RGPD AVOIR TOUJOURS LES BONS RÉFLEXES

Fiche n°1

La CNIL frappe à votre porte : que faire ou ne pas faire ?

CONTEXTE

La CNIL a le pouvoir de contrôler tout organisme qui traite des données à caractère personnel (DCP).
Dans le cadre de ses missions, la Commission effectue régulièrement des contrôles pour s'assurer du respect de la loi informatique et libertés du 6 janvier 1978 et du règlement général sur la protection des données (RGPD) du 27 avril 2016.

L'ESSENTIEL À RETENIR

- Maintenir ma documentation à jour de manière proactive et qu'elle soit conforme au RGPD.

- Identifier et « coacher » les interlocuteurs du contrôle.

L'audition de contrôle peut s'effectuer selon diverses situations :
- Par essence même de certains métiers traitant régulièrement des données
- La déclaration d'un problème de sécurité ou d'une fuite/perte de données
- La dénonciation par un tiers ayant été sollicité sans son consentement
- Une initiative de la Commission

Elle a la possibilité d'intervenir de quatre manières différentes, que sont :
- Le contrôle sur place
- L'audition sur convocation
- Le contrôle en ligne
- Le contrôle sur pièces

Le site de la CNIL détaillant suffisamment bien les procédés mis en place lors d'un contrôle, nous vous invitons à vous y référer directement : https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil

ACTIONS À RÉALISER

- Maintenir la relation avec les personnes :

Informer : Expliquer les finalités du traitement des données mis en œuvre et préciser les droits des personnes concernées
Suivre : Conserver les traces des demandes et tenir un recueil des consentements
Traiter : Répondre et conserver les réponses faites aux personnes

- S'assurer régulièrement de la mise à jour des documents :

Mettre à jour ses politiques et procédures de traitement des données.
Tenir son registre de traitement **à jour.**

- Renforcer la sécurité

Sécuriser ses sites web
Sécuriser des lacunes de sécurité visibles en réalisant des tests
Ex : l'accès à des domaines privées (comptes, extranet)

- Éviter les fuites de données

De manière générale **sécuriser au mieux ses applications** hébergeant des DCP, en suivant l'état de l'art. (Il n'y a pas obligation de résultat mais de moyen : par exemple laisser une faille de sécurité critique connue non patchée sera reprochée, mais une attaque sur une faille 0 day non connue non).

- Faire des audits à blanc de ses systèmes informatiques

Lancer des requêtes sur son système pour vérifier son bon fonctionnement (ex : effacement d'une donnée)
Conserver les rapports d'audit dont vous disposez

POUR ALLER PLUS LOIN

Club Utilisateurs Oracle : Découvrez le Replay du Webinar Mise en conformité RGPD – Audit à Blanc (1er octobre 2020) : https://www.youtube.com/watch?v=tSgmMbDxAQc

POINTS DE VIGILANCE

Lors de tout type de contrôle, nous pouvons retenir deux règles d'or :

1) Déterminer quels sont les acteurs qui ont le droit de parler et maîtriser le champ d'action des personnes qui répondent et qui en ont l'autorisation

2) Répondre factuellement aux questions pour ne pas donner d'autres idées de contrôle

Il est conseillé d'avoir la présence de tous les acteurs concernés par le contrôle, tel que le juriste, le référent RGPD ou DPD, le Responsable du Traitement, les chefs de projets, etc...
Pour rappel, **la CNIL est en droit d'interroger toutes les personnes qu'elles soient technique ou métier dans le cadre du contrôle.**

Prévenir tout le personnel du contrôle dans le cas où d'autres acteurs seraient interrogés sur les moyens de traitements mis en place.

RISQUES

- Ne pas prendre à la légère les contrôles effectués par la Commission.
- Connaître les peines encourues : https://www.cnil.fr/fr/les-sanctions-penales
- S'informer sur les sanctions et les risques d'un contrôle.

Exemple d'une sanction de la CNIL sur la société Carrefour :
https://www.cnil.fr/fr/sanctions-2250000-euros-et-800000-euros-pour-carrefour-france-carrefour-banque