VARONIS

GDPR

GUIDE PRATIQUE

VARONIS

GDPR

Devenez conforme, **restez** conforme

- Localisez et protégez les données à caractère personnel
- Empêchez les fuites de données
- Découvrez les comportements suspects
- Construisez une stratégie de « Privacy by Design »

Demandez votre évaluation gratuite à la conformité GDPR

https://info.varonis.com/gdpr-risk-assessment-fr

Sommaire

VARONIS France SAS :

T +33 184 88 56 00 **E** sales-france@varonis.com **W** www.varonis.fr

GDPR DE L'UE – LEÇON 1

Qu'est-ce que le GDPR (ou RGPD, pour Règlement Général sur la Protection des Données) ?

Le GDPR est une évolution d'une loi européenne existante : la DPD (Directive de Protection des Données).

Il s'agit d'une règlementation contraignante applicable dans toute l'UE et au-delà, qui oblige à documenter les processus informatiques, à effectuer des analyses de risque, à signaler toute atteinte aux données; elle vise à ce que les données nominatives des personnes concernées soient mieux protégées.

Le GDPR édite des lois sur la sécurité des données, en particulier dans le cadre de la Protection des Données dès la Conception (principe de PbD, pour "Privacy by Design"), afin de minimiser la collecte des données à caractère personnel, supprimer les données qui ne sont plus nécessaires, resteindre les accès, et sécuriser les données tout au long de leur cycle de vie.

Quel type de données est protégé ?

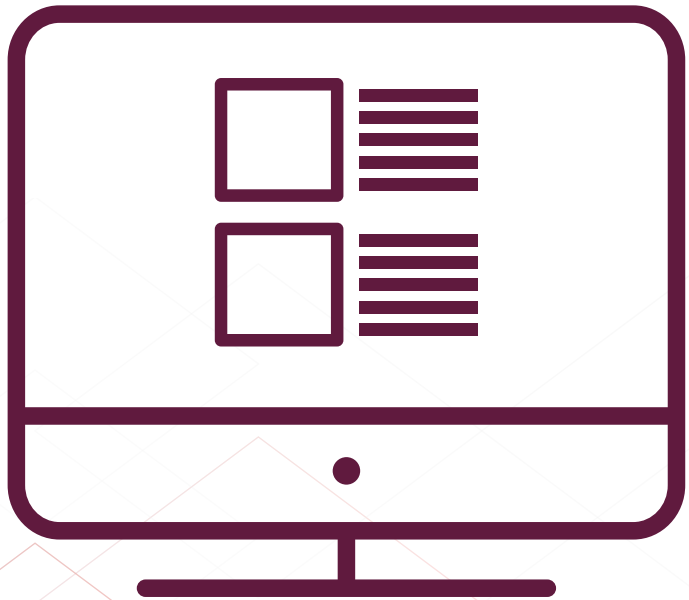
Les données à caractère personnel, aussi appelées PII (Personally Identifiable Information). Ce sont les noms, adresses, numéros de téléphone, numéros de compte, et plus récemment les adresses e-mail et les adresses IP.

Qui est affecté ?

Le GDPR s'applique à toute entreprise recueillant des données à caractère personnel de ressortissants européens, qu'elles aient ou non une présence physique dans l'UE.

Comment cela vous affecte ?

Le GDPR engendre désormais de nouvelles lois et exigeances pour la collecte, l'enregistrement, et le stockage des données à caractère personnel et des activités de traitement, ainsi que de nouvelles obligations concernant les notifications de violation des données, les sanctions liées à ces violations, et plus encore.



Quelles sont les nouvelles obligations ?

Respect de la vie privée dès la conception – Le GDPR a formalisé les principes de la protection de la vie privée dès la conception (PbD) dans ses règlements, notamment en minimisant la collecte et la conservation des données et en obtenant le consentement des consommateurs lors du traitement des données.

Évaluations d'impact du GDPR (Privacy Impact Assessments [PIA]) – Les entreprises devront d'abord faire une analyse des risques d'atteinte aux données avant de traiter certaines données sensibles.

Droit à l'effacement et à l'oubli – C'était une demande exprimée depuis longtemps au titre de la DPD, pour permettre à tout consommateur ou usager de demander la suppression des données à caractère personnel le concernant. Le GDPR étend ce droit, qui recouvre désormais toutes les données publiées sur le Web. Il s'agit là du « Droit à l'oubli » qui fait néanmoins toujours l'objet de controverses.

Extraterritorialité – Le nouveau principe d'extraterritorialité du GDPR signifie que même lorsqu'une entreprise n'est pas physiquement présente dans l'UE, mais si elle recueille des données à caractère personnel relatives à des ressortissants de l'UE – par exemple au travers d'un site Web –, alors toutes les obligations définies par le GDPR lui sont applicables. En d'autres termes, cette nouvelle législation a une portée dépassant les frontières de l'UE. Les entreprises extra-européennes les plus affectées seront celles dont les activités comprennent le commerce électronique, les entreprises hébergeant des données dans le Cloud, mais aussi les entreprises à l'international dont le siège serait en dehors de l'UE.

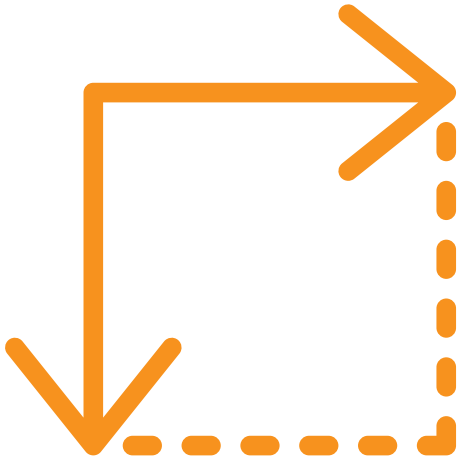
Notification en cas d'atteinte aux données – Les entreprises devront signaler les atteintes aux données à caractère personnel dans un délai de 72 heures au plus tard après en avoir pris connaissance. Les personnes dont leurs données ont été atteintes doivent également être averties, mais seulement si ces données présentent un risque pour leurs droits et leurs libertés.

Amendes – Les infractions graves peuvent engendrer une amende allant jusqu'à 4% du chiffre d'affaires mondial de l'entreprise. Ces infractions peuvent inclure des violations des principes de base liés à la sécurité des données - en particulier les principes de "Privacy by Design". Une amende de moins de 2% des revenus mondiaux peut être émise si les enregistrements de la société ne sont pas en ordre ou si les autorités et les personnes concernées ne sont pas notifiées après une violation.

Le GDPR sensibilise les entreprises à la protection des données : où sont enregistrées les données sensibles, qui y accède et qui devrait y accéder est maintenant plus critique que jamais.

GDPR DE L'UE – LEÇON 2

Protection des données à caractère personnel dès la conception et par défaut



Le principe de prise en compte des questions de vie privée dès la conception d'un système – vous pouvez consulter notre fiche pratique sur le sujet – est notamment conçu pour amener les dirigeants d'entreprises à prendre les questions de respect et de sécurité de la vie privée plus au sérieux. De manière générale, c'est là une idée bien intentionnée, qu'il y a lieu de soutenir.

Mais avec sa formalisation dans le cadre du Règlement général sur la protection des données (GDPR), cela devient plus qu'un principe ou une bonne idée : c'est une obligation légale pour quiconque souhaite commercer au sein de l'UE !

Les principes cardinaux du GDPR sont même utiles, en matière de sécurité des données, à toute entreprise, un mot suffisant à expliquer pourquoi : minimisation.

Et on peut donc partir du principe que si votre entreprise opère déjà selon l'équivalent américain de ce principe, dit "Privacy by Design", elle devrait déjà être largement « dans les clous » du GDPR.

Tout cela étant dit, est-ce qu'exploitation de données massives ("Big Data") et respect de la vie privée peuvent tout de même faire bon ménage ? La nouvelle législation part du principe que c'est le cas, à condition de mettre en application les principes suivants :

- Minimiser les données (surtout à caractère personnel) recueillies auprès des consommateurs et usagers
- Ne pas conserver des données à caractère personnel une fois qu'elles ont été utilisées pour l'objet initial
- Accorder aux consommateurs et aux usagers un droit d'accès (et de rectification) et la propriété ultime de ces données

GDPR DE L'UE – LEÇON 3

Le droit à l'oubli

Le « droit à l'oubli », qui reste controversé, a désormais force de loi dans l'UE.

Du point de vue des entreprises, il se traduit en un droit des consommateurs à demander l'effacement des données à caractère personnel les concernant conservées par l'entreprise.

Le GDPR a renforcé ce droit à l'effacement qui existe déjà dans la DPD et l'a complété du droit à l'oubli. Il contient des clauses obligeant le responsable du traitement de ces données à faire tous les efforts raisonnables pour répercuter auprès des tierces parties ayant accès à ces données toute demande de suppression de cet ordre.

L'article 17 et les clauses liées du texte adopté du GDPR précisent que « le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais [...] en particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant [...] et la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données à caractère personnel la concernant ».

Cela signifie par exemple que si un service de réseau social répercute les données à caractère personnel d'un de ses abonnés à d'autres services Web, il devra non seulement se faire fort d'effacer les enregistrements d'origine de ces données, mais aussi contacter tous les prestataires Web auxquels il les a répercutées, en les informant de cet impératif. Ce ne sera certainement pas un processus aisé !

Et si le « responsable du traitement » confie ces données à caractère personnel, pour stockage ou traitement, à un service d'hébergement dans le Cloud ?

Le large périmètre d'application des règlements de l'UE englobe tout à fait ce type de cas : le prestataire de service dans le Cloud est considéré par le texte comme un « sous-traitant » et est tout autant tenu d'effacer les données à caractère personnel lorsqu'il est informé de la demande de la personne concernée par le responsable du traitement.

Traduction : le consommateur, ou « personne concernée », peut exiger à tout moment d'une entreprise qu'elle efface les données à caractère personnel le ou la concernant de ses supports de stockage. Dans l'Union européenne, les données à caractère personnel appartiennent au peuple !

GDPR DE L'UE – LEÇON 4

Qui est affecté par le GDPR de l'UE ?

L'un des aspects les plus complexes du nouveau GDPR est lié à la notion « d'extraterritorialité ». D'après l'article 3, le GDPR s'appliquera à toutes les données transférées à l'extérieur de l'UE.

Selon ces nouvelles règles, si une entreprise américaine recueille des données relatives à des ressortissants de l'UE, elle encourt les mêmes obligations légales qu'une entreprise qui aurait son siège en France, au Royaume-Uni, ou en Allemagne, par exemple, et ce même si elle ne dispose d'aucune antenne ni d'aucun serveur sur le territoire de l'UE.

Des experts en droit font remarquer que ces dispositions ne seront pas si aisées à faire respecter, mais à supposer qu'une multinationale de premier plan enfreigne l'une de ces dispositions – notamment l'obligation stricte de signaler toute atteinte aux données concernées –, il est probable que les régulateurs de l'UE la ciblent. Il est certain que l'extraterritorialité se justifie dans le cas des services Web de base comme la recherche d'informations, les réseaux sociaux, le commerce électronique ou encore les services de location ou de mise à disposition d'appartement en ligne, etc.

Des règles qui évoluent

Dans le cadre règlementaire de la Directive sur la protection des données à caractère personnel (DPD), il existait une marge de manoeuvre qui permettait aux acteurs de la collecte de données d'échapper à son application. Cette échappatoire, pour les fournisseurs de services ou d'applications, consistait à effectuer les traitements des données hors de l'UE.

On considérait que si l'essentiel du traitement et des serveurs se trouvaient à l'extérieur de l'UE, alors ces règles ne s'appliquaient pas. C'était l'approche adoptée par de grands acteurs tels que Google, Facebook et d'autres opérateurs de réseaux sociaux.

Encore que !...

Google avait précisément fait valoir cet argument lorsqu'une autorité de contrôle de la protection des données espagnole lui avait demandé d'effacer une entrée de la page de résultats d'une recherche donnée. Cette affaire était remontée jusqu'à l'instance judiciaire suprême de l'UE, la Cour de Justice européenne (CJE), qui avait statué contre Google.

L'autorité du législateur de l'UE avait donc prévalu : Google avait fini par supprimer l'entrée mise en cause.

Cette idée d'étendre l'application du GDPR en dehors du territoire européen est explicité dans l'article 3. Le GDPR sera appliqué aux entreprises basées dans l'UE, ainsi qu'aux entreprises collectant des données sur les citoyens de l'UE même si elles n'ont pas de présence physique sur le territoire.

GDPR DE L'UE – LEÇON 5

Que se passera-t-il si je ne me conforme pas aux règles du GDPR de l'UE ?

Le GDPR prévoit des sanctions graduées susceptible de faire très mal aux finances des contrevenants ; et les clauses du GDPR s'appliquent aussi bien aux « responsables de traitement » de ces données qu'à leurs « sous-traitants », catégorie dans laquelle on peut ranger tous les opérateurs de services dans le Cloud ; donc ces derniers, notamment les plus gros, ne sont certainement pas à l'abri des mêmes types de sanctions.

Le non-respect des obligations prévues peut déboucher sur des amendes allant jusqu'à 4 % du chiffre d'affaires mondial du contrevenant.

Une entreprise peut se voir imposer une amende allant jusqu'à 2 % de son chiffre d'affaires (article 83) si son registre des activités de traitement n'est pas correctement tenu (article 28), si elle omet de signaler à l'autorité de contrôle, voire à la personne concernée, une violation (articles 33 et 34) ou si elle n'effectue pas d'analyse d'impact (article 35).

Et n'oubliez pas que l'obligation de notification prévue par le GDPR ne se résume pas à signaler simplement que vous avez subi une atteinte aux données. Vous devrez indiquer la catégorie dont relève les données, les enregistrements compromis et le nombre au moins approximatif de personnes concernées. Pour être en mesure de fournir ces informations, vous devrez disposer vous-mêmes de mécanismes de suivi qui vous permettront, en cas d'incident, de savoir si des hackers ou des personnes en interne sont intervenues.

Les infractions plus graves encourent une amende pouvant aller jusqu'à 4 % du chiffre d'affaires. Il s'agit notamment des violations des principes fondamentaux de la sécurité des données (article 5) et des conditions applicables au consentement des consommateurs (article 7), considérées comme des infractions à l'esprit même du règlement, qui invite à intégrer le respect de la vie privée à tout dispositif (voir notre fiche pratique Privacy by Design).

Afin que les entreprises soient en conformité avec le GDPR, les régulateurs de cette loi imposent aux entreprises de nommer un Délégué à la Protection des Données (ou DPO, pour "Data Privacy Officer"). Le DPO devrait être chargé de créer des contrôles d'accès, de réduire les risques, d'assurer la conformité, de répondre aux demandes, de signaler les infractions sous 72 heures et de créer une solide politique de sécurité des données.

GDPR DE L'UE – LEÇON 6

Et maintenant ?
Que faut-il faire concrètement ?

Examinons de plus près quelques-uns des défis que pose le GDPR et la façon de les relever :

▶ Article 25 : Protection des données à caractère personnel dès la conception et par défaut

Ce que cela signifie : Intégrer à la culture d'entreprise que respect de la vie privée et responsabilité doivent être pris en compte au démarrage de chaque projet

Comment faire : Redéfinir tous les accès aux données dans le sens des « privilèges a minima »

▶ Article 30 : Registre des activités du traitement

Ce que cela signifie : Prendre des mesures techniques et organisationnelles pour traiter correctement les données à caractère personnel ;

Comment faire : Créer un registre des fichiers sensibles ; Comprendre qui y a accès ; Savoir qui y accède ; Distinguer quand certaines données peuvent et doivent être supprimées.

▶ Article 17 : Droit à l'effacement (« droit à l'oubli »)

Ce que cela signifie : Être capable de localiser et de cibler des données spécifiques afin d'automatiser leur suppression

Comment faire : Localiser, marquer, effacer.

▶ Article 32 : Sécurité du traitement

Ce que cela signifie : Mettre en oeuvre des privilèges d'accès « a minima » ; Mettre en place un système de responsabilité, avec des détenteurs désignés des données ; Produire des rapports attestant que les politiques et processus adéquats sont actifs et efficaces.

Comment faire : Automatiser et imposer le système de privilèges a minima en conduisant des audits des besoins en accès et en promouvant explicitement une éthique globale de la question.

▶ Article 33 : Notification à l'autorité de contrôle d'une violation de données à caractère personnel

Ce que cela signifie : Détecter les atteintes aux données et remplir les obligations d'alerte ; Disposer d'un plan de réponse actif.

Comment faire : Détecter les atteintes aux données, les infractions à la règle et signaler ces manquements en temps quasi réel.

▶ Article 35 : Analyse d'impact relative à la protection des données

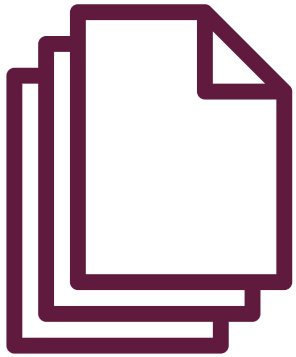
Ce que cela signifie : Quantifier les profils de risque d'atteinte aux données

Comment faire : Évaluer le traitement des données sensibles et à haut risque.

Quels sont les points sur lesquels vous devez vous concentrer pour être en conformité avec le GDPR ?

Classification des données – Sachez où sont conservées les données à caractère personnel sur votre système, surtout s'il y en a qui ne sont pas sous forme de base de données mais disséminées dans des documents textuels, des présentations ou des feuilles de calcul. Cet aspect est crucial pour la protection de ces données ainsi que pour être en mesure de répondre à des demandes de rectification ou de suppression de ces données.

Métadonnées – Pour satisfaire à l'obligation de retrait des données périmées, vous devrez disposer de métadonnées telles que la date de recueil desdites données, la raison de leur collecte et leur objet. Les données à caractère personnel stockées sur le système informatique doivent être périodiquement passées en revue pour réévaluer les justifications de conservation.



Encadrement – Le GDPR souligne la nécessité de revenir aux bases. Pour les données d'entreprise il s'agit de comprendre qui a accès à ces données sur les systèmes de partage de l'entreprise, qui a vocation à y avoir accès, puis de dresser un répertoire des permissions d'accès en fonction du rôle réel de chacun dans l'entreprise.

Surveillance – L'exigence de notification des atteintes aux données impose une charge de travail supplémentaire aux responsables de traitement de ces données. Dans le cadre du GDPR, le mot d'ordre, en matière de sécurité informatique, c'est « Surveillance en continu ». Vous devrez être à même de détecter des comportements d'accès aux fichiers de données à caractère personnel inhabituels et de rendre compte rapidement à l'autorité de contrôle compétente de tout accès illicite. Tout manquement à cette obligation peut être un motif d'imposition de lourdes amendes, tout particulièrement pour les grandes multinationales réalisant un chiffre d'affaires mondial important.

De manière générale, le message envoyé aux entreprises concernées par le GDPR est qu'il est désormais encore plus crucial qu'avant de traiter les données à caractère personnel avec un soin tout particulier et rigoureux, c'est-à-dire notamment de savoir en permanence où sont conservées les données sensibles, qui les exploite et qui peut disposer de l'accès à ces données.

Demandez-nous une Évaluation gratuite de votre État de préparation au GDPR.

C'est nous qui prendrons en charge le gros du travail pour vous : méthode d'approche, configuration et analyse, avec des propositions de mesures concrètes pour favoriser votre mise en conformité avec ce Règlement général sur la protection des données.

Varonis dispose d'une bibliothèque de règles de confidentialité à jour et peut aider à créer des règles personnalisées selon les besoins, à analyser en permanence votre environnement et à signaler toute violation des données trouvée dans le monde entier.

UN INGÉNIEUR DÉDIÉ PRENDRA EN CHARGE LES MISSIONS SUIVANTES :

- Identifier les données entrant dans le champ d'application du GDPR
- Repérer et révoquer les accès non justifiés à des données à caractère personnel
- Faire un audit des actions des utilisateurs, détecter les comportements à risque et les vulnérabilités aux ransomware
- Trouver des données à caractère personnel sous-utilisées ou obsolètes

Programmez dès maintenant l'évaluation de votre entreprise !

https://info.varonis.com/gdpr-risk-assessment-fr

VARONIS France SAS :

T +33 184 88 56 00 **E** sales-france@varonis.com **W** www.varonis.fr

À propos de Varonis

Varonis est une plate-forme de sécurité des données innovante qui permet aux entreprises de gérer, d'analyser et de sécuriser les données d'entreprise. Varonis est spécialisé dans la création de logiciels qui gèrent et protègent les données de l'entreprise contre les menaces internes, les violations de données et les cyberattaques en détectant et en alertant sur les déviances par rapport aux comportements habituels connus, en identifiant et en atténuant l'exposition des données sensibles et en automatisant les processus pour sécuriser les données d'entreprise.

Varonis compte plus de 5 350 clients dans le monde et nous aidons déjà des centaines d'organisations de toutes tailles et de tous secteurs avec des projets GDPR.

DÉTECTER les menaces internes et cybermenaces en analysant les données, l'activité des comptes et le comportement des utilisateurs.

ÉVITER la catastrophe en verrouillant données sensibles et périmées, en limitant l'accès généralisé et en simplifiant les autorisations.

MAINTENIR un état de sécurité en automatisant les autorisations, les migrations et les suppressions.

Témoignages

« Varonis fonctionne dans toute notre organisation : au sein de notre infrastructure, dans Active Directory et sur l'ensemble de notre matériel et de nos logiciels. Elle nous permet de savoir ce qui se passe et de découvrir ce qui nous attend. Nous avons pu détecter et bloquer une infection de ransomware 10 minutes seulement après l'attaque. »

– Wade Sendall | Vice-président informatique, Boston Globe

« Les stratégies fondées sur le périmètre de sécurité classique ne conviennent plus aux menaces auxquelles nous avons à faire face aujourd'hui. [...] Ce que je recherchais, c'était une plateforme de sécurité des données qui me permettrait de consulter tous nos types de données, qui y accède et le détail de nos processus les concernant. Il est clair que Varonis est la plateforme qui répond à nos attentes. »

– Gary Hayslip | Directeur de la sécurité informatique

« Il est rassurant de savoir que Varonis veille sur nous et nous aide de manière proactive à empêcher les violations internes et externes. »

– Jim Hanlon | SVP & CTO, Dedham Savings Bank