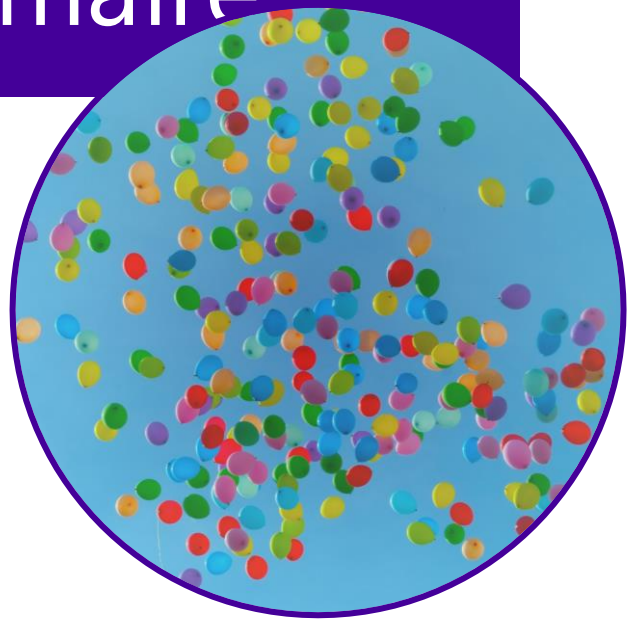
RGPD : règlement général sur la protection des données

INAE janvier 2019

Raymond Allonas
rallonas@passerellesetcompetences.org

Passerelles et Compétences

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

Contexte (1/3) : Evolution technologique

- La révolution des technologies « Informatique » et « Télécommunications » rend « universel » l'usage du numérique.
- Nos usages (Internet, Smartphones, etc..) multiplient nos « traces numériques personnelles »
- La croissance exponentielle des capacités de calcul, de transports et de stockages de données rendent possible l'exploitation efficace de bases de données gigantesques.
- Les organisations et les échanges sont de plus en plus « numérisés » *(« informatisés »)*

Passerelles et Compétences

Contexte (2/3) : Exploitation et diffusion des données

- Les données personnelles sont de plus en plus exploitées par des grandes organisations mondiales ou régionales
  - Publicité
  - Profilage
  - Commerce en ligne
  - …

- Les moyens de diffusion extrêmement rapides des informations augmentent les risques liés à la détention de données personnelles confidentielles. Le cyberharcèlement en est un exemple.

Passerelles et Compétences

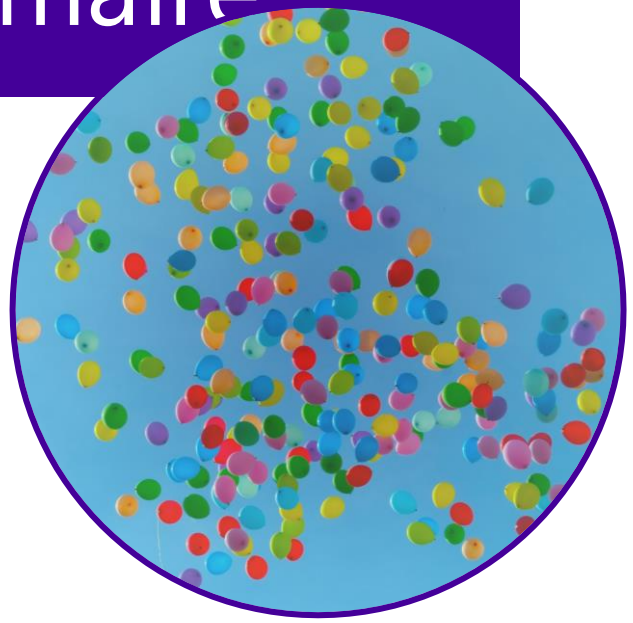
Contexte (3/3) : Conséquences

- Nécessité de responsabiliser les acteurs
  - Ceux qui exploitent les données à grande échelle
  - Ceux qui gèrent des données personnelles
    - Et, en particulier, ceux qui gèrent des données sensibles

- Nécessité de donner aux personnes la maitrise de l'usage de leurs données personnelles

Passerelles et Compétences

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

Principes du RGPD (1/3)

- Règlement **européen** : s'applique de façon « uniforme » et immédiate sur tout le territoire de l'Union Européenne (pas de distorsion de concurrence)
- Est concernée toute organisation publique ou privée qui traite des données personnelles, pour son compte ou non dès lors :
  - Qu'elle est établie sur le territoire de l'UE
  - Que son activité cible directement des résidents européens
- Pour la France, refonte de la loi de 1978 sur la CNIL (commission nationale informatique et liberté)➔ 80% des obligations du RGPD étaient déjà en vigueur
- De nouveaux droits aux personnes
- De nouvelles obligations aux organisations

Passerelles et Compétences

Principes du RGPD (2/3) : Droit des personnes

1. Droit à l'information : quelles données collectées et à quelles fins?
2. Droit d'accès aux données
3. Droit de rectification
4. Droit d'opposition
5. Droit à l'oubli (nouveau) : effacement des données
6. Droit à la limitation du traitement (nouveau)
7. Droit à la portabilité des données (nouveau)

- Interprétation : droit à un traitement « correct et loyal » des données.
- CNIL : interlocuteur unique en cas de litige avec l'organisation

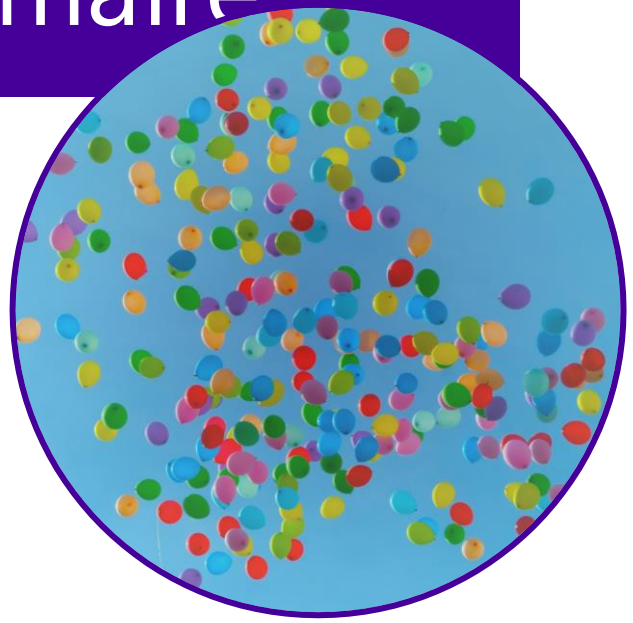
Passerelles et Compétences

Principes du RGPD (3/3) : Obligation des organisations

- Elles sont en regard du droit des personnes
- Il n'y a plus de déclarations préalables à faire à la CNIL
- L'organisation doit :
  - Respecter les obligations du règlement
  - **MONTRER** qu'elle a mis en place les mesures techniques ou organisationnelles appropriées
- L'organisation doit être en mesure de répondre aux demandes des personnes relatives à leurs droits sur leurs données personnelles.
- Toutes les données personnelles sont concernées, y compris celles au format papier
- Obligation de déclarer à la CNIL les incidents de sécurité
- La CNIL agit sur plainte ou dénonciation
- Le RGPD ne s'applique pas à une personne physique dans le cadre d'une activité strictement personnelle ou domestique

Passerelles et Compétences

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

Données personnelles (1/4) : identifiants

- Identifiants
  - Nom/prénom adresse
  - Numéros d'identification (Sécurité sociale, numéro fiscal)
  - Adresse mail
  - Adresse IP
  - Identifiant en ligne
  - Données biométriques
  - …

Passerelles et Compétences

Données personnelles (2/4) : données sensibles

- Données sensibles
  - Données concernant la santé ou la sexualité
  - Opinions politiques, philosophiques ou religieuses
  - Appartenance syndicale
  - Origines « ethniques » ou raciales
  - Données « judiciaires » : condamnations, infractions (ex : infractions routières, amendes…)
  - Données génétiques ou biométriques

  - Zones libres (ex commentaires sur situation personnelle)

  - Attention particulière aux données portant sur des mineurs ou des personnes vulnérables

Passerelles et Compétences

Données personnelles (3/4) : autres données

- Autres données
  - adresse
  - Couleur des yeux
  - Date d'entrée dans l'organisation
  - Poste occupé
  - Historiques de commandes
  - Historiques de navigations
  - Historiques de demandes
  - .....

Passerelles et Compétences

Données personnelles (4/4) : Principe de minimisation

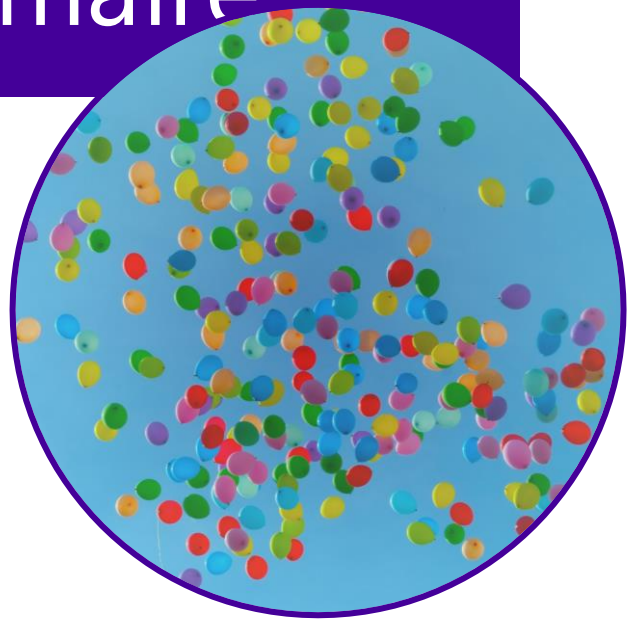
NOUVEAU et FONDAMENTAL

- Les données personnelles stockées dans l'organisation doivent être
  - Adéquates et pertinentes
  - Limitées à ce qui est nécessaire à la finalité des traitements
  - A durée de vie limitée (conforme à la finalité des traitements)
  - Accessibles aux seules personnes habilitées

- Ne pas recueillir/stocker des informations « au cas où on pourrait en avoir besoin un jour »
- Eviter absolument de recueillir/stocker des informations sensibles ou identifiantes non nécessaires

Passerelles et Compétences

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

Traitement de données personnelles (1/2) : définition

- Toute opération portant sur des données personnelles
  - Enregistrement d'un adhérent
  - Livraison d'une commande
  - Collecte de données via un questionnaire
  - Suivi de navigation…

- Le degré d'automatisation n'a pas d'incidence sur le fait que ce soit un traitement de données personnelles

- Il s'agit bien de données personnelles et non de données d'entreprise : l'enregistrement d'un fournisseur (société) n'est pas un traitement personnel

Passerelles et Compétences

Traitement de données personnelles (2/2) : traitements sensibles

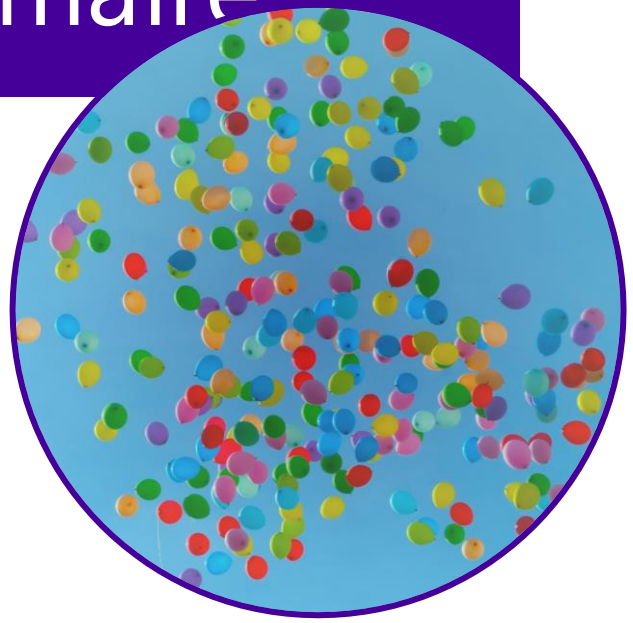
- Traitement à grande échelle de données personnelles

- Traitement de données sensibles ou portant sur des personnes vulnérables

Remarque :

- Sont aussi à prendre en compte les transmissions de fichiers avec des données sensibles à d'autres organisations ou à l'intérieur de l'organisation. Ces traitements ne font pas partie, au sens strict, des traitements sensibles mais doivent, surtout quand ils sont faits de façon électronique, répondre à des impératifs de sécurité (protocoles de transmissions sécurisés (ftps…), fichiers cryptés, fichiers protégés par mots de passe..)

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

Mise en conformité : préambule

Si les données personnelles ne sont pas au coeur de votre activité,
les moyens à déployer pour vous mettre en conformité au RGPD
ne seront pas très importants !
En effet, le critère à prendre en compte est le volume ou la sensibilité
des données traitées et non pas la taille ou le nombre d'employés
d'une entreprise.

Extrait du « guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises » (site de la CNIL)

Passerelles et Compétences

Mise en conformité , étude d'existant (1/4) : éléments à vérifier

1. Eléments à vérifier
   a) Référencer les données personnelles : quels sont les fichiers, avec quelles données, dans quels logiciels, sans oublier les fichiers bureautiques, la messagerie ou les fichiers papier. Vérifier la sensibilité (y compris zones de commentaires).
   b) Préciser les durées de conservation des données
   c) Facilité d'accès aux données (sur papier uniquement, accessibles sur un site web…)

   d) Référencer les traitements
   e) Vérifier les procédures (qui a accès à quoi? départ d'une personne)

   a) Vérifier la conformité des sous-traitants au RGPD

Si nécessaire, il existe des fiches de description des traitements sur le site de la CNIL

Passerelles et Compétences

Mise en conformité , étude d'existant (2/4) : évaluation

Evaluation

Il sera nécessaire de faire une analyse de risques s'il existe dans l'organisation des traitements (« sensibles ») répondant à au moins deux des éléments suivants :

a) Collecte de données sensibles (santé, données économiques, sociales ou judiciaires…)
b) Personnes vulnérables (malades, personnes âgées, mineurs, etc…)
c) Décision automatique avec effet légal ou équivalent
d) Exclusion du bénéfice d'un droit ou d'un contrat
e) Evaluation/scoring (profilage…)
f) Croisement de données
g) Collecte de données personnelles à grande échelle
h) Usage « innovant »

Passerelles et Compétences

Mise en conformité , étude d'existant (3/4) : évaluation suite

Nouveauté (novembre 2018) : liste de 24 traitements pour lesquels une analyse d'impact est obligatoire

Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes	- collecte de données sensibles - évaluation ou notation - personnes dites « vulnérables »	- traitement mis en œuvre par un établissement ou une association dans le cadre de la prise en charge de personnes en insertion ou réinsertion sociale et professionnelle ; - traitement mis en œuvre par les maisons départementales des personnes handicapées dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi de ces personnes ; - traitement mis en œuvre par un centre communal d'action sociale dans le cadre du suivi de personnes atteintes de pathologies chroniques invalidantes en situation de fragilité sociale.

Passerelles et Compétences

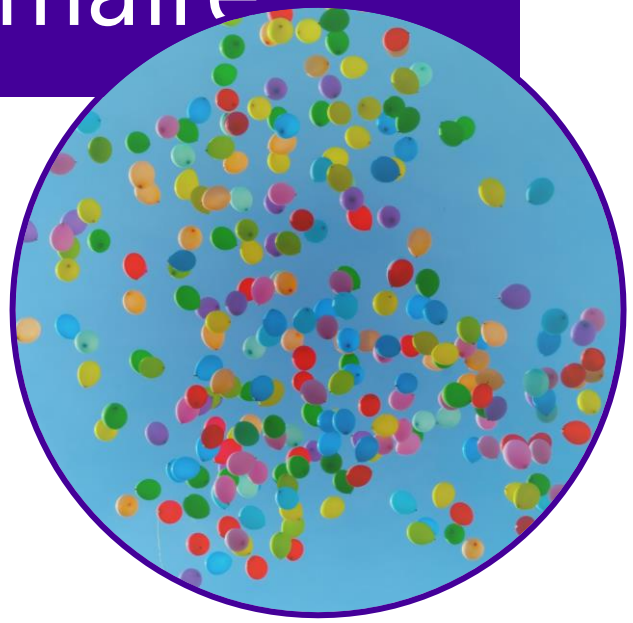
Mise en conformité , étude d'existant (4/4) : suite de l'étude

A l'issue de cette étude , 2 cas sont possibles

- L'association est « peu sensible » (pas ou guère de fichiers ou de traitements sensibles) ➔la démarche est presque finie.
- Dans le 2eme cas, nécessité de faire des « analyses d'impact » et, *éventuellement*, de nommer un « délégué à la protection des données » DPO (Date Protection Officer)

Passerelles et Compétences

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

Mise en conformité : Analyse d'impact (PIA : Privacy Impact Assessment) (1/2)

Cette analyse doit concerner tous les traitements sensibles de données personnelles référencées au cours de l'étude d'existant.

Elle comporte quatre phases :

1. Le contexte du traitement
   - L'objectif est « d'avoir une vision claire du traitement » , qui en est responsable? à quoi sert-il?
2. Les principes fondamentaux
   - Les données manipulées obéissent-elles aux obligations du RGPD? Minimisation, accord, durée de conservation …
3. L'étude des risques (voir slide suivant)
4. La validation du PIA par le responsable du traitement

Passerelles et Compétences

Mise en conformité : Analyse d'impact (PIA : Privacy Impact Assessment) (1/2)

L'analyse des risques se mesure suivant deux axes bien distincts.

Elle concerne les atteintes à la vie privée

Le niveau d'un risque se mesure en terme de gravité et de vraisemblance

a) **La gravité** présente l'ampleur d'un risque, l'estimation de l'ampleur du préjudice si le risque survient
b) **La vraisemblance** traduit la possibilité qu'un risque se réalise (évaluation des menaces) ; c'est à ce niveau que la sécurité est analysée

Une méthode pour réaliser un PIA est disponible sur

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Mise en conformité : Délégué à la protection des données (DPD ou DPO data protection Officer) (1/1)

Il n'y a pas d'obligation de nommer un DPD s'il n'y a pas de traitements à « grande échelle » de données personnelles et si l'organisme n'est pas une autorité ou un organisme public.

Le rôle du DPD :

- Informer et conseiller le responsable du traitement
- Contrôler le respect du règlement
- Conseiller sur les analyses d'impact (nécessité, évaluation)
- Coopérer avec la CNIL

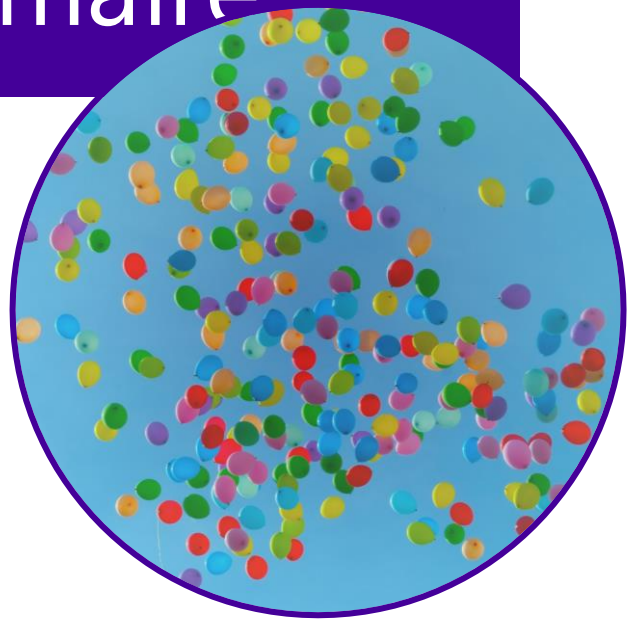
Le DPD n'est pas responsable de la conformité des traitements.

La nomination d'un DPD peut faciliter la démarche de mise en conformité.

Le DPD peut-être extérieur et partagé.

Passerelles et Compétences

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

Mise en conformité : fin de la démarche (1/2)

1. Etudier l'existant

2. Faire le tri des données
   a) Supprimer les données inutiles s'il y en a
   b) Définir précisément la durée de vie des données et purger les données trop anciennes

3. Faire évoluer les procédures
   a) Limiter les accès aux données
   b) Sensibiliser les « utilisateurs » du système

Passerelles et Compétences

Mise en conformité : fin de la démarche (2/2)

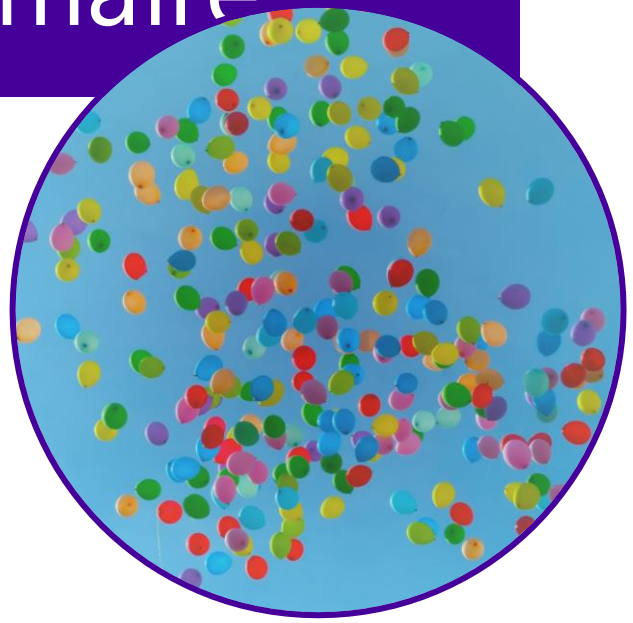
4. Respecter le droit des personnes
   a) Informer les personnes sur la collecte d'information et sa finalité
   b) Demander le consentement des personnes (cas des mineurs de moins de 15 ans➔ accord des parents)
   c) Mettre en place les procédures pour répondre aux demandes des personnes sur les accès aux données et autres droits

5. **Vérifier la sécurité Informatique** : sécurité d'accès, mots de passe, sauvegarde, hébergement (cas des sous-traitants) .

   L'obligation de « sécurité informatique » n'est pas une nouveauté!

Passerelles et Compétences

RGPD
Sommaire



1. Le contexte du RGPD
2. Les principes du RGPD
3. Données personnelles
4. Traitement de données personnelles
5. Mise en conformité
    1. Etude de l'existant
    2. Eléments supplémentaires
        1. Analyse des risques
        2. Délégué à la protection des données
    3. Fin de la démarche
6. Conclusion

Passerelles et Compétences

CONCLUSION(1/5)

- Il est **INDISPENSABLE** d'entamer une démarche de mise en conformité

  - D'une part, parce que le risque d'amende est très élevé (jusqu'à 10 millions d'Euros ou 2% du chiffre d'affaires mondial pour une entreprise)

  - Mais, surtout, car c'est de **NOTRE RESPONSABILITE** en tant qu'organisation

Passerelles et Compétences

CONCLUSION (2/5)

- La démarche à suivre doit être adaptée à la taille de l'association

A minima :

- Etudier l'existant
- Vérifier les pratiques de sécurité d'accès aux données (accès aux bureaux et aux classeurs, sauvegardes et sécurités informatiques (antivirus…))
- Préciser l'utilisation des données personnelles
- Officialiser la démarche (Conseil d'administration, présence à la formation…)

Il est conseillé de décrire plus finement certains traitements (enregistrement et maj des données personnelles de personnes vulnérables)

Passerelles et Compétences

CONCLUSION(3/5)

- L'association est responsable des données qu'elle héberge.
- Les moyens à mettre en œuvre pour la protection des données personnelles sont « proportionnels » aux moyens de l'association et à son objet.
- La mise en conformité est l'occasion d'améliorer les procédures

Passerelles et Compétences

CONCLUSION (4/5)

- Pour **Isabelle Falque-Perrotin**, Présidente de la CNIL
- *Il faut en finir avec l'alarmisme sur le RGPD ! Avec ce guide, nous voulons montrer aux PME que se mettre en conformité c'est **facile,** en adoptant simplement de bons réflexes. A l'heure où les consommateurs sont de plus en plus soucieux de leurs données personnelles, proposer une relation de confiance à ses collaborateurs, clients, prospects, c'est aussi **utile** à l'entreprise. Enfin, un couperet ne va pas tomber sur les entreprises le 26 mai.*

Passerelles et Compétences

CONCLUSION(5/5)

- **QUEL PLAN D'ACTION?**
  - **Le définir s'il n'existe pas déjà.**

Passerelles et Compétences

Bibliographie

- Comment gérer dans mon entreprise la protection des données personnelles (éditions Francis Lefebvre)
- Le site de la CNIL et notamment le « Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises »
- https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement
- www.cnil.fr
- https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Passerelles et Compétences