ManageEngine
EventLog Analyzer

Tout ce que vous devez savoir pour vous conformer au Règlement général sur la protection des données (RGPD) de l'UE

Sommaire

Introduction

L'augmentation du nombre, de l'ampleur et du coût des failles de sécurité des données a poussé les gouvernements du monde entier à faire passer des lois de conformité plus strictes en matière de protection des données personnelles des citoyens. L'Europe ne fait pas exception à la règle. Depuis 2012, la Commission européenne encadre de nouvelles protections des données visant à améliorer les méthodes de traitement des données, à renforcer la sécurité des données et à harmoniser la protection des données sensibles dans l'ensemble des pays européens.

Avec beaucoup de modifications apportées aux règles de protection actuelles, le nouveau Règlement général sur la protection des données (RGPD) attire de plus en plus d'attention. Le cadre européen du RGPD est complexe à mettre en œuvre, avec de nouvelles politiques d'obligation de responsabilisation, des procédures de notification en cas de violation des données et des règles strictes en matière de flux international des données. Avec seulement quelques mois avant la mise en œuvre de ce nouveau règlement, il est grand temps pour les organisations de revoir leurs stratégies sécuritaires.

Ce manuel vise à souligner les principaux changements, défis et plans d'action que les organisations devront respecter pour assurer leur conformité vis-à-vis du RGPD.

Changements, exigences et plans d'action

Le RGPD n'a pas de frontières

Le RGPD est une loi de protection des données à l'échelle internationale qui s'étend au-delà des entreprises opérant uniquement au sein de l'UE. Toute organisation ciblant des consommateurs au sein de l'UE, traitant les données personnelles de citoyens européens ou surveillant le comportement des sujets des données de l'UE doit se conformer aux exigences du RGPD.

Exigences :

- Il est temps de revoir les cadres et les politiques de sécurité des entreprises. Les organisations qui n'opèrent pas au sein de l'UE mais traitent des données européennes vont devoir prendre les mesures nécessaires pour se conformer à ce nouveau RGPD.
- Les organisations qui opèrent au sein de l'UE et qui respectent les lois actuelles en matière de protection des données européennes vont devoir également revoir leur cadre sécuritaire de façon à s'assurer qu'elles respectent les exigences plus strictes de la nouvelle RGPD.

Les plans d'action

- Si votre organisation fournit des marchandises ou des services ou surveille le comportement de citoyens basés au sein de l'UE, vous devez vous conformer aux exigences du RGPD au plus tard le 25 mai 2018.
- Revisitez vos politiques de sécurité et assurez-vous que vous prenez les mesures adéquates, telles que soulignées ci-dessous dans le cadre de la gestion des données personnelles.
- Rédigez des notes de confidentialités en bonne et due forme et d'autres documents susceptibles de fournir un consentement explicite et éclairé de la part des individus pour le traitement de leurs données personnelles. Si vous avez de tels documents, envisagez de les faire réviser et examiner à la lumière de cette nouvelle réglementation.
- Surveillez les mesures techniques et organisationnelles qui sont prises pour assurer la confidentialité et la sécurité des données personnelles recueillies.
- Si nécessaire, nommez des responsables capables de surveiller les processus relatifs aux données et responsables de la sécurité des données personnelles et sensibles.

Élargissement de l'étendue des données personnelles

Ce nouveau règlement élargit la définition des données personnelles et des informations personnelles sensibles.

Selon le RGPD, les données à caractère personnel concernent « toute information en lien avec un individu identifié et identifiable. » Ceci comprend également les « identifiants en ligne » tels que les adresses IP ou les cookies.

En plus de définir les données à caractère personnel, le RGPD classe certaines données personnelles dans la catégorie des informations personnelles sensibles. Selon le RGPD, les données personnelles sensibles désignent « toute information en lien avec les origines raciales ou ethniques, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la santé ou la vie sexuelle ainsi que les données biométriques. »

Ces nouvelles exigences imposent également que les organisations obtiennent un consentement valide de la part des « sujets des données » avant le traitement de leurs données à caractère personnel.

Défis :

- Cette large définition des données personnelles et l'inclusion des « identifiants en ligne » oblige les organisations traitant avec l'analyse des données, les analyses comportementales, la publicité et les réseaux sociaux à se conformer au RGPD.

Les plans d'action

- Définition de la portée des données que traite votre organisation.
- Si les données correspondent à la définition du RGPD des « données à caractère personnel », préparez une note de confidentialité ou un document demandant un consentement explicite et éclairé des individus pour un traitement supplémentaire des données.
- Si vous cherchez déjà le consentement pour traiter les données, envisagez de le revoir et de l'examiner conformément aux nouvelles exigences de conformité.

Redéfinition des principes de protection des données

Le principe de protection des données qui sous-tend les exigences du RGPD reste le même que celui stipulé dans la Loi sur la protection des données à caractère personnel, la réglementation de conformité précédente, avec quelques éléments supplémentaires ajoutés.
Les six principes de protection des données soulignent que les données personnelles et les données personnelles sensibles doivent être :

- Traitées de façon équitable, dans le respect de la loi et de manière transparente.
- Collectées pour des motifs spécifiés, explicites et légitimes et ne devraient pas être traitées de manière incompatible avec les motifs susmentionnés. Un archivage supplémentaire des données pour des intérêts publics ou scientifiques, historiques ou statistiques ne doit pas être considéré comme incompatibles avec les motifs initiaux.
- Adéquates, pertinentes et limitées à ce qui est nécessaire en relation avec l'objectif pour lequel les données sont traitées.
- Exactes et à jour. Les étapes ont été prises pour supprimer ou rectifier les données à caractère personnel qui sont inexactes.
- Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Elles peuvent être archivées pour une plus longue période uniquement si l'archivage soutient des intérêts ou est effectué pour des motifs scientifiques, historiques ou statistiques. De plus, les organisations doivent prendre les mesures techniques pour protéger les droits et les libertés des individus.
- Traitées avec les mesures techniques et organisationnelles adéquates qui assurent une bonne sécurité, y compris la protection contre tout processus illégal, perte accidentelle, destruction ou dommage.

Le nouveau RGPD donne les grandes lignes des exigences de responsabilité qui rendent les contrôleurs des données a) responsables de s'assurer que les principes de protection des données sont bien en place et b) démontrer que l'organisation respecte le RGPD.

Exigences :

- En plus de répondre aux principes de protection des données en tant que tels, les entreprises doivent clairement définir leur rôle dans le traitement des données (c'est-à-dire contrôleurs ou processeurs) et accepter leurs responsabilités conformément au nouveau règlement.
- Les organisations doivent réviser leur flux d'audit des données pour se conformer aux nouvelles exigences d'exigibilité du RGPD.

- Une nouvelle approche basée sur les risques doit être adoptée par les entreprises qui traitent les données personnelles de haut risque. Les contrôleurs de données doivent effectuer des évaluations de l'impact de la protection des données (EIPD) pour évaluer les risques associés aux données à caractère personnel avant leur traitement. Cet EIP permettra également d'identifier et d'atténuer les violations de données à un stade précoce de façon à réduire les dommages et intérêts susceptibles d'être versés.
- Si un projet traitant de données à caractère personnel est lancé, les organisations doivent adopter une approche inhérente de confidentialité de façon à réduire les risques de violation des données.

Les plans d'action

- Documenter toutes les informations en lien avec le traitement des données, notamment :
  - Quel genre de données à caractère personnel sont recueillies.
  - Comment elles sont collectées, utilisées, transmises ou stockées.
  - Comment elles sont protégées et empêchées d'être divulguées à chaque étape.
- En plus de documenter les informations (notamment où les données sont stockées et qui est propriétaire des données), les entreprises doivent constamment surveiller les activités telles que :
  - Qui a accès aux données à caractère personnel.
  - Avec qui ces données sont partagées.
- Suivre en continu le fichier ou le dossier où les données sont stockées de façon à identifier de façon immédiate et de signaler toute tentative d'accès non autorisée ou illégale.
- Conserver un enregistrement de la durée pendant laquelle les données vont être stockées. Et pendant leur stockage, s'assurer que les données sont cryptées et protégées contre les manipulations.

Responsabilité et transparence

Chaque organisation traitant des données à caractère personnel ou des données sensibles est soit un contrôleur, soit un processeur. Pour garantir leur responsabilisation, le RGPD établit un bon équilibre entre le rôle des contrôleurs et celui des processeurs, les rendant équitablement responsables du bon respect de la conformité.

Contrôleurs de données

- Selon le RGPD, « les contrôleurs sont toute personne physique ou morale agissant seule ou de concert qui détermine comment et pourquoi les données à caractère personnel sont traitées. »
- Les contrôleurs sont responsables de :
  - L'examen de toutes les activités de traitement des données.
  - Le maintien de la documentation pertinente en rapport avec toutes les activités de traitement des données.
  - La mise en place d'évaluations des risques relatifs à la protection des données pour les processus à haut risque.
  - La mise en œuvre de la protection des données dès la conception des politiques et par défaut.
  - La nomination de processeurs de données et la définition de consignes sur la façon de traiter les données.
  - La notification des autorités en cas de violation des données, de quelque nature qu'elle soit.

Processeurs de données

- Selon le RGPD, un processeur de données désigne « toute personne (autre que l'employé du contrôleur de données) qui traite des données pour le compte du contrôleur des données. »

  Les processeurs de données effectuent les tâches suivantes :
  - Traiter les données uniquement en fonction des instructions documentées par le contrôleur.
  - Prendre des mesures sécuritaires et organisationnelles pour éviter les violations de données.
  - Supprimer toutes les données à caractère personnel à la fin du traitement et sur instruction du contrôleur.
  - Conserver un enregistrement écrit des activités de traitement effectuées pour le compte des contrôleurs.
  - Désigner un responsable de la protection des données si nécessaire.
  - Informer immédiatement les contrôleurs en cas de violation des données.
  - Fournir toutes les informations aux contrôleurs qui sont nécessaires à la démonstration de la conformité et autoriser la réalisation d'audits par le contrôleur.

Exigences :

- Les entreprises doivent examiner avec précaution et réviser leurs contrats de traitement des données existants pour répondre aux nouvelles exigences de responsabilité. Tout nouveau contrat doit respecter les nouvelles exigences du RGPD.
- Ceux qui traitent et contrôlent les données doivent réviser leurs politiques de sécurité, d'audit et de violation des données pour répondre aux nouvelles exigences du RGPD.
- Les organisations doivent conserver les enregistrements des actions prises pour éviter les violations des données.

Les plans d'action

- Conserver un enregistrement clair du flux de données à l'intérieur de l'organisation : la façon dont la collecte, l'accès, le partage et la propriété des données est effectué et/ou accordé.
- Encadrer les politiques de sécurité susceptible d'éviter les violations de données. Ceci comprend :
  - La surveillance du réseau de l'organisation pour détecter toute anomalie.
  - Le suivi des comportements des utilisateurs, en particulier des utilisateurs privilégiés ayant accès au traitement des données à caractère personnel.
  - L'audit du fichier et du dossier dans lesquels les données à caractère personnel sont stockées. Obtenez des informations immédiates en cas de tentative d'accès inapproprié ou non autorisé aux données à caractère personnel.
  - S'assurer que les bonnes mesures techniques et organisationnelles sont prises pour protéger les réseaux de l'entreprise des attaques et menaces.

Notification de violation des données

Le RGPD définit une violation des données à caractère personnel comme une « violation de sécurité menant à une destruction, une perte, une altération, une divulgation non autorisée des données à caractère personnel ou un accès à ces données. »

Ceci explique qu'une violation des données constitue beaucoup plus qu'une simple perte des données. Ce règlement oblige également les organisations à signaler les violations de données « sans retard excessif et si possible » sous 72 heures.

Exigences :

- Les entreprises doivent avoir mis en place une procédure interne de signalement des violations.
- Les organisations doivent effectuer des examens des chaînes d'approvisionnement et des audits réguliers pour s'assurer qu'elles répondent aux nouvelles exigences en termes de sécurité.
- Les entreprises doivent déployer un système technique et sécuritaire qui facilite la détection instantanée des violations de données. Le système doit également fournir des informations approfondies pour accélérer la réponse ou contenir la violation à un stade précoce.

Les plans d'action

- Identifier les indicateurs de compromis qui sont à l'origine des violations de sécurité au sein du réseau et préparer des politiques de sécurité pour les empêcher.
- Déployer des systèmes de sécurité comme des pare-feu et des systèmes de détection et de prévention d'intrusion (IDS/IPS) susceptibles de les aider à se protéger des attaques sécuritaires.
- Envisagez de mettre en œuvre des solutions de sécurité pour les organisations capables de détecter, alerter et signaler instantanément en cas de violation de sécurité. De plus, les solutions devraient pouvoir alerter en temps réel en cas de problème ou de tentative de violation.
- Faire appliquer les politiques de sécurité qui aident à garantir l'intégrité des données en identifiant les actions non autorisées suivantes :
    - Accès ou tentatives d'accès
    - Suppression
    - Partage
    - Copie ou tentative de copie des données personnelles
- Surveiller le comportement des utilisateurs privilégiés (c'est-à-dire les utilisateurs ayant accès aux données à caractère personnel) pour identifier les activités anormales en cas de vol d'identité et les signaler immédiatement.

Les droits des sujets des données

Toute action que vous pouvez effectuer avec des données est considérée comme un traitement de données. Cependant, le RGPD définit des limites strictes en matière de ce que les organisations peuvent faire ou non avec les informations personnelles qu'elles recueillent.

Droit à être informé : Il démarre dès le moment de la collecte des données. Les organisations doivent informer les sujets des données que les informations recueillies sur eux seront traitées de manière transparente et équitable, via un message de confidentialité. De plus, les entreprises ont pour obligation d'obtenir un consentement clair et valide des sujets des données pour le traitement de leurs informations personnelles via un document de consentement rédigé dans des termes clairs.

Droit d'accès : Les sujets des données ou les individus doivent avoir le droit d'accéder à tout moment à leurs informations personnelles. Selon cette exigence, le RGPD s'assure que des individus ont le droit de vérifier et de valider leurs informations avec un traitement équitable.

Droit à la rectification : Si des individus estiment que leurs données à caractère personnel sont incomplètes ou imprécises, ils ont le droit de demander à l'entreprise de rectifier leurs données personnelles. Si une demande de rectification a été faite, il est de la responsabilité du contrôleur de fournir des informations sur les actions prises sur cette demande sans retard excessif pour les individus concernés.

Droit à la restriction du traitement des données : Si le traitement des données est restreint, le contrôleur peut stocker uniquement les données à caractère personnel et ne peut effectuer aucun processus sur les données, de quelque type que ce soit. Les utilisateurs peuvent restreindre leur traitement des données si :

- Les données sont considérées comme imprécises ou incomplètes.
- Les données sont traitées de façon contraire à la loi.
- Le contrôleur n'a plus de raison (conformément aux principes de protection des données) de traiter les données à caractère personnel.

Droit à la portabilité des données : Les individus, à tout moment dans le temps et sans obstacle, peuvent obtenir leurs données et les transférer vers un autre contrôleur pour traitement. Ce droit permet aux individus de déplacer, copier ou transférer facilement des données à caractère personnel d'un environnement à un autre de façon sécurisée.

Droit à l'oubli : Le RGPD accorde aux individus des droits complets de demander la suppression ou le retrait de leurs données à caractère personnel. La demande de suppression des données peut être effectuées dans les circonstances suivantes :

- Si le stockage des données à caractère personnel n'est plus nécessaire en lien avec le motif pour lequel elles ont été recueillies ou traitées.
- Lorsque l'individu retire son consentement pour le traitement des données.
- Lorsque le sujet des données émet une demande d'arrêt du traitement des données en raison d'un traitement illégal des données ou en cas de violation des données.
- Si les données doivent être supprimées pour se conformer aux obligations légales.

Les plans d'action

- Rédiger un formulaire de consentement adéquat pour obtenir le consentement éclairé et explicite des individus pour le traitement de leurs données à caractère personnel.
- Documenter les techniques et les flux de traitement des données de façon à ce que vous puissiez les fournir aux individus lorsqu'ils les réclament en faisant valoir leur droit d'accès.
- Prendre des mesures pour effacer automatiquement les données à caractère personnel une fois l'objectif de leur collecte atteint.
- Pendant le stockage des données, vérifiez que leur intégrité est préservée en chiffrant les données.
- Documentez les informations de chiffrement pour les fournir aux sujets des données, si nécessaire.

Pénalités de violation de conformité

Si les organisations ne se conforment pas au RGPD ou ne respectent pas les exigences du RGPD, les administrateurs peuvent imposer une pénalité allant jusqu'à ***10 millions d'euros ou 2 % du chiffre d'affaire annuel mondial de l'entreprise sur l'exercice financier précédent,*** si celui-ci est plus élevé. Les contrôleurs et les processeurs de données sont tenus de régler cette amende importante si les conditions suivantes ne sont pas respectées :

- Principes en matière de protection des données principales
- Conditions de traitement des données non personnelles
- Conditions pour l'accord
- Conditions de traitement des données personnelles sensibles
- Droits des sujets des données

Le commissaire chargé de la protection des données qui impose cette amende prend en considération la nature et l'intensité de la violation, les mesures d'atténuation prises, les mesures techniques et organisationnelles mises en œuvre et d'autres points pour décider du montant de la pénalité.

Satisfaire aux exigences de conformité RGPD avec les solutions de sécurité informatiques de ManageEngine

Le portefeuille de solutions de sécurité informatiques de ManageEngine possède une gamme d'outils étendue qui aide les organisations à se conformer aux RGPD. Nous possédons dans notre suite,

- **Log360**, un outil SIEM complet qui aide les entreprises à détecter les violations de données, à assurer la sécurité des données personnelles stockées, et suivre l'accès aux données personnelles, confirmant ainsi les exigences en matière de reddition de comptes.
- **File Audit Plus**, un outil de surveillance et d'audit de fichiers en temps réel qui aide à suivre toutes les modifications critiques du fichier et du dossier dans lequel les données personnelles sont stockées.

Comment nos solutions aident à se conformer aux exigences du RGPD

- **Les mesures techniques et organisationnelles pour se défendre contre ou mitiger les conséquences des violations de sécurité :** Le déploiement de Log360 et File Audit Plus peut constituer la mesure technique adoptée par les organisations pour se défendre contre ou mitiger les conséquences des violations de sécurité. Ces solutions permettent de surveiller les activités de tous les périphériques et utilisateurs dans votre réseau et de signaler instantanément les anomalies aux administrateurs. Le professionnel de sécurité peut ensuite étudier l'incident à l'aide des rapports complets, et si l'incident se trouve être une violation de sécurité (ou une tentative de violation), vous pouvez alors prendre immédiatement des mesures pour l'atténuer à un stade précoce.
- **Audit des données :** L'option de surveillance de l'intégrité des fichiers en temps réel de File Audit Plus permet de suivre en continu les changements aux données critiques. Elle offre également des informations complètes sur les personnes ayant accédé aux données, la date de consultation et le lieu d'accès aux données. Ce rapport détaillé aide à fournir des informations aux sujets des données sur les accès aux données et surveille également les flux de données.
- **Réalisation de pistes d'audit :** L'option de recherche avancée de journaux de Log360 vous aide à effectuer facilement une analyse d'investigation. C'est l'une des exigences du RGPD pour trouver les causes premières de la violation des données ou tentative de violation de façon à résoudre immédiatement le problème. Notre solution peut vous aider à identifier les causes fondamentales d'une violation de données en cherchant dans plusieurs téraoctets de données de journaux en seulement quelques minutes. Cette solution offre également une option permettant d'exporter les résultats des recherches sous la forme d'un rapport d'investigation prêt à être envoyé aux responsables de la protection des données. De plus, la demande de recherche peut être convertie en profil d'alerte pour atténuer les futures attaques de sécurité du même type.

- **Réponse aux exigences PIA/DPIA :** Les rapports complets de Log360 et les profils d'alerte détectent immédiatement toute anomalie de réseau ou toute tentative de violation de la sécurité. Ceci contribue à atténuer les violations de données à un stade précoce mais aussi à minimiser les dommages et intérêts relatifs aux données qui seraient autrement subis, répondant ainsi aux exigences PIA/DPIA du RGPD.

- **Exigence de notification en cas de violation :** Log360 permet d'envoyer des e-mails en temps réel ou des alertes par SMS aux administrateurs. Ceci les aide à signaler le plus rapidement possible la violation à des responsables à un niveau hiérarchique supérieur. Cette solution est proposée avec plus de 600 profils d'alerte prédéfinis en étant basé sur divers IOC. Ceci aide à détecter les tentatives de violation instantanément et sans trop d'efforts. De plus, cette solution offre également l'option de créer des alertes personnalisées en fonction de vos besoins de sécurité internes.

À propos de ManageEngine

ManageEngine vous fournit les outils de gestion informatique en temps réel qui permettent à votre équipe informatique de répondre aux besoins de votre organisation pour des services et une assistance en temps réel. Dans le monde entier, plus de 60 000 entreprises anciennes et nouvelles (dont plus de 60 % du classement Fortune 500) comptent sur les produits ManageEngine pour assurer des performances optimales pour leurs infrastructures informatiques critiques, notamment leurs réseaux, serveurs, applications, bureaux et bien plus encore. ManageEngine est une filiale de Zoho Corp. avec des bureaux dans le monde entier, notamment aux États-Unis, au Royaume-Uni, en Inde, au Japon et en Chine.

À propos de l'auteur

Subhalakshmi Ganapathy travaille actuellement comme analyste marketing produit senior des solutions de sécurité informatique chez ManageEngine. Elle possède des connaissances approfondies sur la sécurité des informations et la gestion de la conformité. Elle fournit des conseils stratégiques aux entreprises en matière de Gestion des informations et événements de sécurité (SIEM), de sécurité réseau et de confidentialité des données.

Contactez Subha à l'adresse suivante : subhalakshmi.g@manageengine.com.

E-mail :
support@eventloganalyzer.com

Ou

Numéro vert (gratuit) :

USA : +1 888 720 9500 Royaume-Uni : 0800 028 6590

AUS : +1 800 631 268 CN : +86 400 660 8680

International : +1 925 924 9500

Ou

Visitez www.eventloganalyzer.com pour des informations détaillées sur cette solution et toutes ses fonctionnalités.