VERLINGUE
COURTIER EN ASSURANCES

Fiche Technique

Mai 2018

RGPD : mode d'emploi

QUELQUES BONNES PRATIQUES POUR ÊTRE « RGPD COMPATIBLE » ET GAGNER DU TEMPS !

> Disposer d'un Délégué à la Protection des Données (DPO) qui pilote la gouvernance des données personnelles de l'entreprise et exerce une mission d'information, de conseil et de contrôle en interne.

> Prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement : minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, rôle et responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données.
Le Délégué à la Protection des Données doit être sollicité.

> Inventorier les traitements de données à caractère personnel à l'aide de la cartographie des applications traitant ou stockant les données

> Sensibiliser et organiser la remontée d'information en construisant notamment un plan de formation et de communication auprès des collaborateurs.

> Traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen).

> Appliquer les principes de sécurity by default par des mesures adaptées aux risques et des procédures périodiques de test de sécurité des SI afin de limiter les risques de faille de sécurité.

L'ANALYSE D'IMPACT SUR LA PROTECTION DES DONNÉES (PIA) : POUR LES TRAITEMENTS SUSCEPTIBLES D'ENGENDRER DES RISQUES ÉLEVÉS

Qu'est-ce qu'une analyse d'impact sur la protection des données (PIA) ?

C'est une étude aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD.

Un PIA est un outil d'évaluation d'impact sur la vie privée qui repose sur 2 piliers :

> Les principes et droits fondamentaux, « non négociables », fixés par la loi. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus.

> La gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriée pour protéger les données personnelles.

Un PIA contient :

- Une description du traitement étudié et ses finalités
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités
- Une évaluation des risques pour les droits et libertés des personnes concernées, ainsi que les mesures envisagées pour faire face aux risques

Quand mener une analyse d'impact sur la protection des données (PIA) ?

Mener un PIA est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées (article 35 du RGPD).

Pour vous aider à déterminer le degré de risque, les 9 critères suivants sont définis :

- Évaluation ou notation
- Décision automatisée avec effet juridique ou effet similaire significatif
- Surveillance systématique
- Données sensibles ou données à caractère hautement personnel
- Données personnelles traitées à grande échelle
- Croisement d'ensembles de données
- Données concernant des personnes vulnérables
- Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles
- Exclusion du bénéfice d'un droit, d'un service ou contrat

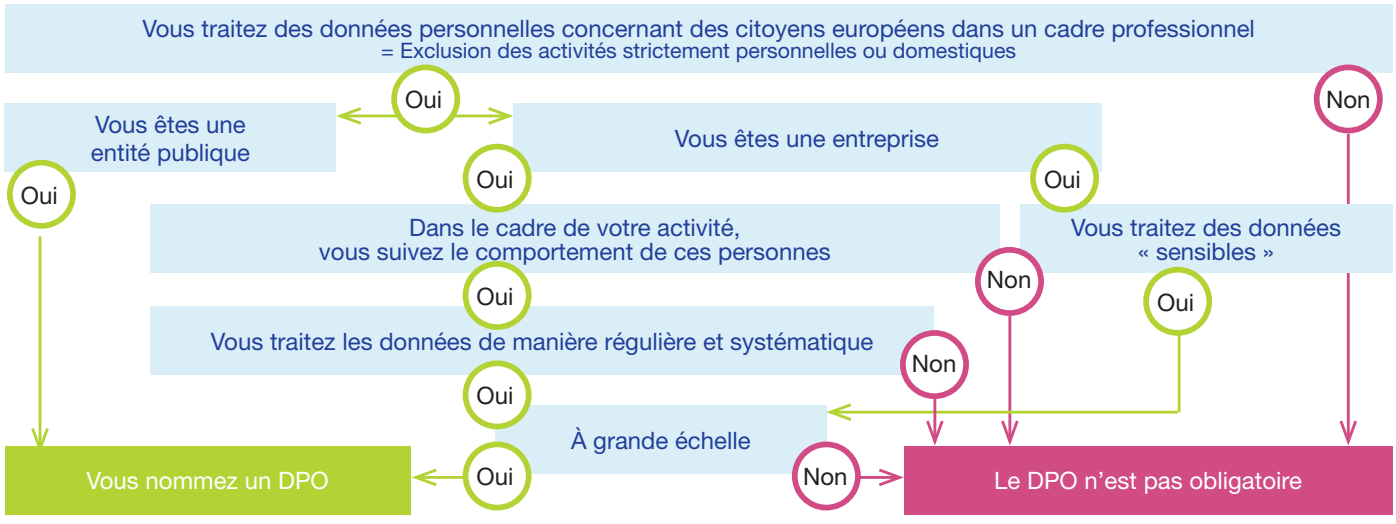
Si votre traitement rencontre au moins 2 de ces critères, alors il est vivement conseillé de faire un PIA.

De manière générale, le PIA est une bonne pratique pour créer un traitement conforme au RGPD et respectueux de la vie privée, que celui-ci soit susceptible ou non d'engendrer des risques élevés. Il doit être réalisé avant la mise en œuvre du traitement. C'est un processus itératif, les analyses doivent être revues et corrigées de manière régulière, en particulier lors de changements majeurs des modalités d'exécution du traitement.

Qui participe à l'élaboration de l'analyse d'impact ?

- Le responsable de traitement : valide le PIA et s'engage à mettre en œuvre le plan d'actions défini
- Le délégué à la protection des données : élabore le plan d'actions et se charge de vérifier son exécution
- Le(s) sous-traitant(s) : fourni(ssen)t les informations nécessaires à l'élaboration du PIA
- Les métiers (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre) : aident à la réalisation du PIA en fournissant les éléments adéquats
- Les personnes concernées : donnent leurs avis sur le traitement

DEVEZ-VOUS DÉSIGNER UN DPO (DATA PROTECTION OFFICER) ?



Directeur de la publication : Éric Maumy - Responsable de la rédaction : Benoît Le Corre - Imprimeur : Cloître Imprimeurs ZA Voie express RN 12 29800 Saint-Thonan - Date de parution et de dépôt légal : mai 2018 - N° ISSN : 2106 - 5144
Siège social : 12 rue de Kerogan - CS 44012 - 29335 QUIMPER Cedex Tel 0 820 260 260 (0,118 € TTC/mn) Fax 0 820 209 242 / SAS au capital de 2 200 294 € / Code APE 6622 Z / Siren 440 315 943 RCS QUIMPER / Numéro ORIAS : 07000 840 - www.orias.fr - N° de TVA intracommunautaire FR 95 440 315 943 - Relevant du contrôle de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution) 61 rue Taitbout 75009 PARIS [12.16].