racine
AVOCATS

FEDERATION EBEN
ENTREPRISES DU BUREAU ET DU NUMERIQUE

Conformité RGPD et DPO eben mutualisé

PARTIE 1

Un an après ou en sommes nous ?

Retour sur une année exceptionnelle

L'entrée en application du RGPD a marqué une forte prise de conscience des enjeux de protection des données, en France comme en Europe. Cela s'est traduit pour les particuliers, sur la période de mai 2018 à mai 2019, par :

- une augmentation considérable des plaintes adressées à la CNIL : plus de **11 900 plaintes en France** (+ 30 %) et 144 376 plaintes au niveau européen ;
- une **coopération européenne engagée et opérationnelle** entre les CNIL européennes sur **1 013 procédures concernant plusieurs milliers de personnes**, dont plus de 800 dans lesquelles la CNIL est impliquée.

70 % des Français se disent aujourd'hui plus sensibles aux problématiques de protection des données.

Sondage IFOP réalisé en avril 2019 sur un échantillon de 1 000 personnes, représentatif de la population française de 18 ans et plus, selon la méthode des quotas.

Cette prise de conscience se manifeste également chez les professionnels, qui s'approprient progressivement les nouveaux dispositifs du RGPD :

- **2 044 notifications de violation de données** en France et 89 271 au niveau européen ;
- **plus de 19 000 délégués à la protection des données** (personnes physiques ou morales) ont été désignés par plus de 53 000 organismes ;
- un **afflux de demandes d'information** de la part des professionnels souhaitant s'approprier ce nouveau cadre qui ont identifié la CNIL comme une source d'information de référence.

Témoin de cette mobilisation croissante des professionnels et particuliers sur la protection des données, le site de la CNIL a cumulé plus de **8,1 millions de visites** depuis un an.

Ce que dit la présidente de la Cnil (La Tribune)

LA TRIBUNE

ECONOMIE BOURSE ENTREPRISES & FINANCE HI-TECH VOS FINANCES IDÉES MÉTROPOLES CARRIÈRES

CAC 40 5 385,46 PTS +0,50%

+ FORTES HAUSSES CAC 40		+ FORTES BAISSES CAC 40					
STMICROELECTRONICS	+4,16%	ENGIE	-5,31%	DOW JONES	+0,69%	Or	+0,06%
ARCELORMITTAL REG	+3,65%	MICHELIN	-1,99%	NASDAQ 100	+1,03%	OAT 10 ans	+8,51%
				FTSE 100	+0,25%	Pétrole Brent	+6,50%

Technos & Medias > Internet

RGPD : « La Cnil sera plus ferme envers les entreprises » annonce sa présidente Marie-Laure Denis

Par Sylvain Rolland | 15/04/2019, 15:34 | 2232 mots

Quelles sont vos priorités de contrôle pour 2019 ?

Le premier axe est le respect de tous les droits des individus comme le droit de rectification, d'opposition, d'oubli, le déréférencement, etc. Le deuxième est le contrôle des sous-traitants, tous secteurs confondus, qui doivent aussi être conformes, même s'ils n'ont pas affaire au consommateur final, en travaillant notamment avec les têtes de réseau dans chaque secteur. Le troisième axe est la protection des droits des mineurs sur Internet, sur les réseaux sociaux, notamment. Enfin, je souhaite que la Cnil exploite davantage les plaintes des concitoyens pour y répondre au plus vite, tout en sachant que 20% des plaintes reçues font l'objet d'une coopération européenne.

Il y a en a pour tout le monde….

UNIONTRAD COMPANY : 20 000 EUROS D'AMENDE POUR VIDÉOSURVEILLANCE EXCESSIVE DES SALARIÉS

La formation restreinte de la CNIL a prononcé une sanction de 20 000 euros à l'encontre de la …

18 juin 2019

SERGIC : SANCTION DE 400 000€ POUR ATTEINTE À LA SÉCURITÉ DES DONNÉES ET NON-RESPECT DES DURÉES DE CONSERVATION

La formation restreinte de la CNIL a prononcé une sanction de 400 000 euros à l'encontre de la …

06 juin 2019

racine
AVOCATS

PARTIE 2

Le pack RGPD

Beaucoup de membres Eben… sont des sous-traitants…

Définition du RPGD

> « Sous-traitant », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

Vison de la Cnil

Sont notamment concernés par le règlement européen :

- les prestataires de services informatiques (hébergement, maintenance,...), les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données,

IN

- les agences de marketing ou de communication qui traitent des données personnelles pour le compte de clients et
- plus généralement, tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme.
- Un organisme public ou une association peut également être amené à recevoir une telle qualification.

Ne sont pas concernés, dans la mesure où ils n'ont pas accès et ne traitent pas de données à caractère personnel, les éditeurs de logiciels ou les fabricants de matériels (badgeuse, matériel biométrique, matériel médical).

OUT

Le problème n°1 – Conformité obligatoire

Article 28

Sous-traitant

1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Le problème n°2 – Le contrat imposé

a) Traitement des données sur instruction documentée du responsable de traitement

b) Obligation de confidentialité des personnes qui « traitent » les données

c) Respecte les exigences de sécurité du règlement

d) Définition des règles de sous-traitance du sous-traitant

Encadrement par un contrat ou autre acte juridique liant le sous-traitant au responsable de traitement

e) Aide le responsable de traitement pour donner suite aux demandes d'exercice des droits des personnes concernées

f) Aide le responsable de traitement à assumer ses obligations de sécurité (sécurité + notification + communication)

g) Suppression ou renvoi des données au responsable de traitement au terme de la prestation (sauf si le droit de l'UE ou de l'Etat membre exige la conservation des données)

h) Mise à disposition du responsable de traitement des informations nécessaires pour apporter la preuve du respect de ses obligations et permettre la réalisation d'audits

Le problème n°3 – La sous-traitance ultérieure…

2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

4. Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

Les « outils » à votre disposition

Fiche d'implémentation Ajoutez votre nom et + si affinité

1. « Politique RGPD membre Eben » – Vous et vos clients Art. 28
2. « Politique RGPD sous-traitance ultérieure » – entre vous et vos propres prestataires
3. « Code de conduite – Confidentialité et sécurité des données de nos clients »)

Notre engagement RGPD

Quand vous êtes « responsable de traitement »

Conseil et légendes urbaines… (registre du sous-traitant obligatoire)

Fiche pratique

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.

250

5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Liste des livrables

racine
AVOCATS

PARTIE 3

Le DPO Kesako

Le rôle du DPO

Article 39

Informer et conseiller

- sur les obligations du responsable du traitement et du sous-traitant découlant du règlement;
- sur demande, en ce qui concerne l'analyse d'impact

Contrôler

- La mise en œuvre et l'application des règles internes, des procédures et des politiques en matière de protection des données
- la mise en œuvre de la bonne application du règlement tels que les principes de protection by design / by default

Vérifier

- la réalisation de l'analyse d'impact
- les réponses aux demandes de l'autorité de contrôle et des personnes concernées

Exercer

- la fonction de point de contact pour l'autorité de contrôle et les personnes concernées.

Veiller

- à la bonne tenue du registre des traitements.

Désignation obligatoire ou pas ?

Section 4

Délégué à la protection des données

Article 37

Désignation du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Pourquoi désigner un DPO quand on est pas obligé ?

1. On traite ou sous-traite des données sensibles (ex on travail pour des clients dans le domaine de la santé) // Exception

2. On veut rassurer le client sur la maîtrise du RGPD en qualité de sous-traitants

3. On veut vérifier l'application du Pack … ou tout simplement l'appliquer

4. On veut être assisté en cas de besoin (client)

5. On veut être assisté en cas de problème (faille)

Qui est le DPO ?

Désignation

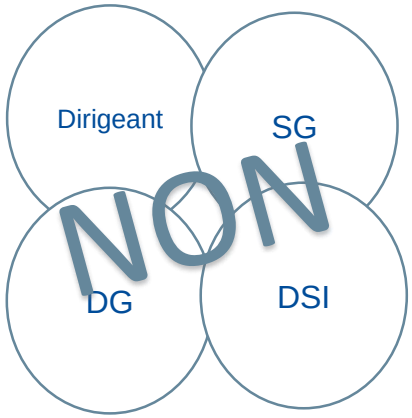
- Indépendamment du type de données traitées

Choix du délégué

- Sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données, de droit administratif et des procédures de l'organisation
- Un agent ou un prestataire externe

Publication des coordonnées

- Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle



L’offre eben = DPO mutualisé

Article 37-3

« Lorsque le responsable de traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille »

- **24 5 00 organismes ont désigné un délégué à la protection des données** (personnes physiques ou morales) ; ce qui représente 13 000 DPO contre 5 000 CIL (correspondants informatique et libertés) avant le RGPD ;

On fait = Conformité RGPD dans le cadre du Pack

On ne fait pas = des demandes sur mesures ou particulières (PIA, violation, …)

Pourquoi pas vous ?

146 membres eben sont abonnés au Pack juridique

+

L'offre DPO eben est incluse dans le pack

+

14 profitent du DPO mutualisé + la fédération (9,58%)

=

Cherchez l'erreur

Et pourtant … retour d’expérience

Merci de votre attention