Application du GDPR : quatre cas d'utilisation clés pour vous éclairer

IBM Security Guardium aide à simplifier la préparation à l'application du règlement sur la protection des données personnelles GDPR (General Data Protection Regulation)

Points clés

- Agir rapidement et lancer une campagne d'évaluation et de préparation à l'application du règlement sur la protection des données personnelles (GDPR)
- Prendre en charge les principaux éléments de protection des données du GDPR pour soutenir la protection des données personnelles
- Tirer parti d'une approche de bout en bout, adaptable à la protection des données avec IBM® Security Guardium®
- Se lancer avec l'accélérateur Guardium GDPR, qui fournit des fonctionnalités pré-intégrées pour vous aider à multiplier vos efforts vis-à-vis du GDPR

L'Union européenne (UE) a marqué le monde entier en adoptant le GDPR en mai 2016. Lorsqu'il entrera en vigueur le 25 mai 2018, toutes les sociétés faisant affaires avec des personnes situées sur le territoire d'un état membre de l'UE, devront se conformer aux dispositions étendues de la loi. Toutes les informations personnelles identifiables d'une personne vivant dans l'UE, quel que soit leur lieu d'envoi, de traitement ou de stockage, devront être protégées et la preuve de la protection devra être vérifiée. En effet, le règlement stipule que la protection des données personnelles est l'un des « droits fondamentaux... des personnes physiques ».[1]

Les entretiens avec les analystes du secteur révèlent que de nombreuses entreprises n'ont pas conscience de l'impact potentiel de ce règlement qui change pourtant la donne. Elles peuvent être mal préparées pour répondre correctement à ses exigences. Par exemple, de nombreuses entreprises qui ne sont pas situées dans l'UE n'ont pas encore réalisé que le GDPR s'applique également à elles. Le fait que les sociétés n'aient pas de locaux ou ne traitent pas de données dans un état membre de l'UE ne les exemptent pas de l'application du GDPR : ne pas se préparer à l'application de ce règlement pourrait avoir de graves conséquences sur leurs résultats financiers, leurs relations avec leurs clients ou leur image de marque. Le non-respect du GDPR peut entrainer des amendes atteignant 20 millions d'euros (environ 22,3 millions de dollars US) ou jusqu'à 4 % de leurs revenus mondiaux totaux pour l'exercice précédent, le montant le plus élevé étant retenu.[2]

La préparation à l'application du GDPR ne se fera pas en un jour. IBM estime que le moment est venu pour les entreprises de commencer à allouer le budget et les ressources nécessaires à la mise en œuvre des processus et des contrôles de gouvernance, et d'identifier les outils qui facilitent la mise en conformité. Pour les aider, IBM Security a créé une fiche « Évaluation de la préparation au GDPR » qui permet d'identifier les lacunes en matière de confidentialité et de sécurité, et qui recommande des plans de correction. En outre, Guardium fournit des modèles et des actifs prédéfinis qui permettent d'accélérer votre mise en conformité à plusieurs obligations clés de la protection des données du GDPR.

La protection et la confidentialité des données d'une personne font la force du GDPR

Le cloud, l'informatique mobile, les plateformes de Big Data et l'Internet des objets (IdO) ont tous relevé le défi du partage, de la gestion, de la gouvernance et de la sécurisation de l'information. Dans ce contexte, il n'y a jamais eu autant de sensibilisation à la nécessité de protéger ses données personnelles : cartes nationales d'identité, adresses e-mail ou données de localisation ; données biométriques, physiques, physiologiques, génétiques ou mentale ; données économiques, culturelles ou religieuses ; données sociales, politiques ou de préférence de genre et plus encore.

Le GDPR vise à protéger les individus et leurs données personnelles par le biais de normes unifiées et modernisées, et d'un ensemble de droits significatifs pour les individus. Certaines obligations du GDPR comprennent :

- **la condition du consentement**, obligeant les entreprises à obtenir un consentement explicite des individus (aussi nommés « personnes concernées ») quant à la collecte de leurs informations, et à être en mesure de prouver qu'elles l'ont obtenu. Le consentement est limité à des fins particulières et les personnes concernées ont le droit de retirer leur consentement à tout moment.[3]
- **le droit d'accéder aux données et de les obtenir**, permettant aux personnes concernées dedemander l'accès aux informations détenues les concernant, de savoir comment on y accède, l'objet de l'accès, l'endroit où on y accède, les catégories de données accessibles et qui a accès à ces informations ;
- le droit d'effacement, donnant aux personnes concernées le droit de demander la suppression de leurs données personnelles si elles ne souhaitent pas autoriser leur utilisation ;
- **le droit de rectification et d'opposition au profilage**, accordant aux personnes concernées le droit de demander la correction de leurs données personnelles si elles sont inexactes et leur permettant de s'opposer à un profilage pouvant entraîner une discrimination à leur encontre.

Ces droits des personnes concernées soulèvent une question de taille : comment une entreprise peut-elle amorcer un programme de conformité au GDPR et remplir ses obligations avec succès ?

GDPR : êtes-vous prêt ?

Le GDPR considère qu'une entreprise doit tenir compte de la confidentialité des données des individus en mettant en œuvre une approche de « protection des données dès la conception lors du développement de la sélection et de l'utilisation des applications, services et produits basés sur le traitement des données personnelles ou qui traitent des données personnelles pour accomplir leur tâche ».[4] Il est plus judicieux pour les sociétés qui traitent des données personnelles d'intégrer dès le départ des protections de confidentialité et de sécurité dans leurs applications, services et produits. Malheureusement, de nombreuses entreprises se retrouvent maintenant dans une position où elles vont devoir rattraper leur retard — et le rattraper vite.

Pour aider les entreprises à accélérer leur préparation à l'application du GDPR, IBM Security recommande d'effectuer une évaluation des pratiques de confidentialité et de sécurité des données de l'entreprise. L'objectif est double : identifier les zones à risque et concevoir des processus permettant d'atténuer ces risques. Les résultats de l'évaluation peuvent vous aider à établir votre feuille de route vers le GDPR. Celle-ci doit soutenir quatre activités clés pour aider à gérer et à protéger les données personnelles :

1. Évaluer la préparation de la protection des données pour identifier et atténuer les vulnérabilités de sécurité.
2. Identifier et classifier les données personnelles.
3. Mettre en œuvre la gouvernance des contrôleurs et des processeurs pour traquer les emplacements de traitement des données personnelles et créer un suivi d'audit.
4. Gérer les violations de données personnelles et informer l'entreprise si et où une violation a eu lieu.

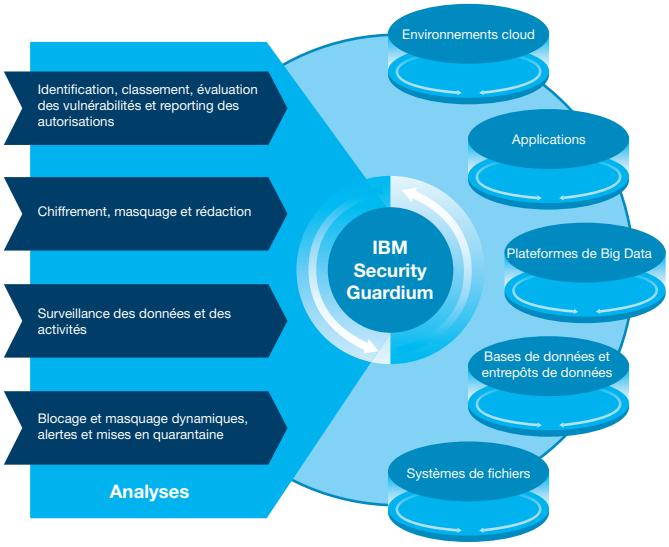
À court et long termes, les sociétés peuvent considérer les obligations du GDPR comme un catalyseur du changement organisationnel — une opportunité pour réévaluer la protection des données et réfléchir plus intelligemment sur cette protection et sur les effets positifs d'une solide approche de sécurité, de confidentialité et de protection des données. Les entreprises qui profitent des avantages compétitifs d'un programme de protection des données structuré et évolutif, notamment pour renforcer la confiance et la loyauté des clients, ainsi que pour donner aux employés le bon niveau d'accès aux données, en bénéficieront pendant plusieurs années.

Suivi des droits d'accès des personnes concernées

Dans le cadre d'une initiative de sécurité globale, une grande banque française devait contrôler les accès aux bases de données sur ses 400 serveurs via des mécanismes d'authentification forte sur 150 applications sensibles. La banque utilise Guardium comme outil pour aider à suivre les droits d'accès des personnes concernées et pour modifier, supprimer et transférer automatiquement les données conformément aux exigences du GDPR.

Guardium permet à l'entreprise d'effectuer les opérations suivantes :

- Importer automatiquement les règles d'accès du référentiel bancaire dans le système Guardium via des interfaces de programme d'application (API) ;
- Capturer, surveiller et produire des rapports sur les commandes de base de données utilisées pour créer, modifier ou manipuler le contenu de la base de données, et renforcer les contrôles de modification affectant les entrées de la base de données ;
- Produire des rapports sur les requêtes SQL détaillées, notamment la source et la date ;
- Traquer et signaler les échecs de connexion, et bloquer les utilisateurs non autorisés et les connexions non réseau.



Guardium : Accélération de la protection et de la confidentialité des données pour appliquer le GDPR

Les meilleures pratiques favorisent un programme fort de protection et de confidentialité des données. Conçu pour protéger les données personnelles dans un grand nombre d'environnements, Guardium est une solution de protection des données qui offre une approche de bout en bout pour protéger les données importantes, y compris les données personnelles, la propriété intellectuelle, les informations propriétaires, les données des partenaires, et d'autres encore sur lesquelles les entreprises s'appuient pour fonctionner. En tant que plateforme modulaire adaptable, Guardium permet aux équipes de sécurité et de conformité d'analyser automatiquement les risques, de hiérarchiser les efforts et de réagir en temps réel à ce qui se passe dans leurs référentiels de données.

Guardium peut aider à répondre à certaines questions clés sur l'accès et le contrôle des données personnelles que le GDPR rend obligatoire :

Aide à identifier et atténuer les vulnérabilités de sécurité

- Identifie les menaces et les failles de sécurité dans les bases de données qui pourraient être exploitées par des pirates informatiques, et fournit des recommandations détaillées pour les atténuer
- Analyse les infrastructures de base de données pour identifier les vulnérabilités telles que les correctifs manquants, les mots de passe faibles, les modifications non autorisées ou les privilèges mal configurés

Identification : Où se situent les données personnelles ?

- Identifie et classifie les données personnelles, et détecte les risques de conformité en fonction de vos critères
- Analyse les modèles d'utilisation des données pour aider à identifier et à corriger rapidement les risques grâce à des analyses automatisées avancées et au machine learning
- Prend en charge la gestion centralisée et l'intégration hétérogène existant, et s'adapte aux changements dans l'environnement (nouveaux utilisateurs ou expansion du volume des données par exemple)

Surveillance : Comment sont utilisées les données et par qui ?

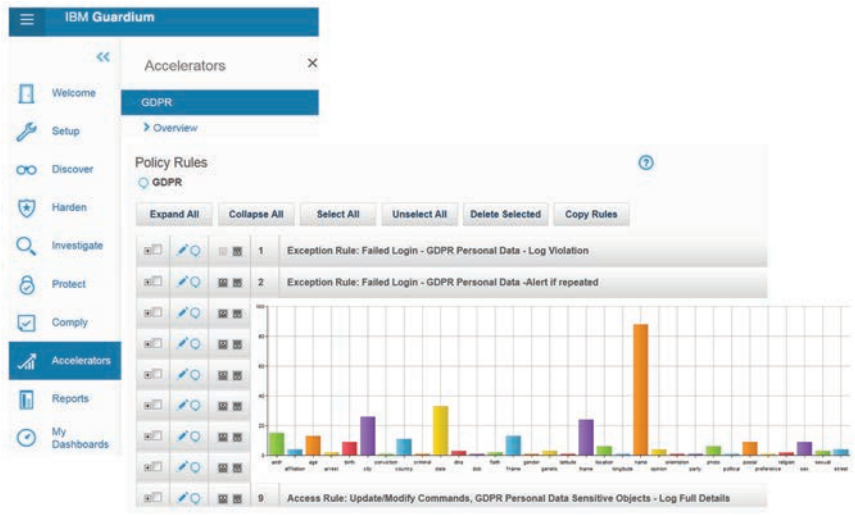
- Surveille qui accède aux données et qui les lit, repère les anomalies et stoppe la perte de données grâce à une surveillance des activités en temps quasi réel et à des alertes dans toute l'entreprise
- Aide à prévenir les accès non autorisés aux données et à recevoir des alertes sur les changements ou les fuites pour assurer l'intégrité des données
- Réduit les coûts opérationnels grâce à un contrôle et un suivi simplifiés de l'accès aux ID partagés des utilisateurs privilégiés

Chiffrement, masquage, rédaction et blocage : Comment sont protégées les données ?

- Utilise un processus rigoureux de rapports, de chiffrement, de masquage, de rédaction, de blocage dynamique et d'alerte sur les droits pour protéger les données personnelles contre l'accès, l'utilisation, la perte ou la modification, que ce soit en mode statique ou dynamique
- Aide à protéger l'entreprise et sa responsabilité contre la perte de données et de manière proactive grâce à l'analyse automatisée des risques, à la validation, aux workflows de conformité automatisés et aux fonctionnalités d'audit étendues
- Alerte et bloque de manière dynamique les données internes et externes illicites et l'accès aux fichiers en temps réel sur une large gamme de plateformes, notamment les bases de données, les fichiers et systèmes de fichiers, les environnements de Big Data, les environnements grand système et plus encore

Rapports de conformité et d'audit : Est-ce rationalisé avec l'automatisation ?

- Capture les privilèges et les droits utilisateur compromis
- Utilise l'analyse automatisée et les contrôles de conformité pour détecter et stopper l'accès aux données et leur utilisation qui ne respectent pas les exigences de conformité
- Se déploie rapidement grâce aux modèles et actifs prédéfinis qui accélèrent vos efforts de mise en conformité
- Prend en charge l'ensemble de votre parcours de protection de la sécurité des données, de la préparation de l'application du GDPR à la mise en place de règles et de contrôles de protection des données automatisés en temps réel, grâce à une infrastructure et à une approche adaptables



Accélère la mise en œuvre de l'application du GDPR et les efforts pour protéger les données

Afin d'être prêtes à remplir leurs obligations vis-à-vis du GDPR, IBM estime que les entreprises doivent commencer à s'y préparer dès maintenant. Certaines obligations peuvent être relativement simples à satisfaire, tandis que d'autres, comme la mise en œuvre de systèmes permettant d'appliquer le droit à l'oubli, peuvent être plus difficiles à réaliser, car elles peuvent nécessiter des changements dans les processus opérationnels. Il n'y a pas une minute à perdre : commencez maintenant. Pour vous aider à démarrer, Guardium propose un accélérateur GDPR. Cet accélérateur fournit des fonctionnalités pré-intégrées afin de vous aider à gérer vos risques et vulnérabilités GDPR en fournissant :

- Une évaluation de l'impact sur la sécurité des données du GDPR qui analyse les sources de données contenant des données personnelles soumises au GDPR (comme décrit ci-dessus) ;
- Des modèles de classification pour aider à identifier les données personnelles soumises au GDPR telles que l'âge, la date de naissance, le sexe, la préférence sexuelle, l'opinion politique, l'adresse e-mail, le nom, la religion, l'opinion religieuse, les renseignements internationaux du passeport, les informations de localisation, les informations génétiques, le casier judiciaire, les données biométriques, la photo, l'adresse, la ville, le code postal, le pays et plus encore ;
- Des ensembles prédéfinis de règles et de groupes de règles qui aident à surveiller, auditer, enregistrer et fournir des alertes sur toute activité non autorisée liée aux données personnelles par des utilisateurs et des applications avec ou sans autorisation. Ces mêmes règles sont également utilisées pour créer des pistes d'audit relatives aux demandes de personnes concernées, telles que les demandes d'accès, de rectification, d'effacement ou de transfert de données personnelles ;
- Des rapports pour identifier qui a accédé aux données personnelles, d'où, quand et comment elles ont été consultées – tous ces rapports pouvant être utilisés pour envoyer des notifications aux auditeurs, aux contrôleurs et aux responsables de la protection des données utilisant le processus de vérification de la conformité de la sécurité des données qui fait partie de l'accélérateur.

Intéressons-nous aux raisons pour lesquelles ces fonctionnalités sont précieuses et comment vous pouvez les utiliser pour vous préparer au GDPR.

L'accélérateur GDPR fournit une mine d'informations sur l'accès par les utilisateurs standard et avec privilèges aux données personnelles soumises au GDPR. Mais, à moins de savoir où sont stockées ces données personnelles et à quoi elles ressemblent, elles ne peuvent pas être surveillées ni protégées. Par conséquent, une première étape pour répondre aux exigences du GDPR est d'identifier les données personnelles et leur emplacement de stockage. Les modèles de classification prédéfinis fournis avec l'accélérateur GDPR simplifient et accélèrent ce processus.

Au début, il est également important d'évaluer les autres vulnérabilités de votre environnement et de vos sources de données, afin de connaître où sont vos faiblesses et risques supplémentaires, et de pouvoir les résoudre. L'accélérateur GDPR fournit des tests d'évaluation de la sécurité des données pré-intégrés, de sorte que vous puissiez rapidement effectuer des évaluations de vulnérabilité sur les sources de données personnelles que vous avez identifiées et obtenir des recommandations pour aider à combler les lacunes. Lorsque vous avez pris connaissance des lacunes et des vulnérabilités, vous pouvez prendre des mesures pour combler ces lacunes et renforcer les sources de données personnelles, afin que les utilisateurs non autorisés ne puissent pas modifier les configurations ou les paramètres d'autorisation de ces sources. Grâce à l'expertise approfondie d'IBM et à des méthodologies propriétaires, l'évaluation de l'impact de l'accélérateur GDPR sur la sécurité des données peut identifier ces zones à risques et faciliter l'auditabilité pour le GDPR.

L'utilisation de ces actifs préconfigurés permet de rationaliser et d'accélérer le processus d'identification des données personnelles au sein d'une entreprise. Elle aide aussi à identifier et à corriger les risques liés à ces sources de données personnelles, afin que vous puissiez commencer à surveiller vos sources de données identifiées comme contenant des données personnelles et prendre des mesures dans le cas où un comportement suspect se produirait. L'accélérateur GDPR comprend des règles et des groupes de règles prédéfinis pour vous aider à amorcer cette surveillance continue plus rapidement. Les règles prédéfinies aident à protéger les sources de données contenant des données personnelles contre les accès et les activités non autorisés, notamment contre les changements, le retrait, la réplication ou la suppression des enregistrements. L'accélérateur GDPR traite également les rapports (que vous pouvez sélectionner par utilisateur, par contrôleur ou par application) relatifs à la surveillance des données pour toutes les activités autorisées et non autorisées sur les données personnelles. En outre, les rapports d'audit peuvent être utilisés pour aider à résoudre les incidents en fournissant un rapport d'activité détaillé.

L'accélérateur vous aide également à suivre et à fournir des pistes d'audit détaillées sur les demandes d'accès des personnes concernées, telles que l'accès aux données personnelles et la rectification, l'effacement ou le transfert des données. Des informations telles que l'utilisateur de l'application, l'utilisateur de la base de données, la requête SQL et l'horodatage sont capturées dans un référentiel d'audit. Des rapports personnalisables sont inclus ; vous pouvez les partager avec vos équipes de conformité, auditeurs et autres. Les données d'identification des individus autorisés à gérer les demandes peuvent être sécurisées grâce à IBM Security Privileged Identity Manager. Ce logiciel permet de gérer l'extraction et la restitution des données d'identification, ainsi que l'enregistrement détaillé des sessions qui peut être lié à vos rapports d'audit Guardium.

Les fonctionnalités de l'accélérateur GDPR, associées aux interfaces de divers outils dans le système sous-jacent, sont organisées de manière tabulaire selon les exigences, ce qui peut accélérer le processus de mise en œuvre et réduire les délais.

Enfin, l'accélérateur GDPR de Guardium fournit un processus automatisé d'audit des workflows pour venir à l'appui de la préparation à l'application du GDPR. Cette fonctionnalité automatise le processus de notification et de vérification pour simplifier et accélérer l'approbation des rapports d'audit préconfigurés relatifs à l'activité des données personnelles (accès, suppression et mises à jour par des utilisateurs et des applications autorisés et non autorisés) qui doit être documentée, enregistrée et vérifiée.

Pourquoi IBM ?

Toute entreprise opérant dans l'UE ou faisant des affaires avec des pays membres de l'UE a besoin d'une approche globale à l'échelle de l'entreprise pour protéger ses données et se mettre en conformité avec le GDPR. Guardium fournit les meilleures pratiques qui aident les entreprises à connaître l'état de leurs données, à réduire les risques, à ajuster les règles et à surveiller et auditer les violations de conformité et de règle.

Guardium fournit une plateforme intégrée et évolutive de sécurité des données qui aide les clients à analyser les risques liés aux données sensibles, à protéger ces données et à s'adapter aux changements de l'environnement informatique. L'analyse permet de gérer la complexité des données et les modèles de données, tandis que la gouvernance et la centralisation aident à gérer l'ensemble des fonctionnalités de protection des données (sécurité, confidentialité et conformité) dans la panoplie des sources de données hétérogènes requises pour exécuter un environnement informatique.

De plus, les services de conseils sur la confidentialité des données d'IBM peuvent vous aider à identifier les zones susceptibles d'être régies par le GDPR et fournissent des recommandations pour vous aider à créer et déployer des règles, normes, directives et procédures opérationnelles complètes de confidentialité qui correspondent aux meilleures pratiques en matière de conformité avec le GDPR. Tout comme l'audit fait partie de la gouvernance de la confidentialité des données, une évaluation préalable est la clé pour une bonne préparation. Lorsque vous vous préparez à l'application du GDPR, les Services IBM peuvent vous aider à optimiser votre niveau de contrôle en établissant une stratégie de protection des données qui non seulement met en œuvre des ressources, mais aussi les intègre (surveillance de l'activité des données 24 h/24 et 7 j/7, avec l'intelligence et l'analyse avancées globales de la menace par exemple).

Que ce soit au début d'une initiative de préparation à la conformité ou lors de l'élargissement d'un programme existant, les entreprises peuvent utiliser la feuille de route des meilleures pratiques de Guardium de manière efficace pour intégrer des mesures de protection des données et se préparer à l'application du GDPR.

Pour en savoir plus

Pour en savoir plus sur les solutions GDPR d'IBM, contactez votre revendeur ou votre partenaire commercial IBM, ou rendez-vous sur le site Web https://www-03.ibm.com/software/products/fr/category/data-security.

A propos des solutions IBM Security

IBM Security offre l'un des portefeuilles les plus avancés et intégrés de produits et de services de sécurité d'entreprise. Ce portefeuille, qui s'appuie sur la recherche et le développement IBM X-Force® de renommée mondiale, fournit des renseignements de sécurité qui aident les entreprises à assurer une protection holistique de leur personnel, de leurs infrastructures, de leurs données et de leurs applications, grâce à des solutions de gestion des identités et des accès, de sécurité des bases de données, de développement d'applications, de gestion du risque, de gestion des nœuds finaux, de sécurité du réseau, etc. Ces solutions permettent aux organisations de gérer efficacement les risques et de mettre en œuvre une sécurité intégrée pour le mobile, le cloud, les médias sociaux et les autres architectures métier de l'entreprise.
IBM exploite l'une des plus vastes organisations au monde de recherche, de développement et de diffusion de solutions de sécurité, surveille 15 milliards d'événements de sécurité par jour dans plus de 130 pays et détient plus de 3000 brevets de sécurité.

En outre, IBM Global Financing propose de nombreuses options de paiement pour financer vos investissements informatiques stratégiques et faire progresser votre activité. De leur acquisition à leur utilisation, nous proposons une gestion complète du cycle de vie des produits et services informatiques. Pour en savoir plus, rendez-vous sur : **ibm.com**/financing

[1] Article 1. 2. « Règlement (UE) 2016/679 du Parlement européen et du Conseil », 27 avril 2016. http://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[2] Article 83, 5. « Règlement (UE) 2016/679 du Parlement européen et du Conseil », 27 avril 2016. http://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[3] Article 7, « Règlement (UE) 2016/679 du Parlement européen et du Conseil », 27 avril 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[4] Paragraphe 78« Règlement (UE) 2016/679 du Parlement européen et du Conseil », 27 avril 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

IBM Security
New Orchard Road
Armonk, NY 10504

Produit aux États-Unis
Juin 2017