VEILLE JURIDIQUE :

Sujet : *La protection des données personnelles (Règlement Général sur la Protection des Données)*

Contexte :

L'essor technologique et l'ampleur croissante de la collecte et du traitement des données personnelles ont soulevé des inquiétudes quant à la protection de la vie privée et des droits des individus, mettant ainsi les entreprises et les développeurs d'applications et de logiciels au centre de ces enjeux.

Dans ce contexte, de nombreuses juridictions ont mis en place des réglementations spécifiques pour encadrer la protection des données personnelles

Les entreprises doivent désormais s'assurer qu'ils collectent et traitent les données personnelles de manière légale et transparente, en obtenant le consentement approprié des individus et en mettant en place des mesures de sécurité adéquates pour protéger les données.

Les utilisateurs sont de plus en plus conscients de leurs droits en matière de protection des données et sont plus exigeants quant à la manière dont leurs informations personnelles sont traitées.

I) Nouvelles directives

Le nouveau règlement européen sur la protection des données personnelles est entré en application le 25 mai 2018.

Source :
https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

- Un cadre juridique unifié pour l'ensemble de l'UE

Le règlement européen adopté est directement applicable dans tous les États membres de l'Union européenne depuis le 25 mai 2018.

- Un renforcement des droits des personnes
- Consentement renforcé et transparence : les utilisateurs doivent être informés de l'utilisation de leurs données et doivent généralement donner leur accord pour que leurs données soient traitées, ou avoir la possibilité de s'y opposer.
- De nouveaux droits :
  - Le droit à la portabilité des données,
  - Des conditions particulières pour le traitement des données des enfants,
  - Introduction du principe des actions collectives,
  - Un droit à réparation des dommages matériel ou moral.

- Une conformité basée sur la transparence et la responsabilisation :
  - Une clé de lecture : la protection des données dès la conception et par défaut (privacy by design),
  - Un allègement des formalités administratives et une responsabilisation des acteurs,
  - Les « analyses d'impact relatives à la protection des données » (AIPD ou PIA),
  - Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements,
  - Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué sous certaines conditions.

- Des responsabilités partagées et précisées :
  - Le représentant légal
  - Le sous-traitant

- Le cadre des transferts hors de l'Union mis à jour
- Des sanctions encadrées, graduées et renforcées :
  - Prononcer un avertissement
  - Mettre en demeure l'entreprise
  - Limiter temporairement ou définitivement un traitement
  - Suspendre les flux de données
  - Ordonner de satisfaire aux demandes d'exercice des droits des personnes
  - Ordonner la rectification, la limitation ou l'effacement des données.

II) Décisions et sanctions
Source :
https://www.cnil.fr/fr/mission-4-controler-et-sanctionner#:~:text=Avec%20le%20RGPD%20(r%C3%A8glement%20g%C3%A9n%C3%A9ral,sanctions%20peuvent%20%C3%AAtre%20rendues%20publiques.

Les procédures de sanction de la CNIL :
Si les responsables de traitement et les sous-traitants ne respectent pas les dispositions du RGPD ou de la loi, la présidente de la CNIL peut prendre des mesures de sanction, soit de manière ordinaire, soit de manière simplifiée, suite à des contrôles ou des plaintes.

1. La procédure de sanction ordinaire
   - Prononcer un rappel à l'ordre
   - Enjoindre de mettre le traitement en conformité, y compris sous astreinte
   - Limiter temporairement ou définitivement un traitement
   - Suspendre les flux de données
   - Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte
   - Prononcer une amende administrative.

2. La procédure de sanction simplifiée
   Le président de la formation restreinte peut :
   - Prononcer un rappel à l'ordre
   - Enjoindre de mettre le traitement en conformité, y compris sous astreinte d'un montant maximal de 100 € par jour de retard
   - Prononcer une amende administrative d'un montant maximal de 20 000 €.

III) Bonnes pratiques et conformité
Source :
https://www.blogdumoderateur.com/conformite-rgpd-bonnes-pratiques/

En quoi la conformité RGPD est-elle devenue un enjeu majeur aujourd'hui pour les entreprises ?
La protection des données personnelles est essentielle pour maintenir l'activité des entreprises, car leur mauvaise gestion peut entraîner des risques financiers, de réputation et de cyber sécurité, et qu'elle est désormais intégrée dans un cadre plus large d'éthique, de responsabilité sociale des

entreprises (RSE) et de cyber sécurité, nécessitant une documentation approfondie et une approche proactive de conformité.

Selon vous, quelles sont les principales bonnes pratiques à suivre pour être en conformité RGPD ? Avez-vous des exemples concrets ?
Jérôme de Mercey, cofondateur et COO de Dastra souligne l'importance de consacrer des ressources et d'intégrer la protection des données personnelles dans la stratégie globale de l'entreprise. Cela implique une gouvernance interne, une communication adéquate, l'utilisation d'outils de gestion des données personnelles, comme ceux proposés par Dastra, et l'adoption de bonnes pratiques dans toutes les activités de l'entreprise. L'implication des différents métiers est essentielle, par exemple en prenant en compte les critères de respect du RGPD lors des achats d'outils ou de services, et en collaborant avec les experts en la matière. Il est également important de se poser des questions pertinentes au sein de chaque service pour optimiser et maintenir un environnement propre en matière de données.

Quels types d'outils peuvent aider les entreprises à s'assurer qu'elles sont en conformité avec le RGPD ?
Il existe des outils spécialisés, tels que Dastra, qui aident à assurer la conformité au RGPD en facilitant la gestion des processus internes, tels que la tenue de registres, le suivi des actions de conformité et la réalisation d'audits pour garantir la responsabilité.

Dastra : est une plateforme RGPD qui permet aux délégués à la protection des données de répondre à toutes les obligations du RGPD : registre, exercices de droits, incidents, PIA, privacy by design, en mode projet, de manière didactique et collaborative.
L'entreprise Dastra a été créée en 2018 par Paul-Emmanuel et Antoine, deux cousins aux compétences complémentaires, avec pour objectif de rendre la protection des données accessible à tous au sein des organisations.