Ethique de la Donnée & de la Sécurité

agora calycé

INNOVATIVE DIGITAL SERVICES

Mise en place du RGPD : 4 mois plus tard, quels retours d'expérience?

> Atelier CIENTICA, 27 septembre 2018

CCI ALSACE EUROMÉTROPOLE

Agenda

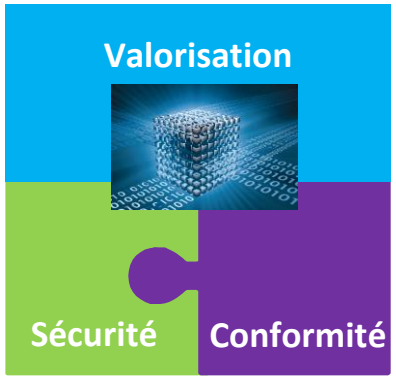
Introduction

Fondamentaux RGPD, mise en pratique et retour d'expérience

Focus sécurité des données

Témoignage Client – Agora Calycé

EDOS > Ethique de la Donnée et de la Sécurité



> Accompagnement des organisations sur 3 domaines d'activité

> **Conformité** & bonnes pratiques – **Sécurité** SI – **Transformation** Numérique

> Equipe pluridisciplinaire

> **Juridique**, **technique**, gestion de projet, accompagnement

> Approche « sur mesure »

> Adaptée à l'organisation, au métier, au besoin

Agenda

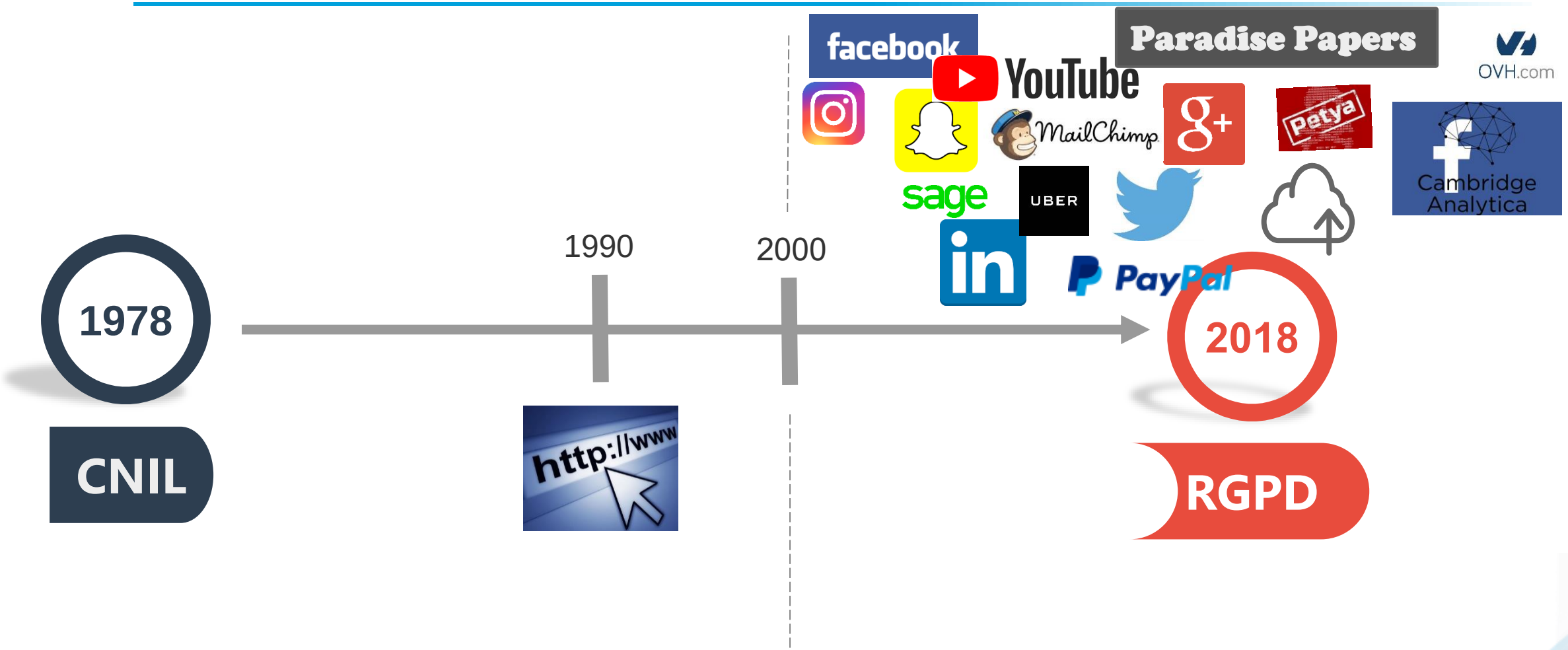
Introduction

Fondamentaux RGPD, mise en pratique et retour d'expérience

Focus sécurité des données

Témoignage Client – Agora Calycé

Bienvenue dans le Dataworld



Le RGPD ou GDPR : de quoi s'agit-il ?

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

> Le Règlement Général sur la Protection des Données (ou General Data Protection Regulation, « GDPR » en anglais)

REGLEMENT EUROPEEN N°2016/679 du 27 avril 2016

> Constitue le nouveau texte de référence européen en matière de protection des données à caractère personnel avec un double objectif :

- > Renforcer la protection des données pour les individus
- > Sécuriser les données de manière collective

ENTRÉ EN APPLICATION LE 25 MAI 2018

Une réforme substantielle

> des « formalités préalables » à un « principe général de responsabilité »

> Abandon des formalités « CNIL » ⇔ **Principe de responsabilité et de transparence** à la charge de tout organisme.

> Vers un principe **d'ACCOUNTABILITY** :

- > Prise en compte de la protection des données par défaut (PRIVACY BY DESIGN) ;
- > Mise en place d'une organisation, de mesures et d'outils internes garantissant une protection optimale des personnes dont les données sont traitées.

> Un principe de **minimisation des données :**

- > Le principe de minimisation des données, selon le RGPD, consiste à ne collecter et traiter que les données « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Quelques définitions

> Qu'est-ce qu'une donnée à caractère personnel ?

> « **toute information se rapportant à une personne physique identifiée ou identifiable** » (article 4.1 du Règlement).

> Une personne peut être identifiée :

> **Directement** (exemple : nom, prénom).

> **Indirectement** (ex : par un numéro client, de téléphone, identité psychique, économique ou encore par la voix).

> Qu'est-ce qu'un traitement de données personnelles ?

> Un traitement de données est « **toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel** » (article 4.2 du Règlement).

> Cela vise également les traitements « papier » de données (tenue d'un fichier client ou fournisseur, collecte).

> Un fichier de coordonnées d'entreprises ou d'emails génériques (contact@compagnie.fr) n'est pas un traitement de données personnelles.

Un monde de données

FINANCES

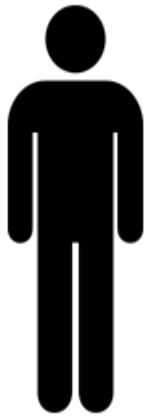
Revenus
Niveau d'imposition
(prélèvement à la source)

RELATIONS

Réseaux sociaux (groupes, intérêts, « j'aime », durée d'inactivité etc.)
Liens (amis, famille, collègues etc.)

IDENTITE

Identifiants (Nom, Email, pseudo, Adresse IP etc.)
Biométrie (Age, Sexe, ADN, empruntes digitales etc.)



SANTE

Soins, Traitements
Arrêts maladie,
Allergies
etc.

CONTENUS

Médias (Photos, vidéos etc.)
Conversation (SMS, appels, discussions sur les réseaux sociaux, mails etc.)

COMPORTEMENT

Navigation sur internet
(fichiers de logs)

CONTEXTE

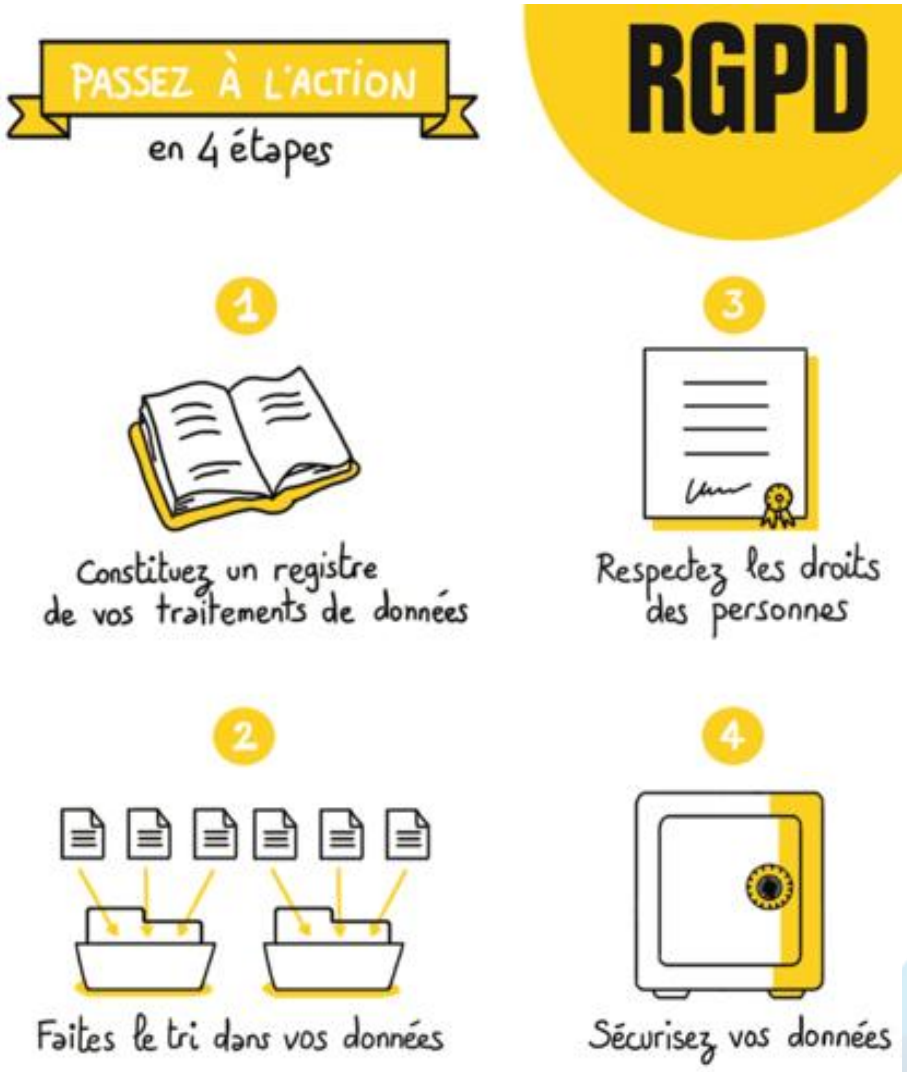
Géolocalisation,
Itinéraires etc.

Application du RGPD > un socle minimum indispensable

> **Recommandations CNIL/BPI France** applicables à toute entité qui traite des données personnelles.

> Défini un **minimum requis**, notamment pour les TPE/PME.

> Mais selon le métier et l'organisation, la mise en conformité **peut nécessiter d'aller bien au-delà**.



Cartographie > Le registre des activités de traitement

> Le RGPD impose, pour tous les organismes, **la tenue d'un registre des activités de traitement**.

> Chaque traitement de données devra être renseigné dans le registre.

> **150 000 téléchargements du modèle de registre simplifié de la CNIL** effectués au 25 sept.

> Pilotage, accompagnement **méthodologique** et **capitalisation** sont importants

> Nécessite une implication de **plusieurs acteurs** de l'organisation

Description du traitement			
Nom/Dénomination du traitement			
N° / REF du registre	Ref-000		
Date d'ajout du traitement dans le registre			
Date des mises à jour			
Date de clôture du traitement			

Acteurs	Adresse	Numéro de téléphone
Responsable du traitement - Service interne en charge du traitement		
Responsable(s) conjoint(s)		
Délégué à la protection des données (DPO)		

Finalité(s) du traitement effectué		
Finalité principale 1		
Finalité principale 2		
Sous-finalité 1		
Sous-finalité 2		
Sous-finalité 3		

Licéité du traitement		Commentaires
Base(s) légale(s) du traitement		

Mesures de sécurité		Précisions
Mesures de sécurité techniques		

Droit des personnes > les obligations d'information

> Le RGPD **renforce l'obligation d'information** lors de toute collecte de données, qu'elle soit directe ou indirecte, papier ou électronique (article 13 et 14 du RGPD).

> **L'obligation d'information consiste à communiquer à la personne concernée les informations limitativement énoncées par l'article 13 du RGPD** (par exemple, la finalité de la collecte, la base juridique du traitement, la durée de conservation des données, les destinataires des données personnelles, les modalités pour exercer le droit d'accès, etc.).

> L'information peut être délivrée selon **plusieurs moyens** :

- Charte de confidentialité ;
- Clause « Données personnelles » dans les CGV/CGA et contrats ;
- Mention sur les formulaires (papier/en ligne).

Droit des personnes > l'exercice des droits

> Le **droit d'accès** : « La personne concernée a le droit **d'obtenir** du responsable du traitement **la confirmation** que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, **l'accès auxdites données à caractère personnel** » (et autres informations).

> Le **droit d'opposition** : « La personne concernée a le droit de **s'opposer à tout moment**, pour **des raisons tenant à sa situation particulière**, à un traitement des données à caractère personnel la concernant (…) ».

En pratique, sur les 4 premiers mois, nous remarquons qu'il n'y a finalement **qu'une faible sollicitations de la part de tiers pour exercer leurs droits** (salariés, clients, fournisseurs).

Focus > Les relations avec les partenaires et sous-traitants

- **Identifier les rôles de chaque acteur** : responsable de traitement, sous-traitant et destinataire.
- **Encadrer les partenariats et la sous-traitance**.
- En effet, l'article 28 du RGPD prévoit que le sous-traitant et le responsable de traitement doivent **signer un contrat** qui doit prévoir, au minimum, que le sous-traitant :
  - Traite uniquement les données personnelles sur instruction documentée du responsable de traitement ;
  - Prend toutes les mesures requises aux fins de sécurité le traitement ;
  - Ne recrute pas un autre sous-traitant sans l'autorité écrite préalable, spécifique ou générale, du responsable de traitement ;
  - (…).

Les actions de la CNIL

- **Explosion des plaintes** : 3 767 plaintes reçues entre le 25 mai et le 25 sept. contre 2 294 plaintes sur la même période en 2017 (**+64%**).
- **Différents outils** mis à la disposition des organismes par la CNIL :
  - Un guide de sensibilisation au RGPD pour les petites et moyennes entreprises ;
  - Modèles de registre des activités de traitement (Excel/Word) ;
  - Exemples de mentions d'information ;
  - Des guides et un logiciel pour réaliser les analyses d'impact relatives à la protection des données ;
  - Les packs sectoriels : logement social, assurance, véhicule connecté, silver economie etc. ;
  - Formulaire de notification des violations de données personnelles.
- De nouveaux outils **à venir** : adoption de référentiels (gestion clients/prospects), d'un « règlement-type » sur la biométrie, de packs de conformité, de codes de conduite et de fiches pratiques.
- La **publicité des sanctions/mises en demeure** (communiqué de presse).

CNIL > Médiatisation des sanctions

- **OPTICAL CENTER** :
  - **sanction de 250 000 euros** pour atteinte à la sécurité des données de ses clients sur son site internet (juin 2018) ;
- **Association pour le Développement des Foyers (ADEF)** :
  - **sanction de 75 000 euros** pour atteinte à la sécurité des données des demandeurs de logements (juin 2018) ;
- **FIDZUP** et **TEEMO** :
  - **mise en demeure** pour absence de consentement des personnes concernées pour le traitement de leurs données de géolocalisation à des fins de ciblage publicitaire (juillet 2018) ;
- **Institut des techniques informatiques et commerciales (ITIC)** :
  - **mise en demeure** de cette école privée pour vidéosurveillance excessive (juillet 2018) ;
- **OPH de Rennes** :
  - **sanction de 30 000 euros** pour utilisation du fichier des locataires incompatible avec la finalité initiale (juillet 2018) ;
- **DAILYMOTION** :
  - **sanction de 50 000 euros** pour atteinte à la sécurité des données des utilisateurs (août 2018) ;
- **Assistance Centre d'appels :**
  - **Sanction de 10 000 euros** pour mise en œuvre illégale d'un système biométrique afin de contrôler les horaires des salariés (Sept. 2018).

Focus > Le Délégué à la Protection des données (Data Protection Officer)

> En dehors des cas de désignation obligatoire, **désigner un DPO est fortement encouragé** par la CNIL et ses homologues européens.

> Pas de transfert « automatique » de CIL à la fonction de DPO.

> Véritable **chef d'orchestre** de la conformité, le DPO doit être doté de :

  > **Qualités professionnelles** spécifiques (techniques, juridiques et gestion **de** projet) ;

  > Connaissances **expertes** en droit des données personnelles et des **pratiques** (référentiel métier).

> **Indépendance** du DPO et absence de conflit d'intérêts avec ses autres missions.

> Le DPO peut être interne, ou externalisé (personne morale).

Selon la CNIL, **24 500 organismes ont désigné un DPO**,
ce qui représente 13 000 DPO contre 5 000 CIL avant le RGPD.

Constat : Beaucoup de nos clients nomment un DPO, même lorsque ce n'est pas obligatoire.

RGPD > Où en sont les organismes 5 mois après?

> La plupart des organismes (Direction générale, responsable) **sont sensibilisés au RGPD** et **ont amorcé leur mise en conformité**.

> Les actions réalisées **en priorité** par nos clients sont les suivantes :

- > **Sensibilisation des collaborateurs** sur le RGPD/Sécurité ;
- > Rédaction du **registre** des activités de traitements ;
- > Apposition des **mentions** d'information/Rédaction d'une **charte** de confidentialité ;
- > Révision des **contrats** avec leurs sous-traitants.

> Pour certains, **crainte** que la mise en conformité au RGPD **ait un impact business négatif sur l'entreprise** (exemple : nettoyage des bases de données, exercice du droit d'opposition par un client).

RGPD > Où en sont les organismes 5 mois après?

> Quelques vécus

- > On a du retard mais (toujours) pas de budget »;
- > « On est dans les clous… (dixit notre service juridique) »;
- > « On attend (toujours) le support de notre maison mère »;
- > « Nos concurrents et partenaires ne semblent pas bouger, il est urgent d'attendre… »;
- > « …Encore une réforme trop coûteuse. Pas vus, pas pris… ».

Selon une étude réalisée par l'institut Talend (juin-septembre 2018) sur 103 entreprises européennes:

- **70% n'ont pas pu répondre aux demandes d'accès** aux données personnelles et de portabilité dans le délai imparti d'un mois à compter de la réception de la demande;
- Seulement 35% des entreprises européennes **(24% pour la France)** interrogées ont pu fournir les données souhaitées.

> Néanmoins, le phénomène « tache d'huile » produit sont effet en B2B.

Agenda

Introduction

Fondamentaux RGPD, mise en pratique et retour d'expérience

Focus sécurité des données

Témoignage Client – Agora Calycé

La protection des données personnelles

General Data Protection Regulation

> Obligation introduite par le Règlement Européen (RGPD)
  > Les données personnelles (salariés, clients, fournisseurs, partenaires) font l'objet d'une **obligation renforcée de sécurité**
> **Collecter**, **Stocker** et **Transporter** les données de manière sécurisée
> Limiter les accès au « **besoin d'en connaitre** »
> Appliquer le principe de « **privilège minimum** »
  > Définir la matrice d'habilitation
  > Appliquer un gestion stricte des comptes d'accès
> Respecter les **finalités** des données collectées, la **durée de conservation**
> **Minimisez** les risques
  > **Détruire** les données inutiles (informatique & papier)
  > **Anonymiser** les données conservées à des fin de statistique

Selon la CNIL, plus de **600 notifications de violations** de données ont été reçues, concernant environ 15 millions de personnes – soit environ 7 par jour depuis le 25 mai 2018.

Comment mettre en place la sécurité des données ?

> Afin de garantir votre organisme contre les risques de cyberattaque, il convient de mettre en place des mesures **techniques** (firewall, mot de passe sécurisé, chiffrement des données, etc.), **organisationnelles** (sensibilisation, formation du personnel) et **physiques** de sécurité.

> Afin **d'évaluer** le niveau de sécurité de votre entreprise, vous pouvez notamment vous poser les questions suivantes :

- Les comptes utilisateurs de vos employés et de vos clients sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux sites sont-ils sécurisés (verrou, digicode, etc.) ?
- Les personnes ayant accès aux données sont-elles bien accréditées ?
- Une procédure de sauvegarde et de récupération des données en cas d'incident a-t-elle été mise en place ?

Quelques bonnes pratiques de sécurité

> *« Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. A ce titre, dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des SI à travers des actions de sensibilisation et de formation » -* Guide d'hygiène informatique de l'ANSSI.

> Exemples de mesures :

- Rédiger une charte numérique ;
- Chiffrer les données avant leur envoi à d'autres organismes ;
- Réaliser une revue annuelle des habilitations ;
- Prévoir une procédure de verrouillage automatique de session ;
- Utiliser des antivirus régulièrement mis à jour ;
- Définir une politique pour les mots de passe ;
- Installer sans délai les mises à jour ;
- Etre informé sur les techniques de hameçonnage (phishing) – Ingénierie sociale;
- …

Pour conclure

Attention aux arnaques !

- La **CNIL** et la direction générale de la concurrence, de la consommation et de la répression des fraudes (**DGCCFR**) mettent en garde les professionnels souhaitant faire appel à une société pour se mettre en conformité au RGPD.
- Certaines sociétés se prétendent mandatées par les pouvoirs publics et proposent **parfois des prestations non suffisantes comme un simple échange ou l'envoi d'une documentation**.
- Certification/logo **« CNIL RGPD » : en cours de refonte** par la CNIL,
- De nombreux organismes situés notamment en **Alsace** ont reçu ce type de courrier/courriel/fax.

MISE EN CONFORMITE - RAPPEL

Numéro de dossier :
Date : 27/06/2018
Objet : Mise en conformité RGPD

Madame, Monsieur,

Nous vous rappelons qu'à compter du 25 mai 2018, les entreprises qui n'auront pas régularisé leur situat
nouveau règlement RGPD 2016/679 sur la protection des données, quelle que soit leur activité ou taille,
de sanctions pénales et financières pouvant s'élever jusqu'à 4% du Chiffre d'Affaire annuel de la société.

Vous êtes invités à vous mettre en conformité sans délai.

Le Pôle administratif RGPD a mis en place un service d'assistance téléphonique centralisé, intégralement
circonstance, disponible du lundi au vendredi de 09h00 à 12h30 et de 14h00 à 18h30 au :

09.71.07.22.40
(prix d'un appel local)

Si vous avez déjà effectué votre rapport RGPD, merci de ne pas tenir compte de ce rappel.

Pôle Administratif RGPD
Le directeur régional

RAPPEL DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions pénales
(Chapitre VIII, article 83, alinea 5)
Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000
chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions civiles
(Chapitre VIII, article 79 alinea 1)

CONFORMITE RGPD

Conformité RGPD
Règlement Général sur la Protection des Données
Région : Alsace

Tel : 09 77 19 55 60

MISE EN CONFORMITÉ

Eléments d'identification :
Objet : Mise en conformité
Réf : 36/MB/86-61
Dossier suivi par : M. Pasquier
Région : Alsace
Date : Le 14/06/18

Madame, Monsieur,

Votre entreprise ne semble pas avoir engagé la procédure de mise en conformité du RGPD.

Le Règlement Général de Protection des Données est entré en vigueur le 25 Mai 2018. Vous devez régler les frais de mise en conformité afin d'être à jour vis a vis de la Loi 2016/679 du 27 Avril 2016

Nous vous invitons à régler ce jour votre mise en conformité pour suspendre toute sanction financière et administrative.

- Par téléphone : 09 77 19 55 60
- Du Lundi au Jeudi de 9h00 à 17h00 et le Vendredi de 9h00 à 12h00

Notre bureau de traitement des dossiers a mis en place une assistance téléphonique afin de vous accompagner dans la démarche de mise en conformité.

Rappel à la loi :
Le règlement général sur la protection des données (RGPD) est le nouveau cadre juridique de l'union européenne qui gouverne la collecte et le traitement des données à caractère personnel des utilisateurs. Il est entré en vigueur le 25 mai 2018. Il s'applique à toutes les entités implantées dans un pays européen qui traitent des données à caractère personnel, ainsi qu'à toutes les entités à travers le monde qui traitent des données à caractère personnel appartenant à des résidents de l'UE.

Informations importantes :

Tout établissement non conforme est passible de sanctions financières ou administratives pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires.

P/O le Référent Technique RGPD

Les travaux sur les premiers référentiels ont déjà débuté. Une certification de Délégués à la Protection des Données est ainsi en cours d'élaboration : des organismes de certification agréés par la CNIL délivreront des certifications de DPO, sur la base d'un référentiel rédigé par la CNIL. Parallèlement, des travaux sont menés en matière de certification de formation RGPD avec le COFRAC.

Contacter EDOS

Jérôme BARON

Directeur Général
Consultant Cyber Sécurité

jbaron@edos.fr

+33 6 77 85 98 55