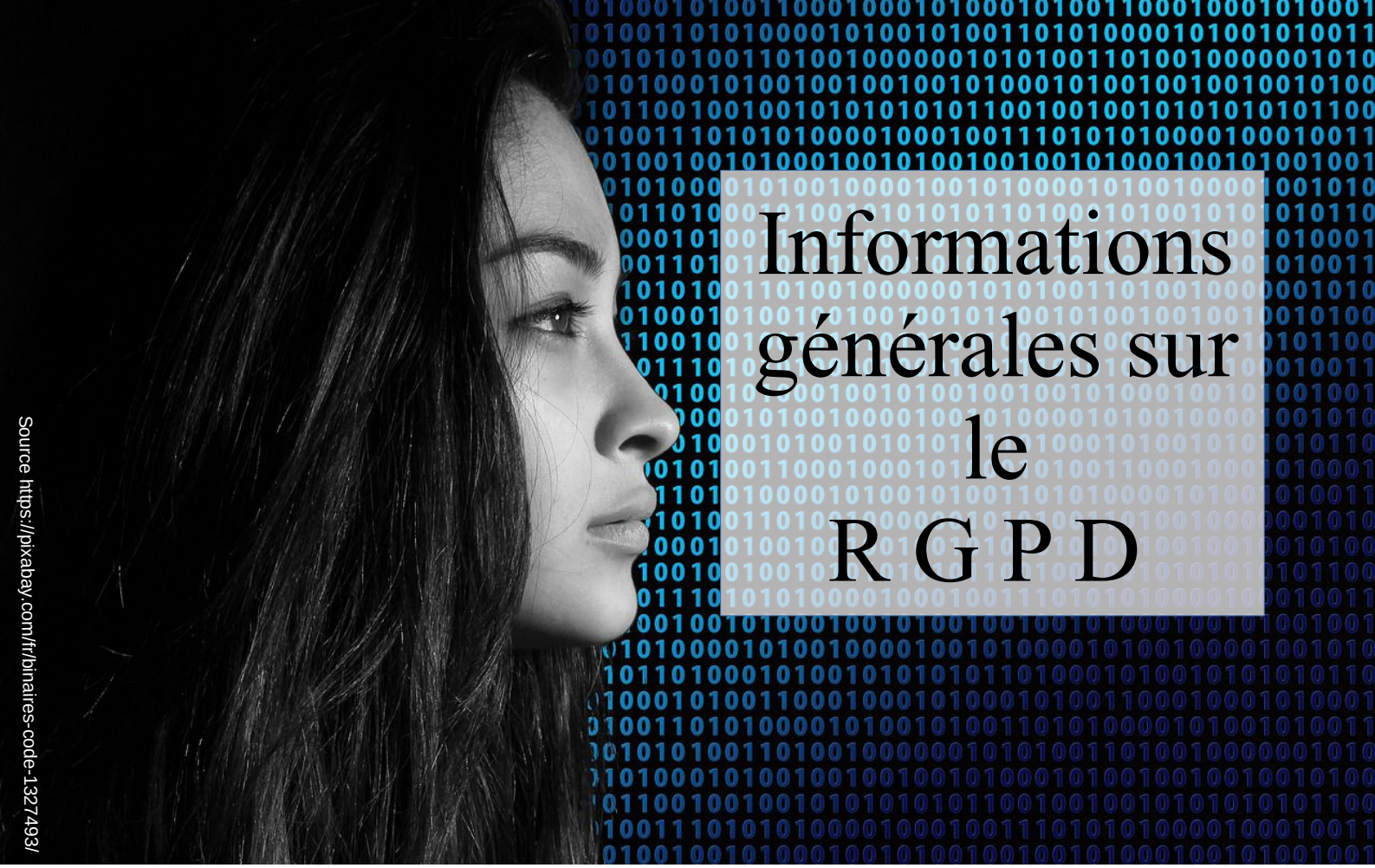

Source https://pixabay.com/fr/binaires-code-1327493/

Cette fiche n'a qu'une valeur de sensibilisation au sujet. La complexité du RGPD nécessite pour ceux qui sont concernés un travail approfondi plus ou moins long en fonction de leur structure et de leurs activités. Un accompagnement est toujours possible avec des cabinets spécialisés en autre pour le PIA.

C'est quoi :

Le **R**ègle**m**ent **G**énéral sur la **P**rotection des **D**onnées est un texte de loi à l'échelle Européenne ayant pour vocation de protéger la vie privée des citoyens européens vis a vis du traitement de la donnée personnelle, face aux nouvelles réalités du numérique.
Adopté par le Parlement Européen en début d'année 2016, il entrera en application le 25 mai 2018.

Texte 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Qui est concerné :

Les acteurs concernés sont l'Etat, les collectivités, les associations et les entreprises, aussi bien les multinationales que les PME, qui traitent les données personnelles des ressortissants européens.

Les objectifs du RGPD :

- Harmoniser les pratiques en terme de protection des données à l'échelle européenne par application directe du règlement à l'ensemble des états.
- Renforcer les règles existantes en matière de collecte et de traitement des données à caractère personnel pour garantir les droits des citoyens, notamment face à l'émergence de nouvelles technologies .
- Permettre un meilleur recours pour les particuliers vis à vis de leurs droits.

LES DIFFERENTES ETAPES :

-1 - Désigner un responsable

Même si votre organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des données (DPO), il est fortement recommandé de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen. Le délégué constitue un atout majeur pour comprendre et respecter les obligations du règlement, dialoguer avec les autorités de protection des données et réduire les risques de contentieux.

- 2 - Cartographier

Recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point. Pour chaque traitements de données personnelles posez vous ces questions :

QUI…….. A la charge du traitement de la donnée personnelle
QUOI……Identifiez les catégories de données traitées
POURQUOI ……..Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données
OU…….Les données sont hébergées comment et à quel endroit.
JUSQU'A QUAND….. combien de temps vous les conservez.
COMMENT……. Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données en question ?

- 3 – Prioriser les actions à mener,

au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

- 4 - Gérer les risques :

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

Consulter les guides PIA de la CNIL

- 5- Organiser :

Mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire)

- 6 – Documenter

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu. Cette documentation vous sera demandée en cas de contrôle.

Se préparer en 6 étapes avec la CNIL

Quelles données sont concernées :

Toutes les données qui permettent d'identifier directement ou indirectement une personne. Ces données peuvent être de nature diverse : nom, prénom, adresse e-mail, numéro de téléphone, adresse IP, etc.
Les données sensibles, au sens de la loi, sont des données pour lesquelles une attention particulière doit être portée. Il faudra notamment réaliser une analyse d'impact sur la vie privée et obtenir un consentement explicite des personnes concernées. Il s'agit de :
- Données de santé, données biométriques et génétiques
- Opinions politiques, religieuses ou philosophiques, appartenance syndicale
- Origine « raciale » ou « ethnique » - Orientation et vie sexuelle

Soyez concernés par cette règlementation :

- Le RGPD vous oblige à prendre des mesures concrètes de protection de la données personnelle avec par exemple :

• une formation continue de l'ensemble de vos collaborateurs.
• Mettre en place des procédures sur la collecte, le traitement, le stockage et le transfert de données afin de s'assurer de la conformité vis-à-vis de la réglementation (durée de conservation, anonymisation, consentement, autorisation auprès de l'autorité de tutelle, ...).
• Assurer une procédure d'évaluation des impacts en matière de protection des données pour toute création de produits ou lancement de projets internes.
• Améliorer le processus de suppression des données personnelles et anticiper les changements dans les systèmes d'informations.

En savoir plus avec *:*

- Site SIAPARTNER : Les fiches synthèses du RGPD
- Comprendre le RGPD par la vidéo et les emojis
- Se préparer au règlement européen avec la CNIL