Le Règlement Général sur la Protection des Données (RGPD)

protiviti®
Face the Future with Confidence

En route vers la conformité !

Octobre 2017

Le parlement européen a adopté le Règlement général sur la protection des données (RGPD) de l'Union (UE) le 14 avril 2016, au terme de quatre années de négociations. La nouvelle législation remplace l'initiative sur la protection des données de l'UE entrée en vigueur en 1995 et en élargit la portée.

Le RGPD s'applique à toutes les organisations qui traitent, stockent ou utilisent des données concernant des citoyens européens. Même les organisations qui n'exercent pas d'activités au sein de l'UE mais qui emploient des citoyens de l'UE ou ont des clients et/ou fournisseurs européens doivent s'y conformer.

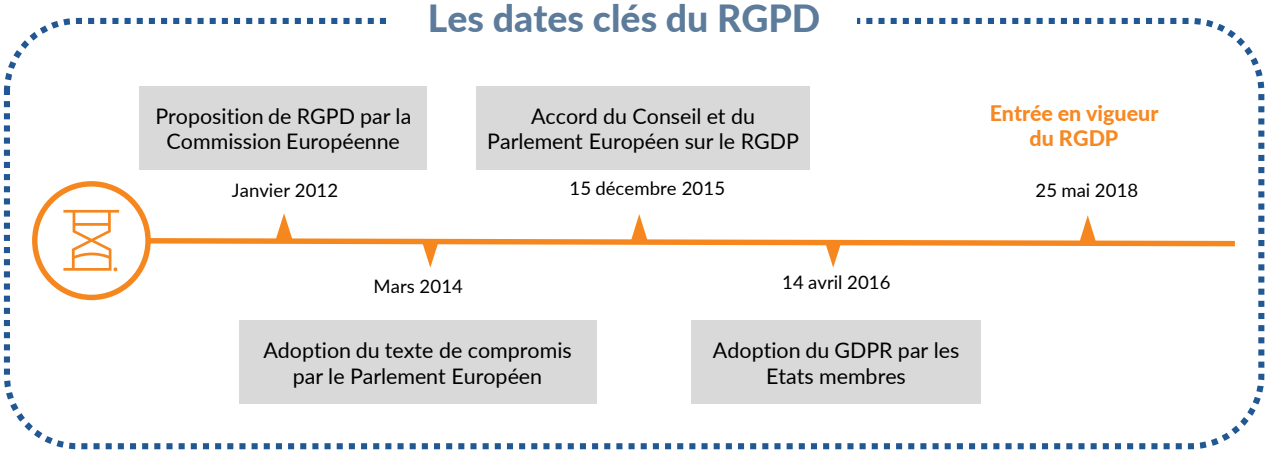
Le non-respect du RGPD peut entraîner de lourdes sanctions, dont des amendes équivalentes à 4 % du chiffre d'affaire global de l'entreprise contrevenante.

Les organisations concernées par la nouvelle législation disposent aujourd'hui **moins de huit mois** pour de revoir leurs pratiques et procédures pour les rendre conformes à la nouvelle réglementation.

Les entreprises dont les activités couvrent plusieurs pays sont face à un défi d'une ampleur sans précédent, considérant qu'elles parviennent déjà difficilement à respecter de manière cohérente la législation actuelle. Il apparait clairement que bon nombre d'entreprises de ce type devront adopter une approche différente en ce qui concerne la gestion de la confidentialité des données à l'avenir. Certaines organisations pourraient même être amenées à repenser en profondeur leur modèle opérationnel.

En bref, les entreprises doivent réagir rapidement pour déterminer le niveau d'efforts requis pour se conformer au nouveau règlement et pour instaurer les plans de remédiation appropriés le cas échéant. Cet article expose les étapes-clés que les organisations doivent franchir pour élaborer un programme efficient de conformité avec le RGPD et présente plusieurs éléments critiques à prendre en considération dans le cadre du processus.

Les dates clés du RGPD



Nos recommandations pour adresser les points clés du RGPD

1. Sensibiliser et responsabiliser les acteurs clés. Cette étape est primordiale à réussite d'un projet RGPD.

2. Revoir les processus de collecte de données afin de recenser de façon précise les traitements de données personnelles que vous mettez en œuvre.

3. Encourager les principes de minimisation de données et d'intégrer les principes de protection des données dès la conception et par défaut (Privacy by Design/Default).

4. Etudier les alternatives avant de vous lancer dans des chantiers couteux d'anonymisation ou de pseudonymisation.

5. Nommer un Délégué à la Protection des données (Data Protection Officer) qui sera principalement chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant et aussi les employés.

6. Revoir la gestion du consentement et présenter les informations de façon claires, intelligibles et précises (par exemple, clause particulières sur l'utilisation des données collectée, les mentions légales, les formulaires papiers et web, etc.).

7. Etre prêt à gérer et traiter les demandes de suppression, modification et portabilité entrantes et sortantes.

8. Revoir la procédure de communication externe avec les autorités qui exigeront des notifications en cas de violation des données au plus tard dans les 72 heures après la détection d'un incident (perte, fuite et piratage).

9. Privilégier une approche de remédiation basée sur les risques et rester concentrés sur les risques les plus élevés.

Qu'est-ce qu'une « donnée à caractère personnel » ?

Une « donnée à caractère personnel» est une information relative à une personne identifiée, ou qui permet d'identifier une personne, directement ou indirectement. Cela concerne donc aussi bien les informations directement nominatives (le nom et le prénom), que les informations qui permettent d'identifier, indirectement, une personne physique. C'est le cas d'un numéro de téléphone (qui permet d'identifier le titulaire de la ligne téléphonique), d'un numéro de plaque minéralogique (qui renvoie au titulaire de la carte grise). C'est également le cas d'éléments du corps humain tels que l'empreinte digitale ou l'ADN d'une personne. Il s'agit aussi de toutes les données qui sont rattachées à une personne.

Donnée personnelle : Toute information identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

Donnée sensible : Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Source des définitions: Qu'est-ce qu'une « donnée à caractère personnel » ?: https://www.cnil.fr/fr/definition

Choisir le bon leadership

Foncièrement, un programme de conformité avec le RGPD consiste à changer les comportements, ce qui peut s'avérer très compliqué dans l'ensemble d'une grande entreprise multinationale ou chaîne d'approvisionnement. Par conséquent, l'initiative devrait être pilotée par une personne dotée des compétences et surtout de l'autorité nécessaires pour induire un changement à travers toute l'organisation. Les aspects administratifs quotidiens liés à cette mission peuvent être délégués, mais l'ultime responsabilité doit être assumée plus en amont si l'organisation tient sérieusement à opérer un changement.

Nous estimons que la responsabilité du programme RGPD pourrait être attribuée à un Chief Operating Officer (COO) ou à une fonction équivalente du senior management. Nous pensons aussi que cette personne, ou quelqu'un occupant un poste d'un niveau équivalent ou proche, devrait assurer la mission de Data Protection Officer (DPO).

C'est dans le choix du DPO ad hoc que résidera la clé du succès du programme de conformité avec le RGPD pour bon nombre d'organisations.

Le RGPD constitue évidemment une obligation de conformité règlementaire. Aussi il faudra fédérer les compétences et expertises appropriées en interne.

Ainsi, nous pensons que le département juridique devrait participer au programme RGPD en accordant une attention particulière à l'élaboration de politiques, procédures et contrats types.

L'équipe de risque et conformité est tout aussi clé au programme. Pour se conformer avec le RGPD, l'entreprise devra procéder à des évaluations de risques conséquentes et faire preuve de pragmatisme dans son interprétation du règlement.

Evidemment la DSI, le RSSI et leurs équipes mettront en œuvre les aspects du programme relatifs à la confidentialité, l'intégrité, la disponibilité et la traçabilité des données. Les équipes chargées de veiller à la sécurité des informations, notamment les SOC vont par la suite exécuter les mesures de protection et de prévention de la perte de données.

Le RGPD impose un grand nombre d'obligations pour le DPO. Ce dernier devra disposer des compétences suivantes :

- Une connaissance des éléments requis pour déployer un programme à l'échelle de l'entreprise ainsi que l'autorité nécessaire pour opérer les changements requis en vue d'intégrer les contrôles appropriés dans les processus opérationnels ;
- Des compétences liées à la protection des données ;
- La capacité de poser des jugements avisés et de prendre des décisions axées sur les risques rapidement afin de respecter les échéances de reporting ;
- La capacité de piloter le changement au sein de l'organisation ;
- L'autorité suffisante pour élaborer et déployer une stratégie.

Démarrage du projet

Nous pensons qu'une approche « top-down » peut améliorer L'efficacité des programmes de conformité.

Tout d'abord, les organisations devraient faire l'inventaire des données sensibles qu'elles collectent via leur modèle opérationnel et leurs sources de revenus. Il conviendrait aussi de documenter comment ces données collectées sont utilisées. Ce faisant, les entreprises pourront concentrer leurs efforts sur les zones à haut risque qui représentent un enjeu majeur.

Si le processus d'identification de ces données est exécuté correctement, il fera partie de l'étude d'impact sur la vie privée (PIA ou EIVP). Cette analyse est rendue obligatoire en vertu de l'article 35 du RGPD.

Une fois que l'entreprise aura décidé comment réagir face aux problèmes situés dans ces zones à haut risque - exprimant ainsi son appétence pour le risque – elle devra s'efforcer de l'intégrer dans sa politique de conformité. Référencer des exemples actuels de l'EIPV est susceptible de rendre les politiques pertinentes et applicables. Une approche « top-down » peut également garantir que ces politiques sont en adéquation avec les communautés d'utilisateurs présentant un risque élevé. Ainsi qu'avec les processus opérationnels connexes.

Les zones prioritaires initiales seront les suivantes :

- Les données à caractère personnel très sensibles que l'organisation détient en vrac (par exemple, données non-structurées aux formats fichiers, photos, documents numérisés, etc.) ;
- Les données à caractère personnel que l'organisation détient, utilise, ou partage sans que l'individu concerné n'en ait nécessairement conscience ou sans qu'il n'ait donné son consentement.

Les entreprises doivent déterminer rapidement si elles détiennent l'un de ces éléments de données et le cas échéant, se demander si elles n'auraient pas d'inconvénient à ce que leur manière d'utiliser des données à caractère personnel soit rendue publique.

Pour les organisations qui ne possèdent pas de données répondant aux critères précités, le processus de mise en conformité avec le RGPD devrait être relativement simple.

Les sanctions pourraient être plus sévères en cas de non implémentation de processus visant à respecter les droits civils des citoyens, dont le droit à l'oubli (qui leur permet de demander aux entreprises qu'elles suppriment leurs données à caractère personnel), le droit à la portabilité des données (leur permettant de demander que leurs données à caractère personnel soit transmises d'un responsable de traitement à un autre) et/ou si le consentement requis n'a pas été obtenu.

RGPD et programme de conformité : autres points à prendre en considération

Nous préconisons de garder les éléments qui suivent à l'esprit lors de l'élaboration d'un programme de conformité avec le RGPD.

Le RGPD pourrait s'avérer disruptif pour les programmes de transformation digitale. Les obligations du RGPD pourraient avoir un impact significatif sur les projets de de transformation digitale d'une organisation si celle-ci est réticente à demander le consentement de citoyens européens pour utiliser leurs données à des fins commerciales et/ou si les consommateurs ne donnent pas leur consentement en masse. Les organisations qui utilisent des données de clients historiques qui ne donneront probablement pas leur consentement, ou qui n'ont pas de lien direct avec un client, pourraient être confrontées à des difficultés majeures. Les organisations pourraient investir des sommes importantes dans des programmes de transformation digitale pour finalement se rendre compte qu'elles ne sont pas en mesure de générer les bénéfices escomptés en raison de restrictions résultant du RGPD. Par conséquent, lors de l'EIPV, les organisations ont intérêt à tenir compte non seulement de leurs activités en cours, mais aussi d'activités futures qui pourraient s'inscrire dans le cadre d'initiatives de digitalisation.

Les sous-traitants deviennent co-responsables de la gestion des données. Selon la législation en vigueur, les actions intentées contre une organisation doivent l'être à l'encontre du responsable de traitement et le sous-traitant et ce par l'autorité chargée de la protection des données. Selon des accords contractuels, le responsable de traitement pourra transférer ce risque, totalement ou en partie, au sous-traitant. Cependant, il n'est pas inhabituel que, suite à des accords de confidentialité, un responsable de traitement éprouve certaines difficultés à dénoncer publiquement un tiers.

Nous vous préconisons de revoir les pratiques sur l'utilisation de données réelles (ou de production) pour des besoins de tests techniques ou de recettes. Beaucoup trop d'organisations en tendance à banaliser des copies des données réelles sans se soucier de leurs sécurisation (méthode de transfert, contrôle d'accès, anonymisation, pseudonymisation, etc.), Par contre, avec les développements et technologies récentes et accessibles, il serait envisageable de penser à créer des jeux de données fictives en utilisation par exemple la robotique qui pourrait être moins couteux que des chantiers d'anonymisation ou de chiffrement de données.

En application du RGPD, l'autorité chargée de la protection des données peut imposer directement des sanctions au sous-traitant, ce qui pourrait avoir des implications majeures pour les organisations qui traitent des données sensibles pour le compte de tierces parties. Les organisations devront dès lors se focaliser autant sur les données prioritaires qu'elles gèrent pour le compte de tiers que sur celles qu'elles détiennent.

Le responsable de traitement n'a pas nécessairement la main sur la notification des violations de données.

Par conséquent, si un responsable de traitement dissimule des informations, l'autorité de protection des données pourra s'en rendre compte immédiatement. Etant donné les délais de notifications très courts prévus dans la nouvelle règlementation, les entreprises devront prendre des décisions rapides et efficaces. C'est l'une des raisons pour laquelle nous pensons que le DPO devrait être un membre senior de l'organisation.

Actions immédiates

Toutes les organisations devant se conformer au RGPD devraient entreprendre sur le champ les démarches suivantes :

Désigner le DPO : la fonction de DPO doit être assignée rapidement afin de garantir que le programme de conformité avec le RGPD dispose du leadership requis pour assurer son succès. L'organisation devra laisser suffisamment de temps au nouveau DPO pour évaluer les changements à apporter, leur impact, et les appliquer.

Procéder à une analyse « top-down » : C'est un bon point de départ pour élaborer un programme de conformité RGPD. L'analyse permet d'identifier les éléments sensibles ou présentant un risque élevé. Cet exercice permettra également au DPO de saisir rapidement la complexité du RGPD pour l'entreprise et de se concerter au plus vite avec les cadres supérieurs en vue de définir une stratégie de mise en conformité.

Réaliser des EIVP : l'organisation doit réaliser des études d'impact sur la vie privée (EIVP) et documenter les résultats en accord avec l'Article 35. Cette étude approfondie formera la base du plan d'action.

Prioriser les actions : L'entreprise devra définir un plan d'action détaillé avec une définition claire des rôles et responsabilités ainsi que fournir les ressources nécessaires pour exécuter ce plan. Bien qu'il ne soit pas possible de préparer ce plan d'action complet tant que l'EIPV n'est pas finalisé, il est conseillé d'enclencher certaines actions de remédiations pour certains éléments à haut risque le plus tôt possible.

Planifier la remédiation : Le management aura pour mission d'établir un plan détaillé du projet, définissant clairement les rôles et les responsabilités. Le tout devra être étayé par une planification ad-hoc des ressources à disposition. Il est aussi impératif d'analyser les dépendances critiques. Il ne faudra pas sous-estimer l'importance de la formation, de la sensibilisation et des activités de conduite du changement dans ce plan.

Revoir l'EIPV: la conformité avec le RGPD est une obligation permanente, et non pas un projet ponctuel. Il est important pour l'organisation d'établir un processus permettant de revoir régulièrement l'EIPV ainsi que les plans d'assainissement si nécessaire.

Le non-respect des droits civils des citoyens européens et de l'obligation d'obtenir leur consentement est passible de sanctions.

Dans de nombreux cas, une perte isolée de données n'entraîne que des dommages limités, à condition que l'organisation puisse démontrer qu'elle a signalé à temps la perte des données et qu'elle a pu limiter le volume de données perdues.

Les sanctions du RGPD pourraient être plus sévères si une organisation n'implémente pas de processus visant à respecter les droits civils des citoyens européens, dont le droit à l'oubli, ou à obtenir le consentement ad hoc de citoyens européens pour utiliser leurs données à des fins spécifiques (ex. : transmission de données).

A titre d'exemple, une entreprise pourrait être condamnée à payer une amende si une enquête sur une perte présumée de données révèle que l'entreprise a utilisé de manière abusive les données d'un citoyen européen (par exemple : le nom d'un citoyen ayant invoqué son droit à l'oubli n'est pas supprimé d'une liste de mailing gérée manuellement par un employé de l'entreprise). Une sanction pourrait être infligée même en l'absence de perte de données.

A propos de Protiviti

Protiviti aide actuellement des organisations du monde entier à évaluer les implications du RGPD sur leurs activités et à élaborer des programmes de conformité efficients qui reflètent leur culture de risque. Nous sommes conscients qu'il n'existe pas d'approche universelle en matière de conformité avec le RGPD et que chaque organisation est unique.

Nous procédons à des analyses des modèles opérationnels des entreprises qui font appel à nos services afin d'identifier les principales zones de risques. En outre, nous aidons des équipes de management à définir des stratégies de conformité avec le RGPD visant à minimiser l'impact sur de futurs plans opérationnels, y compris relatifs à la transformation digitale. Protiviti est un acteur global de conseil en management et audit interne.

Nos consultants experts assistent nos clients dans les domaines de la finance, des opérations, des projets, des processus, des technologies de l'information, de la cybersecurité, des contentieux, de la gouvernance, de la gestion des risques et de la conformité. Hautement qualifiées et bénéficiant de formations régulières, nos équipes d'experts développent et mettent en œuvre des solutions adaptées et innovantes aux enjeux auxquels sont confrontés nos clients en Europe, au Moyen-Orient, en Asie et en Amérique.

Contacts

Bernard Drui
Country Market Leader
Paris, France
+33 1 42 96 41 16
bernard.drui@protiviti.fr

Arnaud Floquet
Managing Director
Paris, France
+33 1 42 96 22 77
arnaud.floquet@protiviti.fr

Nuvin Goonmeter
Managing Director
Paris, France
+33 1 42 96 22 77
nuvin.goonmeter@protiviti.fr