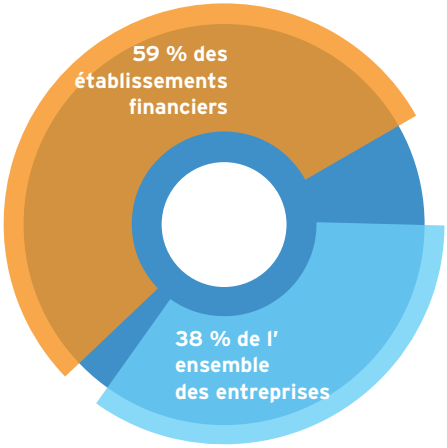
POURQUOI LIRE CE DOCUMENT

PARCE QUE LA MISE EN PLACE D'UN PROGRAMME EFFICACE DE GESTION DES INFORMATIONS ET DES ARCHIVES VOUS PERMETTRA DE VOUS PRÉPARER AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) BIENTÔT EN VIGUEUR.

COMPLEXITÉ CROISSANTE DE L'ENVIRONNEMENT RÉGLEMENTAIRE EUROPÉEN

L'ensemble des règlements européens qui touchent la conservation et la destruction des archives est complexe. Non seulement vous devez respecter les lois locales qui régissent la conservation des archives dans chaque marché où vous avez des activités, mais vous devez aussi prendre en compte les besoins commerciaux et opérationnels et la tolérance au risque de votre entreprise. Des équipes entières d'avocats se concentrent sur le suivi de la réglementation. Les récents chiffres de **Thomson Reuters**[1] montrent que 38 % des entreprises et 59 % des établissements financiers dans le monde occupent une journée complète par semaine à l'analyse des changements de réglementation.

Entreprises passant une journée par semaine sur le suivi de la réglementation



L'établissement de règles servant à organiser les données de votre entreprise est encore plus compliqué par la croissance exponentielle du volume et de la diversité des données créées et traitées par les entreprises et par le besoin grandissant d'optimiser leur valeur. En effet, **IDC**[2] prévoit que les données créées chaque année représenteront 40 Zo d'ici 2020, soit 50 fois plus qu'en 2010. En plus de tout cela, les entreprises devront procéder à la conservation et à la destruction des données conformément au nouveau **Règlement général de l'UE sur la protection des données**[3] (RGPD), qui entrera en vigueur en 2018.

Le nouveau règlement se concentre sur la protection du droit constitutionnel à la vie privée des résidents européens, mais ne définit pas d'exigences de conservation particulières. Cependant, le non-respect du règlement peut avoir des conséquences financières considérables et des répercussions sur la réputation, de sorte qu'il est important de conserver correctement les archives. Le règlement insiste sur le traitement des données personnelles dans son ensemble et prévoit des sanctions et des amendes plus importantes. À cela s'ajoute l'obligation de tenir à jour les politiques et règles relatives aux données, ainsi que les informations sur la localisation des données, en particulier pour les informations nominatives. Si vous n'agissez pas maintenant, il sera difficile de rattraper le temps perdu lorsqu'une erreur ou un oubli sera répréhensible et coûtera cher à votre entreprise.

[1] http://searchcompliance.techtarget.com/feature/Firms-face-regulatory-fatigue-higher-cost-of-compliance
[2] http://searchdatamanagement.techtarget.com/feature/Big-data-growth-increases-data-integration-degree-of-difficulty
[3] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

ENTRÉE EN VIGUEUR IMMINENTE DU RGPD

Conçu pour protéger les renseignements personnels dans un monde de plus en plus numérisé, le RGPD constitue une législation de poids à l'échelle européenne, qui aura des répercussions importantes sur les entreprises et leur façon d'utiliser et de conserver les données personnelles, quelle que soit leur forme.

Le règlement protège le droit d'un résident européen de décider si ses données personnelles peuvent être divulguées, quand, où, comment et à qui elles peuvent l'être, et aussi de quelle manière elles peuvent être utilisées. Il s'appliquera à toutes les entreprises basées dans l'UE, ainsi qu'aux activités de traitement des données de celles qui ciblent des données de résidents européens, et couvrira l'acquisition, l'utilisation, la transmission, le stockage, la destruction et la violation des données personnelles. Le non-respect du règlement entraînera rapidement de lourdes sanctions, avec des amendes pouvant atteindre **4 % du chiffre d'affaires annuel ou 20 millions d'euros**[4], selon l'éventualité la plus élevée.

POUR LES ENTREPRISES QUI VEULENT PROTÉGER LES DONNÉES PERSONNELLES CONFORMÉMENT À LA LOI, L'ÉPOQUE OÙ L'ON CONSERVAIT TOUT, POUR TOUJOURS, JUSTE AU CAS OÙ, EST RÉVOLUE.

Cependant, malgré le risque d'amendes élevées et le délai de mise en conformité de deux ans seulement, un **cinquième des entreprises**[5] en Europe ne se rendent toujours pas compte de la mesure dans laquelle elles seront affectées par ces changements ni de l'impact que ces derniers auront sur le stockage et le traitement des données personnelles.

Il est maintenant temps de vérifier où se trouvent les informations nominatives au sein de votre entreprise ou chez vos fournisseurs et de cerner vos obligations en matière de conservation et de destruction de ces informations.

Exemple d'amende pour une entreprise du FTSE 100 non conforme

Amende pour non-conformité
1, 21 milliard EUR

QUESTIONS À SE POSER DÈS MAINTENANT

- **Comprenez-vous suffisamment le nouveau règlement pour savoir si vous êtes prêt ou non ?**
- **Que sont les « données personnelles », où se trouvent-elles dans votre entreprise, qui a accès à ces données et comment assurez-vous la mise à jour des règles relatives à leur conservation ? Cela inclut les données dans les systèmes internes, les appareils personnels des employés, les archives hors-site et les armoires de classement, ainsi que les informations stockées par les fournisseurs, les sous-traitants et les partenaires commerciaux.**
- **Existe-t-il un comité de gouvernance de l'information dans votre entreprise ? Dans quelle mesure les responsables de la confidentialité et de la gestion des informations et des archives travaillent-ils avec leurs collègues pour préparer votre société au nouveau règlement ?**

Faites part de ces questions à vos collègues.

[4] http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf (article 79)
[5] https://www.ipswitch.com/blog/european-businesses-feel-the-financial-burden-of-preparing-for-gdpr/

TERMINOLOGIE ESSENTIELLE DU RGPD

1 Données personnelles et portée géographique, demandes d'accès par les personnes visées

Pour cerner quelles parties du règlement s'appliqueront à vos données et dans quelle mesure, il faut d'abord comprendre ce que sont les données personnelles. Les « données personnelles » sont des données liées à une personne, appelée la « personne visée », qui peut être directement ou indirectement identifiée selon ces données par un « responsable du traitement des données » dans une entreprise. Ces données regroupent aussi les identifiants de connexion à un appareil, les cookies et les adresses IP. En vertu du RGPD, les responsables des données doivent connaître l'ensemble des données personnelles dont ils ont le contrôle et doivent pouvoir démontrer qu'ils comprennent les risques relatifs à la protection des données.

2 Évaluation de l'impact sur le respect de la vie privée

En amont de tout projet susceptible d'augmenter les risques relatifs aux données appartenant à des personnes visées, une entreprise est tenue de procéder à une évaluation initiale des risques pour la vie privée afin de déterminer si une évaluation de l'impact sur le respect de la vie privée est nécessaire. Cette évaluation est beaucoup plus facile une fois que vous savez où se trouvent les données personnelles dans votre entreprise.

3 Demande d'accès par les personnes visées

Droit d'un individu de consulter et de recevoir une copie de ses données personnelles traitées par une entreprise (et ses partenaires commerciaux).

4 Droit d'effacement et de portabilité des données

Mieux connu sous le nom de « droit à l'oubli ». Les entreprises doivent être en mesure de repérer et de supprimer ou de transférer rapidement des données personnelles à la demande de la personne visée. Vous pouvez le faire seulement si vous savez exactement quels renseignements vous détenez et où ils se trouvent.

5 Avis et consentement

Nous avons assisté ces dernières années à une prise de conscience des citoyens qui demandent plus de transparence dans l'utilisation des données personnelles. Les autorités réclament aussi aux entreprises de démontrer qu'elles transmettent les avis nécessaires et demandent le consentement des personnes visées. Par défaut, le consentement pour le traitement des données doit être libre, spécifique, éclairé et explicite. Les individus doivent accorder leur consentement en connaissance de cause et de leur plein gré. Pour cela, les entreprises doivent être transparentes sur l'utilisation des données traitées et la durée pendant laquelle elles prévoient de les conserver, d'autant plus qu'elles doivent fournir une preuve d'avis et de consentement.

LA CONFORMITÉ DANS LA PRATIQUE : MONTREZ QUE VOUS SAVEZ

Pour respecter vos obligations réglementaires (attribution du droit d'accès, rectification de données personnelles erronées ou suppression de données personnelles obsolètes), vous devez d'abord savoir où se trouvent les données. Un plan des données physiques et numériques, notamment des données personnelles, est utile car il permet de localiser les données à l'échelle de l'entreprise pour garantir que les risques sont constamment évalués et maîtrisés.

Une fois que vous savez où se trouvent les données, vous devez savoir comment les utiliser et combien de temps les conserver. Pour cela, vous devez veiller à tenir à jour vos politiques de conservation, afin de garder et de détruire les données personnelles (et toutes les autres archives) uniquement lorsque vous y êtes contraint de manière justifiable par la loi, un règlement ou un contrat.

De plus, les informations que votre société souhaite extraire à des fins d'analyse ou de constitution de big data doivent être purgées des données personnelles qu'elles contiennent, puis agrégées pour être stockées dans des répertoires et non des archives.

LA PLUPART DES ENTREPRISES DANS LE MONDE AVAIENT L'HABITUDE, POUR DES RAISONS PRATIQUES, D'APPLIQUER LA MÊME PÉRIODE DE CONSERVATION POUR TOUTES LES ARCHIVES. AVEC L'ARRIVÉE D'UNE RÉGLEMENTATION PLUS STRICTE, IL EST NÉCESSAIRE DE REVOIR DE MANIÈRE APPROFONDIE LES POLITIQUES ET PROCÉDURES EN MATIÈRE DE CONSERVATION[6], AFIN DE RÉPONDRE AUX EXIGENCES ET D'ÉVITER DE CONSERVER TROP LONGTEMPS LES DONNÉES PERSONNELLES.

[6] http://www.ironmountain.co.uk/Knowledge-Center/Reference-Library/View-by-Document-Type/Best-Practices/D/Mini-Document-Retention-Guide-United-Kingdom-2015.aspx

APPRÉHENDER LE DÉFI RÉGLEMENTAIRE

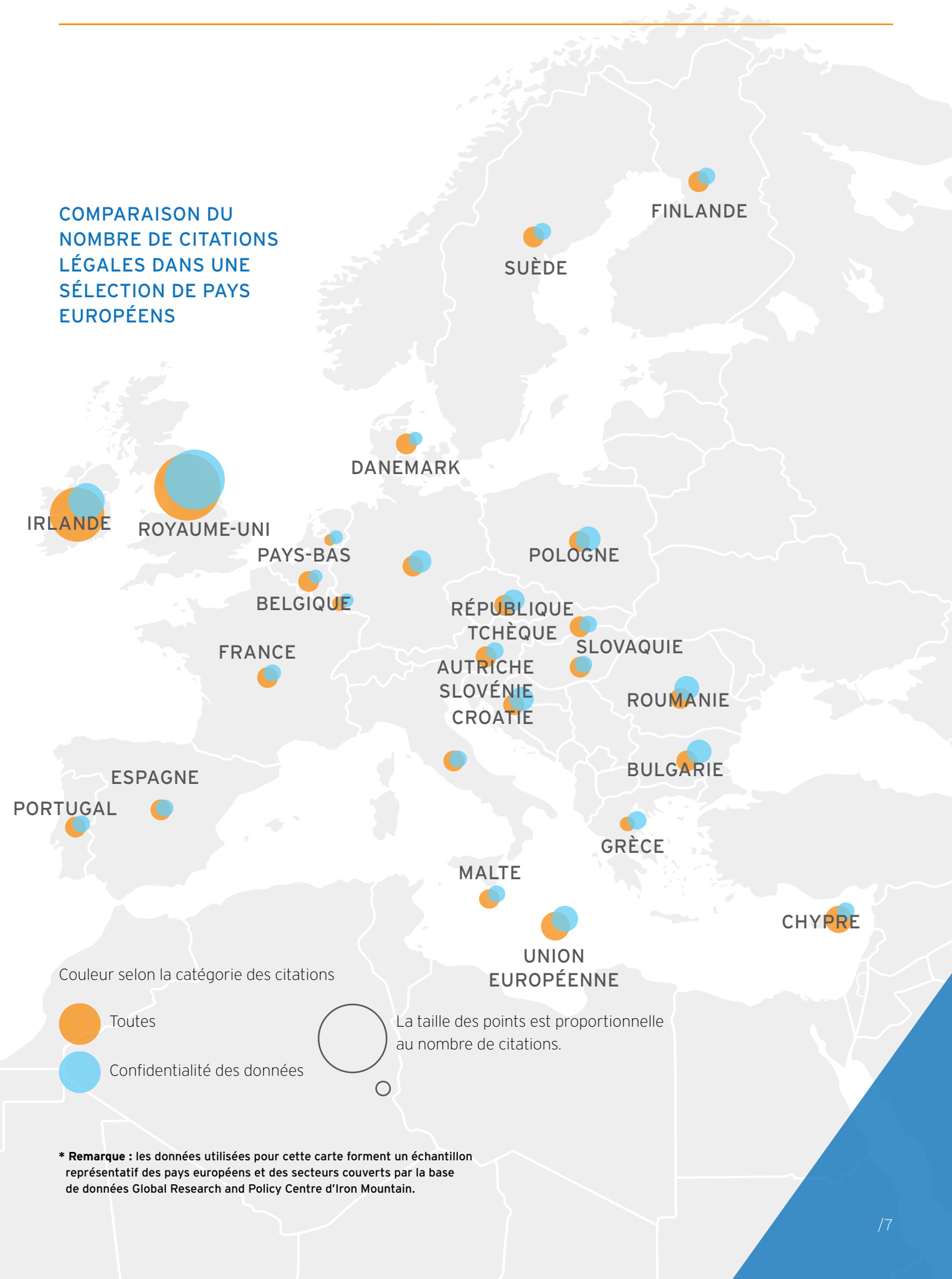
Un des défis auxquels les entreprises sont confrontées consiste à comprendre à quel point les données personnelles et potentiellement confidentielles sont répandues parmi l'ensemble de leurs données. Certains types d'archives, comme les documents relatifs aux comptes client et les dossiers d'employés, contiennent forcément des informations nominatives, mais d'autres types de documents, moins évidents, comme les contrats ou les dossiers d'actionnaires, sont aussi visés par le RGPD.

Afin de comprendre et de démontrer dans quelle mesure les lois et règlements actuels dans tous les secteurs ont un impact sur la conservation des données personnelles, nous avons étudié un échantillon de la base de données de **Global Research and Policy Centre d'Iron Mountain**[7], qui recense et résume 30 000 exigences en matière de conservation.

La carte ci-après représente la répartition de l'échantillon de données utilisé pour cette étude et illustre la proportion de règles qui pourraient s'appliquer aux données personnelles dans chaque pays.

[7] http://www.ironmountain.co.uk/Services/Records-Management-And-Storage/Global-Research-and-Policy-Center/Global-Research-Service.aspx

COMPARAISON DU NOMBRE DE CITATIONS LÉGALES DANS UNE SÉLECTION DE PAYS EUROPÉENS



*** Remarque :** les données utilisées pour cette carte forment un échantillon représentatif des pays européens et des secteurs couverts par la base de données Global Research and Policy Centre d'Iron Mountain.

LA THÉORIE MISE EN PRATIQUE

2018 n'est pas le temps des surprises

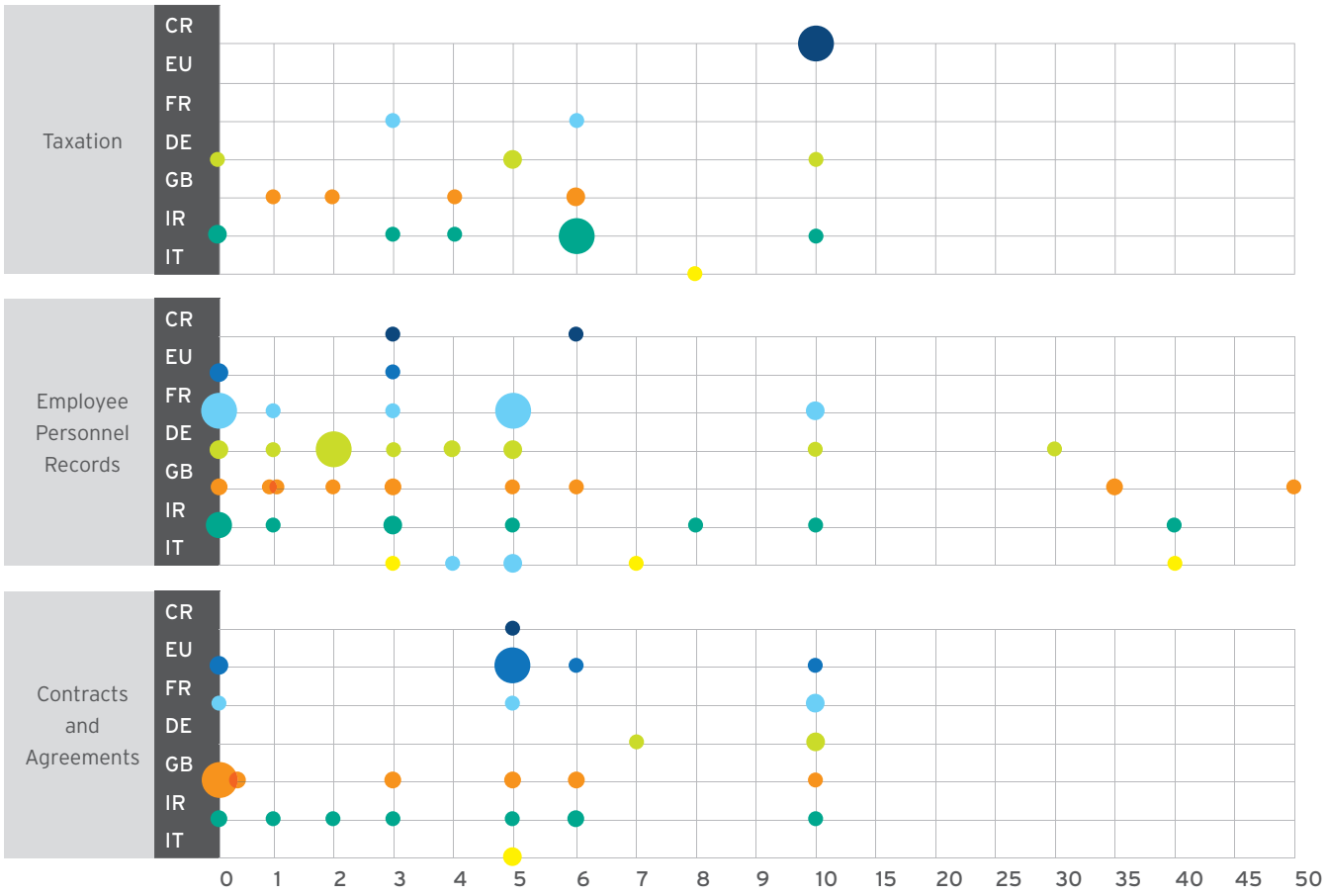
La conservation des archives n'est pas un nouveau défi pour les entreprises. Avec l'arrivée du RGPD et des sanctions qui lui sont assorties en cas de non-conformité, une conservation correcte des données est devenue essentielle. Pour échapper au courroux des régulateurs, il est essentiel de savoir quelles archives, numériques et physiques, se trouvent dans les unités commerciales, et plus particulièrement quelles archives contiennent des données personnelles.

Organiser les archives par fonction, catégorie et type permet d'appliquer plus facilement des règles fiables de conservation à chaque document et d'éviter de découvrir soudainement que vous avez perdu des données que vous auriez dû conserver ou que vous détenez des informations que vous n'êtes plus sensé garder.

Les mêmes politiques de conservation doivent s'appliquer aux informations qui passent entre les mains des employés, des sous-traitants et des fournisseurs.

Étant donné que la réglementation change et impose au fil du temps de nouvelles sanctions aux entreprises, vos politiques de conservation doivent être dynamiques et flexibles pour s'adapter aux environnements réglementaire et commercial changeants.

COMPARAISON DES PÉRIODES DE CONSERVATION MAXIMALES PAR TYPE D'ARCHIVES DANS UNE SÉLECTION DE PAYS EUROPÉENS



Les graphiques montrent qu'il existe des écarts importants de durée de conservation pour chaque type d'archives dans les différents pays d'Europe.

La complexité des exigences de conservation et les différentes périodes de conservation qui s'appliquent sont illustrées pour une sélection de pays européens. Cela montre également la portée de la réglementation à travers l'UE.

Une couleur par pays
- Croatie
- Europe
- France
- Allemagne
- Grande-Bretagne
- Irlande
- Italie

Taille selon le nombre
La taille des points représente le nombre citations pour la période de conservation correspondante.

Passez la souris sur le titre de chaque graphique pour obtenir des informations approfondies sur la conservation.

CE QUE NOUS POUVONS FAIRE

Une approche globale n'est pas la solution pour satisfaire aux obligations du RGPD. **Le service Global Research and Policy Centre d'Iron Mountain**[8] peuvent aider votre entreprise à automatiser le développement et le suivi de votre plan de conservation. Nos spécialistes des services aux professionnels utilisent une méthodologie de conseil éprouvée pour définir et concevoir une bibliothèque de recherche faite sur mesure en fonction du profil de risque et de la portée globale de votre entreprise. Dans le cadre de ce processus, nous élaborons un plan d'ensemble de vos données, mettant en évidence l'existence de vos données personnelles, confidentielles et sensibles. Ceci vous permettra de répondre plus rapidement aux demandes d'informations, d'identifier précisément les personnes dont les données doivent être détruites et de réagir à toute violation de façon plus ciblée.

Une fois que votre bibliothèque et votre plan des données auront été créés et que votre plan de conservation aura été élaboré ou mis à jour, vous recevrez des directives d'orientation à jour selon les localités où se déroulent vos activités, par l'intermédiaire du **Global Research and Policy Centre**, un portail dans le cloud qui contient votre plan de conservation.

Vous pourrez alors modifier vos politiques en conséquence afin de rester à jour et détruire en toute confiance les données qui atteignent la fin de leur période de conservation. Les spécialistes sont à votre disposition pour vous expliquer les changements de réglementation et vous aider à contrôler et à réduire les risques à toutes les étapes du cycle de vie des données, afin de satisfaire aux exigences du RGPD et même d'aller plus loin.

POUR OBTENIR DE L'AIDE

Si vous souhaitez en savoir plus sur le sujet, les spécialistes des services aux professionnels d'Iron Mountain et le **service Global Research and Policy Centre** peuvent aider votre entreprise dans sa préparation pour se conformer pleinement à la réglementation qui la vise.

Pour de plus amples informations, veuillez appeler au :

+32 2 712 2020

ou consulter notre **site**.

[8] http://www.ironmountain.co.uk/Services/Records-Management-And-Storage/Global-Research-and-Policy-Center.aspx

À PROPOS D'IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) est le leader des services de gestion et de stockage de l'information. Son parc immobilier de presque 80 millions de mètres carrés, réparti en plus de 1 350 sites dans 45 pays, permet à l'entreprise de servir ses clients avec rapidité et précision. En outre, ses solutions de gestion des archives, des donnée et des documents aident les entreprises à réduire leurs dépenses de stockage, à se conformer à la réglementation, à reprendre leurs activités après un sinistre et à tirer de meilleurs avantages concurrentiels de l'utilisation des renseignements. Fondée en 1951, Iron Mountain stocke et protège des milliards d'actifs d'information, notamment des documents commerciaux, des bandes de sauvegarde, des fichiers électroniques et des données médicales. Consultez le site : www.ironmountain.be/fr pour de plus amples informations.

IRON MOUNTAIN®