

Accompagnement au RGPD

Mise en conformité de votre SI au RGPD : Interdata vous accompagne

Le règlement relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (RGPD) a une date d'entrée en vigueur au 25 mai 2018.

Quel est ce règlement ? Suis-je concerné ? Que cela implique- t'il pour mon organisation ?

Voici quelques-unes des questions que vous vous posez sûrement. Une chose est sûre, les entreprises privées et les entités publiques doivent engager au plus vite une démarche de mise en conformité.

Fort de ses recherches, de son expertise et de son expérience acquise depuis plusieurs années autour des solutions de sécurité du système d'information et grâce à son service d'audit SafeView, Interdata est un allié dans la mise en conformité de votre SI au RGPD.

Pour amorcer cette mise en conformité, nous avons élaboré les étapes suivantes :



Initialisation du projet

Interdata peut sensibiliser la direction pour la mise en place de moyens humains et financiers afin d'entrer en conformité avec le RGPD au travers de présentations ciblées.



Définition d'un cadre projet RGPD

Interdata propose des prestations permettant l'identification et la localisation des données concernées. Par une méthode d'audit, nous identifions les acteurs interagissant avec ces données, mais aussi la nature et la durée des traitements de ces données.



Identification des traitements à risque et gestion des risques

Le cadre juridique RGPD permet d'identifier les traitements à risque. Pour les plus sensibles, une étude d'impact sur la vie privée (EIVP) est requise. Nous vous proposons nos méthodes d'étude de risque type EBIOS qui sont en totale adéquation avec l'analyse des risques potentiels sur les données privées traitées au sein de vos projets.



Protection des données

Interdata, fort de son expertise et de son offre, vous propose un ensemble d'outils pour sécuriser les données, l'accès à ces données ainsi que leurs traitements : firewall applicatif, SIEM, gestion des politiques de sécurité, authentification forte, contrôle d'accès...



Organisation des processus internes : Privacy by design , réclamation, déclarations ...

Interdata accompagne votre organisation pour établir les lignes directrices d'intégration des processus liés à la gestion des risques sur les données privées dans vos projets de traitement. Cela peut aller de la simple prise en compte des processus de protection jusqu'à la gestion et le traitement des réclamations en passant par la notification des autorités en cas de brèche.



Respect des obligations liées à la conformité

Enfin, dans une volonté de suivi du projet de protection des données privées, un contrôle continu des processus de traitement des données peut être mis en place afin d'assurer la mise à jour permanente des documentations servant de preuves à la conformité.

RGPD en bref

Quels sont les objectifs ?

Ce règlement a pour but d'établir des règles quant au traitement et à la libre circulation des données à caractères personnels. L'objectif est de protéger les libertés et les droits fondamentaux des personnes physiques résidant dans l'Union Européenne (art. 1).

Comme tout règlement, il s'applique directement et instantanément le 25 mai 2018 à tous les pays de l'UE sans passer par une loi ou un décret d'application national.

Quelles sont les obligations ?

- *Obligation de protéger les données dès la conception du traitement (privacy by design) et de les protéger par défaut (privacy by default) (art.25).*
- *Obligation de documentation via un registre qui contient toutes les informations relatives à la collecte, au traitement etc..(art. 30)*
- *Obligation de sécurité des données et du traitement telles que la « pseudonymisation », le chiffrement, la capacité à rétablir la disponibilité des données, la mise en place de procédures pour tester régulièrement la sécurité et le traitement des données (art. 32). Ceci est une obligation de moyens et non une obligation de résultats.*
- *Obligation de réaliser des analyses d'impacts, si le risque est élevé pour les droits et libertés des personnes physiques (données sur les idées politiques, sur la santé ...) (art. 35).*

Quels sont les risques encourus en cas d'irrespect du règlement

- *Une amende plafonnée à 2% du chiffre d'affaires global ou 10 millions d'€ pour les organisations n'ayant pas convenablement fait la documentation, n'ayant pas informé l'autorité de contrôle d'une violation ou encore n'ayant pas réalisé les analyses d'impacts (art. 83 § 4).*
- *Une amende plafonnée à 4% du chiffre d'affaires global ou 20 millions d'€ pour les infractions plus graves telles que la violation des principes de base de la sécurité des données et des conditions de consentement des utilisateurs (art. 83, § 5).*
- *Les victimes peuvent aussi saisir le tribunal pour demander réparation du préjudice subi (art. 82).*

Qui est concerné ?

Ce règlement s'applique à toute organisation qui collecte, traite et / ou stocke des données personnelles de citoyens européens et dont l'utilisation peut directement ou indirectement identifier une personne physique ; peu importe que l'organisation ou les données soient situées dans l'UE ou à l'extérieur de l'UE, du moment que les données concernent des citoyens européens (art. 3).

- *Obligation d'informer l'autorité de contrôle de toute violation des données à caractère personnel (destruction, perte, divulgation ou accès non autorisé à ces données) sous 72h après la découverte de la violation (art. 33). Obligation d'informer aussi la ou les personnes physiques concernées par la violation des données à caractère personnel (art. 34).*
- *Obligation de nommer un délégué à la protection des données si le traitement est réalisé par une autorité publique, si le traitement exige un suivi particulier ou si le traitement repose sur des données sensibles à grande échelle (art. 37 à 39). Son rôle est d'informer, de faire respecter le règlement, de faire les analyses d'impact et d'être le point de contact avec l'autorité de contrôle.*

Contactez-nous

01 64 86 86 00

contact@interdata.fr

www.interdata.fr

RGPD

Interdata est votre partenaire de confiance face à cette nouvelle réglementation européenne et s'engage auprès de vous dans cette démarche.