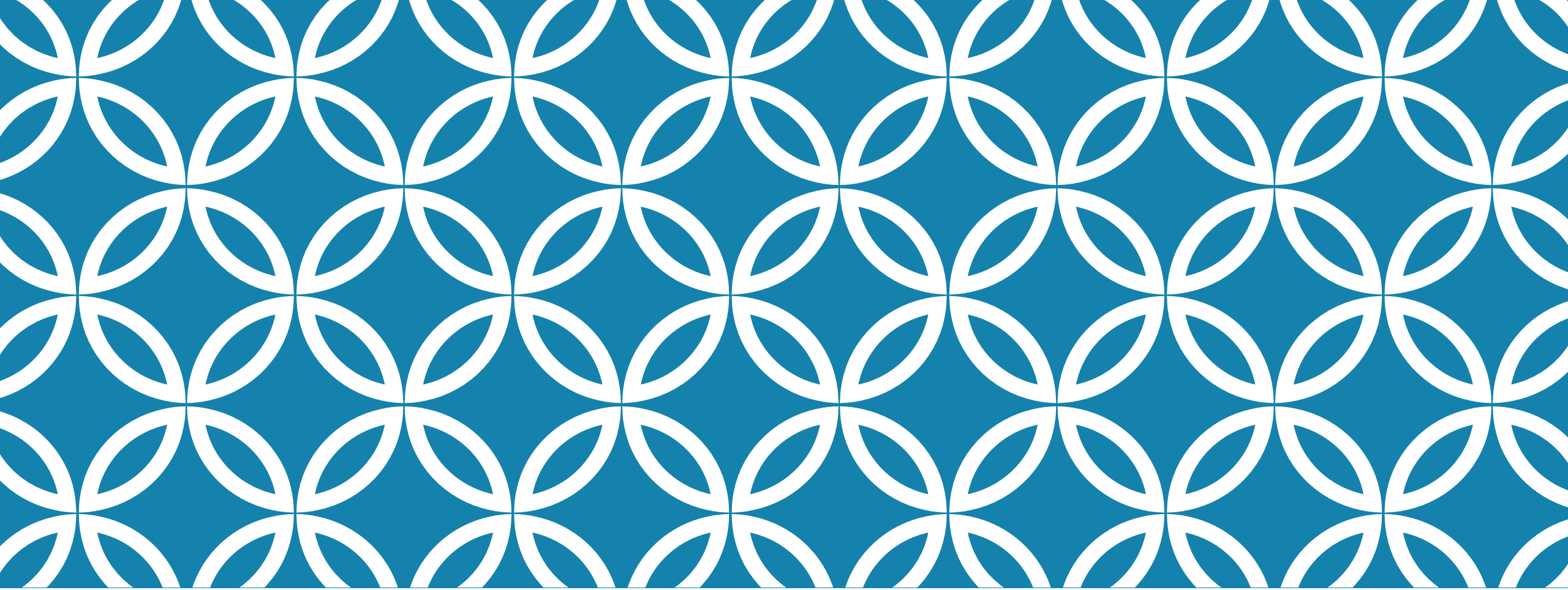

PROTECTION DES DONNÉES PERSONNELLES GDPR

INTRODUCTION

Le GDPR* (ou RGDP en français) est le nouveau règlement européen (Règlement 2016/679) sur la protection des données personnelles, entré en vigueur le 24 mai 2016, et applicable le 25 mai 2018.

Seront concernées toutes les entreprises, collectivités, associations… manipulant des données à caractère personnel de résidents européens.

* Général Data Protection Regulation

POURQUOI LE GDPR?

La donnée est le nouveau pétrole de notre monde!

Nos données sont partout.

Le GDPR est un règlement obligatoire dont l'objectif est de protéger les citoyens de l'UE à l'égard du traitement des données à caractère personnel.

Il est temps pour l'UE de rattraper son retard en matière de cybersécurité et de préparer les états-membres en termes stratégiques, législatifs et opérationnels afin de répondre de manière efficace aux cyber-menaces et d'assurer la cyber-résilience de l'UE pour le futur.

LES SANCTIONS DU GDPR

Dès lors, les entreprises qui ne respectent pas les dispositions de ce règlement (manquement délibéré ou négligence) s'exposeront à des pénalités pouvant aller jusqu'à 4 % de leur revenu mondial ou 20 millions d'euros.

=> Démontrer les procédures et politiques mises en place même en cas d'absence de violation des données

QU'EST-CE QUE LA DONNÉE PERSONNELLE?

« Les données sont considérées « à caractère personnel » dès lors qu'elles concernent des personnes physiques identifiées ou identifiables directement ou indirectement.»

Photographie

N° de téléphone

Nom – prénom

N° d'immatriculation

Empreinte digitale

Adresse IP

Infractions pénales et condamnations

Philosophie religieuse

Génétique

Appartenance syndicale

Opinion politique

Orientation sexuelle

Origine raciale

Ethnique

NOS DONNÉES SONT DES EMPREINTES DIGITALES QUE NOUS LAISSONS PARTOUT OÙ NOUS PASSONS

TYPOLOGIE DES DONNÉES A CARACTERE PERSONNEL (CDP)

EXTRAIT DU GUIDE CNIL PIA, L'OUTILLAGE (P5 /25)

Les catégories sont généralement les suivantes :

- DCP courantes :État-civil, identité, données d'identification Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses…) Vie professionnelle (CV, scolarité formation professionnelle, distinctions…) Informations d'ordre économique et financier (revenus, situation financière, situation fiscale…) Données de connexion (adresses IP, journaux d'événements…) Données de localisation (déplacements, données GPS, GSM…)
- DCP perçues comme sensibles: Numéro de sécurité sociale (NIR) Données biométriques Données bancaires
- DCP sensibles au sens de la [Loi-I&L]1: Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle Infractions, condamnations, mesures de sécurité

LES DONNÉES PERSONNELLES SONT UNE CIBLE DE CHOIX POUR LES HACKERS

A secteur équivalent, une entreprise française consacre en moyenne un budget 10X inférieur à ses homologues américains pour la protection des données.

Le pays occupe le 2nd rang européen et 4ème mondiale en matière de cyber menaces recensées.

NOUS SOMMES TOUS CONCERNES!

«Le règlement s'applique au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union »

Entreprises

Collectivité locales

Administrations

Syndicat d'entreprise

Associations

QU'EST CE QUE LE TRAITEMENT DE LA DONNÉE?

«Un traitement est une opération ou un ensemble d'opérations appliquées à des données à caractère personnel.»

Cette mise en conformité concerne en grande partie les traitements que vous effectuez sur les données à caractère personnel.

En effet, le but du GDPR est de protéger les citoyens européens à l'égard du traitement des données à caractère personnel. Et à partir du moment où vous … une donnée à caractère personnel, on parle de traitement de la donnée.

… Enregistrez

…Collectez

… Transmettez / diffusez

… Extrayez

… Détruisez

… Conservez

L'EUROPE A ÉLABORÉ LE « GENERAL DATA PROTECTION REGULATION »

3 GRANDS AXES :

- Droits des personnes physiques
- Obligations
- Mise en conformité

DROITS DES PERSONNES PHYSIQUES (CHAPITRE III – 2016/679)

12 articles y font références, quelques points en exemple :

Consentement clair requis

Droit de rectification et de suppression

Droit à l'oubli

Droit à l'information en cas de piratage de données personnelles et/ou incident lié à la sécurité dans les 24 heures

Droit à la portabilité

OBLIGATIONS

«Mettre en place une gestion des risques pour assurer une cyber résilience»

Prévenir des fuites

Informer en cas d'incident les autorités dans les 72h

Présenter les logs suite à un incident

MISE EN CONFORMITÉ : SE PREPARER EN 6 ETAPES

La mise en conformité concerne toutes les actions et obligations à mettre en œuvre afin de respecter le règlement général sur la protection des données.

1. **Désigner un pilote**
2. **Cartographier vos traitements de données personnelles**
3. **Prioriser les actions**
4. **Gérer les risques**
5. **Organiser les processus internes**
6. **Documenter la conformité**

Retrouvez le détail des étapes sur le site de la CNIL : https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

DÉSIGNER UN PILOTE

La désignation d'un délégué à la protection des données est obligatoire en 2018 si :

- vous êtes un organisme public
- vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et à des infractions*

Le pilote met en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer, et être en mesure de démontrer, que les traitements sont effectués conformément au GDPR.

En cas sous-traitance, cette responsabilité ne peut pas être remise en cause.

Le responsable du traitement doit s'assurer de la conformité du sous-traitant auquel il fait appel. En termes de mesures organisationnelles, on retiendra la mise en place de campagnes de sensibilisation aux données à caractère personnel. Les mesures techniques et la documentation des traitements s'articulent autour de la gestion des risques, afin d'assurer une cyber résilience, et du « Privacy by design ».

Le responsable du traitement doit être en mesure de justifier des moyens mis en œuvre pour répondre aux obligations du règlement.

*Même si votre organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des données, 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.

CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre. La tenue d'un registre des traitements vous permet de faire le point.

- les différents traitements de données personnelles
- les catégories de données personnelles traitées
- les objectifs poursuivis par les opérations de traitement de données
- les acteurs (internes ou externes) qui traitent ces données
- vous devrez notamment clairement identifier les prestataires sous-traitants, les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne

QUI? **OÙ?** **QUOI?** **JUSQU'À QUAND?** **POURQUOI?** **COMMENT?**

PRIORISER LES ACTIONS

Identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

- Assurez-vous que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.
- Identifiez la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale).
- Révisez vos mentions d'information afin qu'elles soient conformes aux exigences du règlement.
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées. Prévoyez les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...).
- Vérifiez les mesures de sécurité mises en place.

PRIORISER LES ACTIONS (SUITE)

Points d'attention nécessitant une vigilance particulière

- Vous traitez certains types de données : des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, - des données relatives à la santé ou l'orientation sexuelle, - des données génétiques ou biométriques, - des données d'infraction ou de condamnation pénale, - des données concernant des mineurs.

- Votre traitement de données personnelles a pour effet : la surveillance systématique à grande échelle d'une zone accessible au public, l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

- Vous transférez des données hors de l'Union européenne ? Vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne. - Dans le cas contraire, encadrez vos transferts

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 étude d'impact sur la protection des données (en anglais, Privacy Impact Assessment ou PIA).

Les outils pour vous aider :

La CNIL met à votre disposition sur son site les guides PIA, catalogues de bonnes pratiques qui vous aide à déterminer les mesures proportionnées aux risques identifiés, en agissant sur :

- les « éléments à protéger » : minimiser les données, chiffrer, anonymiser, permettre l'exercice des droits, etc.
- les « impacts potentiels » : sauvegarder les données, tracer l'activité, gérer les violations de données etc.
- les « sources de risques » : contrôler les accès, gérer les tiers, lutter contre les codes malveillants etc.
- les « supports » : réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier etc.

Retrouvez le guide PIA de la CNIL : https://www.cnil.fr/fr/PIA-privacy-impact-assessment

ORGANISER LES PROCESSUS INTERNES

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent 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 de données personnelles (par exemple : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire etc.).

Organiser les processus implique notamment de :

- Prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement.
- Sensibiliser et organiser le remontée d'information en organisant un plan de formation et/ou de communication auprès de vos collaborateurs
- Traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits
- Anticiper les violations de données en prévoyant la notification de protection des données dans les 72h et aux personnes concernées dans les meilleurs délais.

DOCUMENTER LA CONFORMITÉ

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.

Votre dossier devra notamment comporter les éléments suivants :

- La documentation sur vos traitements de données personnelles
- L'information des personnes
- Les contrats qui définissent les rôles et les responsabilités des acteurs