La conformité de la protection des données personnelles à l'échelle mondiale

Après quatre ans de travail, le Règlement général sur la protection des données de l'Union européenne (UE) a été publié le 4 mai 2016 dans le journal officiel de l'Union européenne[1]. Il définit officiellement une date de mise en vigueur[2]. Bien que le règlement soit entré en vigueur le 24 mai 2016, celui-ci ne s'applique qu'à partir du 25 mai 2018. Ce règlement a été élaboré en conjonction avec la directive européenne sur le traitement des données personnelles pour atteindre des objectifs communs sur la protection des données personnelles, des enquêtes et des poursuites judiciaires. Ce partenariat dévoile de radicales mises à jour des règles sur la protection des données.

La grande majorité des répondants (84 %) ont indiqué qu'ils anticipent que le règlement affectera leur organisation[3].

> **"Le nouveau règlement touche surtout les entreprises multinationales."**

Le nouveau règlement, tel que soumis par la Commission européenne en 2012 et convenu par le parlement européen en décembre de la même année, va remplacer la Directive 95/46/EC sur la protection des données.Au cours des quatre dernières années, les entreprises proactives ont mis en œuvrefor

Les processus et les procédures nécessaires sur la confidentialité des données selon la directive 95/46/EC. Les entreprises devront à nouveau mettre sur pied les nouvelles mesures de protection des données de l'EU lorsque le nouveau règlement rentrera en vigueur. Des amendes substantielles seront imposées aux sociétés qui ne seront pas équipées avec des processeurs et des contrôleurs de données conformes.

Ce nouveau règlement touche de nombreuses sociétés. Les entreprises qui comptent plus de 250 employés et qui traitent les données personnelles des citoyens européens seront soumises à ce nouveau règlement.Ce nouveau règlement concerne également tout traitement de données personnelles par les organisations de l'Union européenne et celles à l'extérieur de l'UE qui traitent des informations de résidents de l'UE. Si une organisation transfert des données personnelles à l'UE, elle sera touchée par ce nouveau règlement. Les règlements concernant les exportations seront également renforcés. Les entreprises concernées seront obligées soit de se conformer ou soit de renoncer à leurs clients de l'UE. Des peines sévères pour des infractions comprennent des amendes supérieures à 20 millions d'euros (environ 23 millions de dollars) et 4 pour cents du revenu global de la société.

Bien que de nombreuses entreprises de toutes tailles seront touchées par ce nouveau règlement, l'impact se fera surtout sentir auprès des entreprises multinationales. Les sociétés devront étendre la portée déjà très complexe de leurs systèmes informatiques à la transmission internationale de données personnelles.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Ilya Kabanov, Ph.D.
Il est un expert en technologie de l'information avec 15 ans d'expérience en informatique. Il a occupé des rôles dans la stratégie informatique, la gestion de projets en matière de technologie, de sécurité et de confidentialité des données dans des entreprises allant d'une start-up à une entreprise mondiale avec des chiffres d'affaire de 36 milliards de dollars. Actuellement, Kabanov est en charge d'assurer la conformité de la confidentialité des données personnelles et de la sécurité globale d'applications pour un fournisseur mondial d'automatisation et de gestion énergétique. En 2013, le magazine Kommersant l'a reconnu comme étant le meilleur directeur informatique dans l'industrie de la logistique et des transports en Russie. Kabanov est un membre de l'Institut des ingénieurs en électricité et en électronique. Il est également membre de l'Association internationale des spécialistes en matière de confidentialité. Il sert de juge lors du symposium des directeurs informatiques de MIT Sloan.

Transformer les coûts en de la valeur

En général, toute conformité est perçue comme un coût. Les entreprises efficaces génèrent avec succès de la valeur pour leurs clients en concevant et en déployant des programmes de protection des données personnels et de conformité.

> **“Chaque société recherche la conformité. Toutefois, celle-ci doit être réalisée de manière à soutenir la croissance et la rentabilité.”**

Par exemple, le principal fournisseur mondial d'automatisation et de gestion énergétique a proposé trois objectifs majeurs pour son initiative globale de conformité sur la protection des données personnelles :

1. Mitiger le risque de 1,2 milliards de dollars d'infraction aux règlements[4] de la protection des données personnelles dans l'Union européenne et les autres pays où la société conduit des affaires.
2. Activer et soutenir la croissance des recettes et la satisfaction des clients dans les domaines des solutions mobiles et de l'Internet :

Comment les dirigeants génèrent de la valeur par le biais de la conformité :
- en développant la satisfaction des clients et en établissant des relations de confiance avec ceux-ci ;
- en permettant la croissance des recettes ;
- en réduisant les coûts de conformité.

3. Parvenir à une réduction des coûts de la conformité concernant la législation sur la protection des données personnelles. Une façon de procéder est d'utiliser les règles de l'entreprise par le biais de la mise en œuvre de différentes méthodes de conformité (y compris l'auto-certification) concernant le risque posé par les applications et les systèmes informatiques impliqués dans le traitement des données personnelles.

En outre, la société croit que sa responsabilité globale dépasse les normes réglementaires. La société dispose de solides principes de conduite en matière d'éthique, d'écologisme et de responsabilité au niveau global. La responsabilité est l'objectif clé au cœur de la gouvernance de la société. Ceci détermine l'engagement de l'entreprise pour définir et répondre aux normes les plus élevées en matière d'éthique et de confidentialité. Cela lui permet de modeler l'avenir de l'industrie en introduisant dès aujourd'hui les meilleurs procédés de demain.

Chaque société recherche la conformité. Toutefois, celle-ci doit être réalisée de manière à soutenir la croissance et la rentabilité. Ce n'est pas une tâche facile. Chaque entreprise devra faire face à plusieurs défis pour atteindre la conformité.

Défis

Le nouveau règlement ainsi que les règlements nationaux sur la protection des données personnelles contraignent les organisations à développer et à déployer des plans concernant les risques et la conformité. Tout en restant conforme aux différentes législations nationales, ceux-ci s'étendent sur plusieurs départements internes tels que le département juridique, celui de la sécurité et de l'informatique. Bien qu'il existe différents points de vue sur les processus que les organisations mondiales peuvent adopter pour mettre en place et gérer les facteurs réglementaires et de conformité, les défis que les entreprises ont besoin d'examiner sont en fait très communs. Ce sont :

- **La complexité**—le volume et la complexité croissante des réglementations en matière de protection des données personnelles ont pris de l'ampleur, notamment dans l'Union européenne, les États-Unis et certains pays en voie de développement. es entreprises mondiales doivent non seulement se conformer à diverses réglementations au niveau national mais également à tous les aspects des affaires telles que les pays, les genres de données, les volumes et les divers lieux de résidence des processeurs de données.
- **L'agilité et la cohérence**—l'agilité est un facteur nécessaire. Les lois et les règlements changent constamment. Le temps nécessaire pour les nouveaux produits informatiques d'atteindre les marchés se rétrécit. La conformité avec ces changements doit également refléter un laps de temps concentré pour être efficace. Les entreprises doivent développer de la cohérence à leurs structures de conformité. Cela doit se produire en temps réel et refléter fidèlement les changements dans les nouvelles réglementations. Chaque entreprise a besoin de développer et de s'aligner sur les cycles rapides de livraison de produits et de systèmes informatiques. La conformité avec

les nouveaux règlements signifie qu'il faut s'assurer que tous les systèmes et processus sont conformes, non seulement lors de leur mise en œuvre, mais également tout au long de leur cycle de vie.

- **La disponibilité et les capacités des experts**— le manque d'expertise en matière de sécurité informatique et la rareté d'experts dans le domaine de la protection des données personnelles ralentissent et compliquent le processus de conformité. Les entreprises mondiales se battent pour le nombre limité d'experts qui peuvent implanter de complexes programmes de conformité en matière de protection des données. Elles rencontrent également des difficultés dans la formation des employés sur la protection des données personnelles.

Bien que les entreprises font face à de gros défis tels que l'échelle, les diversités géographiques, les conflits de priorités et de communications, leurs perspectives ne sont pas complètement sombres. Il y a certains facteurs qui aideront à établir avec succès un cadre de conformité.

Cadres de la vie réelle

Un exemple réussi de conformité a été démontré par une entreprise mondiale qui a introduit une certification pour assurer la sécurité et la conformité des applications et des systèmes. Elle garantit ainsi aux clients et aux employés une protection efficace de leurs données personnelles. Elle garantit également les droits conférés par la législation ainsi que la conformité aux normes de l'entreprise et de l'industrie. Le cadre a été conçu pour couvrir plus de 1 000 logiciels vendus chaque année. Ceux-ci emmagasinent des milliards d'enregistrements de données structurées et non-structurées. Ces données sont accessibles à des millions de personnes à travers le monde.

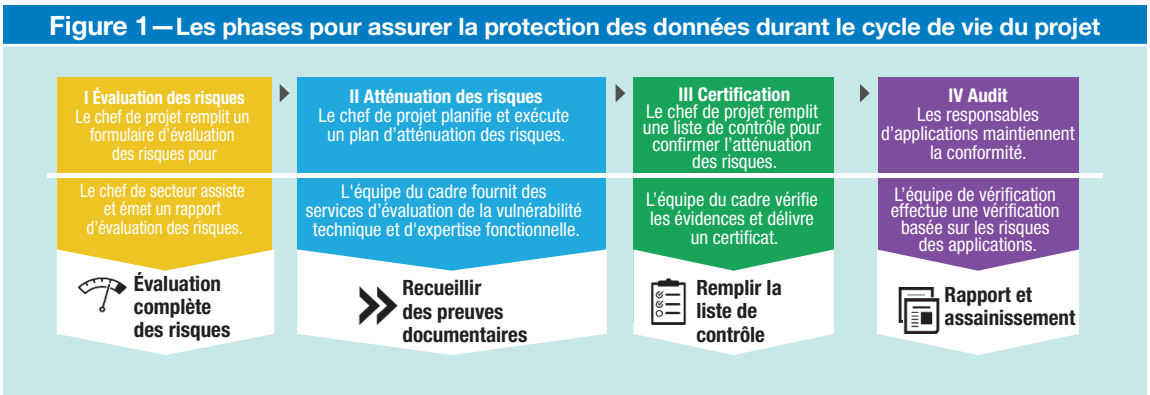
À un stade précoce du développement du cadre, il a été reconnu que le processus de conformité doit complètement couvrir le cycle de vie de l'application et doit assurer à chaque étape la confidentialité et la protection des données. Le cadre repose sur un processus en quatre étapes qui inclut l'évaluation des risques, l'atténuation des risques, la certification et l'audit après l'homologation (figure 1).

> *Le cadre repose sur un processus en quatre étapes qui inclut l'évaluation des risques, l'atténuation des risques, la certification et l'audit après l'homologation (figure 1). de communication multicanale sur toute l'année. Nous avons mis à profit des médias sociaux internes, des webinaires et des formations en ligne pour encourager l'adoption du cadre, la confidentialité des données et pour augmenter la sensibilisation des risques en matière de sécurité. Notre objectif était non seulement d'intégrer le cadre que nous avons conçu dans les processus existants mais également d'assurer que la conformité devienne une partie de la connaissance professionnelle des gestionnaires de projets et des équipes de conception d'applications.*
>
> – Le directeur de l'architecture informatique de l'entreprise

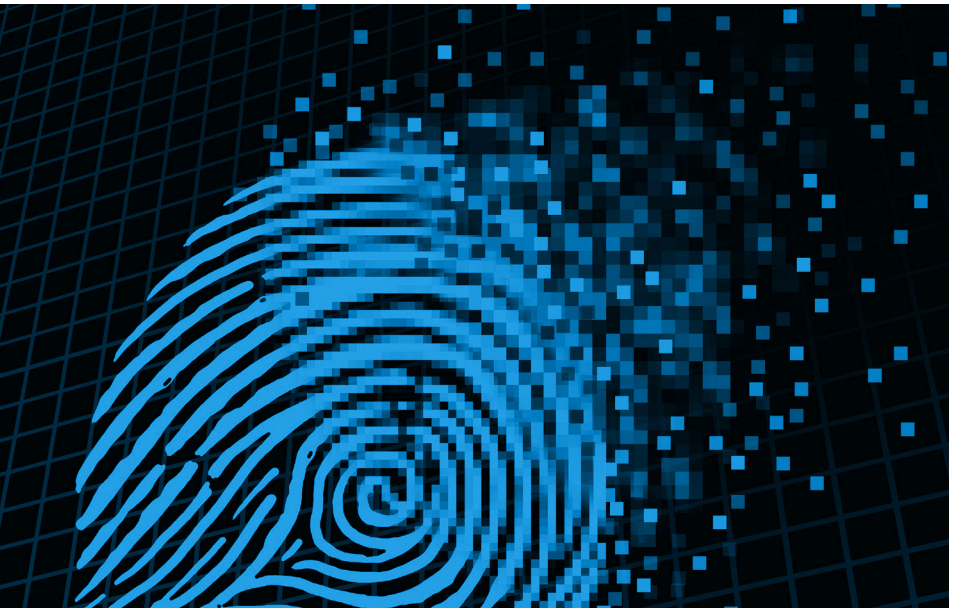
Il existe quatre principaux défis dans l'adoption de la conception du cadre :

1. La complexité des règlements internes et externes. Le cadre a pris en compte plus de 200 lois ainsi que diverses politiques, normes

Figure 1—Les phases pour assurer la protection des données durant le cycle de vie du projet



Source : I. Kabanov. Reproduit sous permission.



et lignes directrices. Le cadre les a alors simplifiées dans les procédures d'évaluation des risques, des recommandations et des contrôles.

2. L'échéance des politiques a requis la forte participation d'experts pour évaluer les risques et guider les équipes du projet dans la mise en œuvre et l'application des contrôles. Cela représentait un sérieux obstacle pour la mise à l'échelle du cadre. Par conséquent, l'équipe a abordé le défi en adoptant une démarche d'expérimentation. Cela a permis à l'équipe de développer de bons procédés et de les documenter dans les formulaires des lignes directrices destinés aux équipes du projet et aux responsables d'applications.
3. La complexité du cadre informatique existant dans lequel les données sont traitées est devenue un défi supplémentaire. En raison de cet obstacle, l'équipe a fourni beaucoup d'efforts dans l'apprentissage de l'architecture existante et la cartographie des données.
4. La mise en œuvre du programme sur une grande échelle, la diversité géographique du déploiement et les différents niveaux de sensibilisation sur la protection des données entre les 2 500 personnes réparties sur 24 fuseaux horaires ont créé un défi important pour le rapide déploiement du cadre.

Le cadre était le résultat d'un travail parfaitement orchestré et étayé par des employés représentant des secteurs fonctionnels clés sur tous les continents. L'équipe a travaillé sans relâche malgré les barrières culturelles et linguistiques et les fuseaux horaires tout en restant concentré sur la conception et le déploiement de ce cadre.

Les facteurs de succès

La conception et le déploiement de programmes de conformité varient considérablement. Chaque organisation doit s'assurer que la conformité soit correctement intégrée dans les processus organisationnels actuels. Plus l'organisation est complexe, plus il sera difficile d'intégrer les programmes de protection de la confidentialité dans l'ensemble de l'organisation.
Le plus haut niveau d'intégration d'un cadre de conformité dans les processus de gestion de programmes et de projets existants garantit la robustesse et l'exhaustivité de ses contrôles sans redondance. À titre d'exemple, le cadre doit être aligné avec les processus qui peuvent avoir différents noms dans les organisations tels que l'excellence du projet de bout en bout et la gouvernance du cycle de vie du développement du logiciel. La sécurité et la conformité ainsi que l'exécution des principes de protection des données personnelles et de la sécurité seront ainsi assurés à chaque étape du cycle de vie des applications de traitement de données.

La communication est un élément essentiel de l'intégration réussie du cadre dans les opérations et les projets d'une entreprise. La communication à grande échelle du projet est un exercice difficile. Pour réussir, les équipes ont besoin de travailler en partenariat avec différentes personnes. Elles doivent concevoir et mener une campagne de communication dans le cadre d'un processus de gestion du changement pour mieux faire connaître le cadre et éduquer les équipes du projet sur la confidentialité des données clés et des risques de sécurité.

La communication soutient la collaboration. Un sondage récent auprès de 550 experts informatiques de l'Association internationale de la protection des données personnelles

a indiqué que la communication est essentielle dans la lutte contre les vols de données. En effet, 90 pour cents des personnes interrogées ont considéré qu'une collaboration entre les différents départements de l'informatique, de la sécurité, de la protection des données personnelles et une équipe d'intervention aux infractions des données est critique pour atténuer le risque de vols de données[5]

La conformité concernant la confidentialité des données personnelles ne relève pas uniquement de la compétence des services informatiques. Toutes les facettes d'une organisation doivent être engagées à mettre en œuvre les nouvelles règles et règlements. L'intégration de ces nouveaux facteurs à travers tous les départements et à tous les échelons de l'entreprise est importante.

Au-delà de la conformité

Les chefs d'entreprise font preuve de leadership éthique dans leurs industries. Ils utilisent l'éthique pour générer des bénéfices et se différencier de la concurrence. Un cadre de conformité peut servir d'élément clé à la sécurité en ligne et aux initiativesde conformité. Ce cadre promeut la croissance des revenus et fournit un environnement sans faille, sûr et sécurisé aux clients et aux employés. Alors que les clients réclament des améliorations dans la productivité, la précision et l'efficacité, les entreprises doivent répondre à ces besoins par le biais de relations de confiance qui garantissent aux clients le plus haut niveau de confidentialité des données ainsi que l'intégrité et la disponibilité des informations.

En outre, les cadres de conformité peuvent jouer un rôle crucial dans la réduction des cycles de projet et dans les délais de livraison des produits pour soutenir la croissance stratégique de l'entreprise dans les domaines des solutions mobiles et des offres connectées.

Conclusion

Les entreprises de toutes tailles découvriront que la conformité au nouveau règlement et sa mise en œuvre ne seront pas faciles. Il faudra une intégration approfondie et sans faille dans les processus uniques de chaque entreprise. Il faudra également mettre l'accent sur une bonne communication et une formation réglementaire. La plupart des entreprises mondiales recherchent déjà une grande conformité fondée sur les normes de l'Organisation internationale de normalisation (ISO) [6] Elles attendent la publication de la Commission électrotechnique internationale (IEC) 29151:2015 (informatique, techniques de sécurité, code de mise en œuvre de la protection des données personnelles identifiables)[7] et de l'ISO/IEC DIS 29134:2016 (informatique, techniques de sécurité, évaluation de l'impact sur la vie privée, lignes directrices)[8]

La volatilité de l'environnement réglementaire et les rapides changements géopolitiques exigent que les organisations mondiales possèdent de robustes cadres de conformité pour tenir compte de ces changements. La Brexit est un parfait exemple de la façon dont le Royaume-Uni quittant l'UE, couplé au nouveau règlement, rendra plus difficile la conformité des entreprises mondiales.

> **"Un cadre de conformité peut servir d'élément clé à la sécurité en ligne et aux initiatives de conformité."**

Parce que la sortie du Royaume-Uni de l'UE n'aura lieu qu'après le 25 mai 2018, il est important de noter que les entreprises européennes devront quand même se conformer au nouveau règlement. Toutes les entreprises qui traitent des données des citoyens du Royaume-Uni seront tenues à ce moment-là à se conformer à la législation du Royaume-Uni.

Steve Wood, commissaire adjoint par intérim au Bureau du commissaire de l'information du Royaume-Uni (ICO), a déclaré : " le rôle de l'ICO a toujours été de travailler en étroite collaboration avec les organismes de réglementation des autres pays et cela continuera

d'être le cas. Avoir des lois bien définies avec des sauvegardes en place est plus que jamais important compte tenu de la croissance de l'économie numérique. Nous consulterons le gouvernement britannique pour expliquer notre point de vue que la réforme du droit de la protection des données au Royaume-Uni demeure nécessaire.[9] " Cela signifie que les lois de protection des données dans le Royaume-Uni seront en constante évolution. En plus du nouveau règlement, on exigera que les organisations au service des clients du Royaume-Uni garantissent la conformité.

Il est important de se rappeler que les règlements de protection des données personnelles sont principalement conçus pour aider les organisations à achever les meilleures protections des données. Ils représentent un bon ensemble de règles à suivre. Fondamentalement, la plupart des exigences de conformité en matière de protection des données personnelles exigent la confidentialité, de bonnes politiques de gestion de l'information, de raisonnables mesures de sécurité, des procédures et des technologies pour minimiser les incidents de perte de données. Par conséquent, les organisations qui ont conçues et déployées de robustes cadres de conformité avec une granularité raisonnable de contrôles seront en mesure de les appliquer sur une grande échelle. Tout en adressant les modifications réglementaires et l'évolution des besoins de conformité, la protection en toute sécurité des données personnelles permettra de générer de nouvelles affaires.

Notes de bas de page

1 Journal officiel de la Communauté européenne, *www.ojec.com/*

2 Journal officiel de l'Union européenne, " le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, la protection des personnes physiques à l'égard du traitement des données personnelles et la libre circulation de ces données, l'abrogation de la directive 95/46/EC (règlement sur la protection des données générales) ", le 4 mai 2016, *http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*

3 Baker et McKenzie, " La préparation aux nouveaux régimes de confidentialité : les opinions des professionnels de la confidentialité sur le règlement général de la protection des données et de la vie privée ", avril 2016, *http://f.datasrvr.com/ fr1/416/76165/IAPP_GDPR_and_Privacy_Shield_Survey_Report.pdf*

4 La Commission européenne, "La protection des données personnelles, " *http://ec.europa.eu/justice/data-protection/*

5 L'Association internationale des professionnels de la confidentialité "Comment les services informatiques et Infosec considèrent la confidentialité," *https://iapp.org/resources/article/how-it-and-infosec-value-privacy/*

6 L'Organisation internationale de normalisation, ISO/IEC 27018:2014 *Informatique, techniques de sécurité, code de pratique pour la protection des informations personnelles identifiables (PII) dans les nuages publiques agissant en tant que processeurs PII),* le 1 août 2014, *www.iso.org/iso/catalogue_detail.htm?csnumber=61498*

7 L'Organisation internationale de normalisation, ISO/IEC DIS 29151 (Informatique, — techniques de sécurité, code de pratique pour la protection des informations personnelles identifiables), le 5 juillet 2016, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62726*

8 L'Organisation internationale de normalisation, ISO/IEC DIS 29134 *Informatique, techniques de sécurité,—évaluation des impacts sur la vie privée, lignes directrices, —le*, 18 juillet 2016, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289*

9 Wood, S.; "Le nouveau règlement demeure pertinent pour le Royaume-Uni" Bureau du commissaire de l'information, le 7 juillet 2016, *https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/*