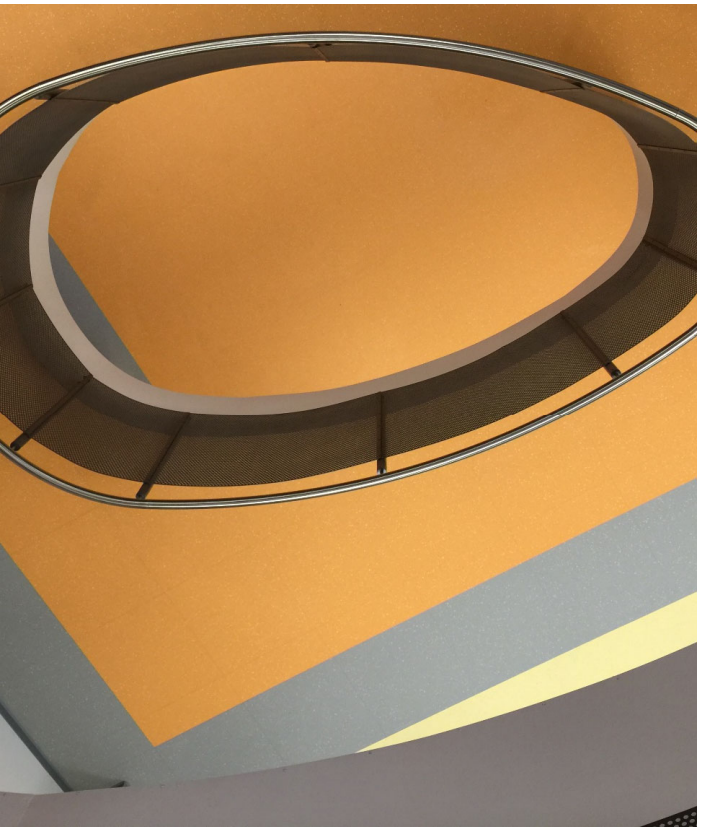


GDPR

(GENERAL DATA PROTECTION REGULATION)

JOURNÉE DES DIRECTEURS – LE MARDI, 16 JANVIER 2018
AU LYCÉE ALINE MAYRISCH

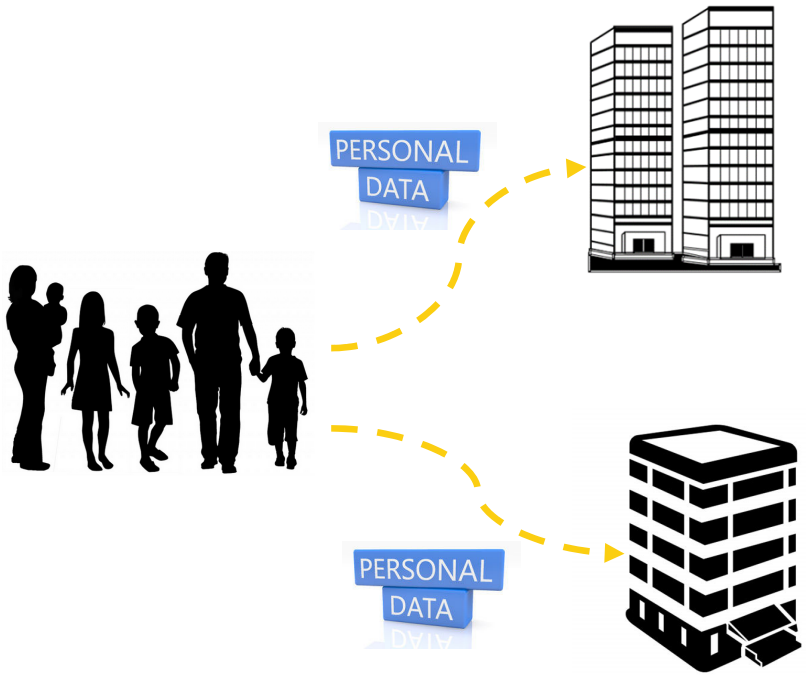
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse

Centre de gestion informatique
de l'éducation

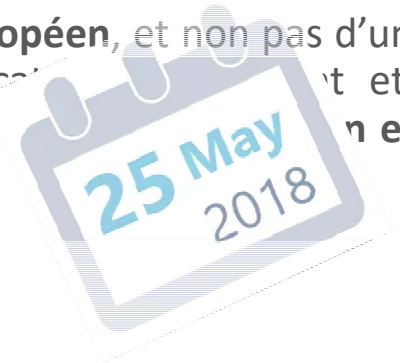
cgie centre de gestion informatique de l'éducation

TABLE DES MATIÈRES

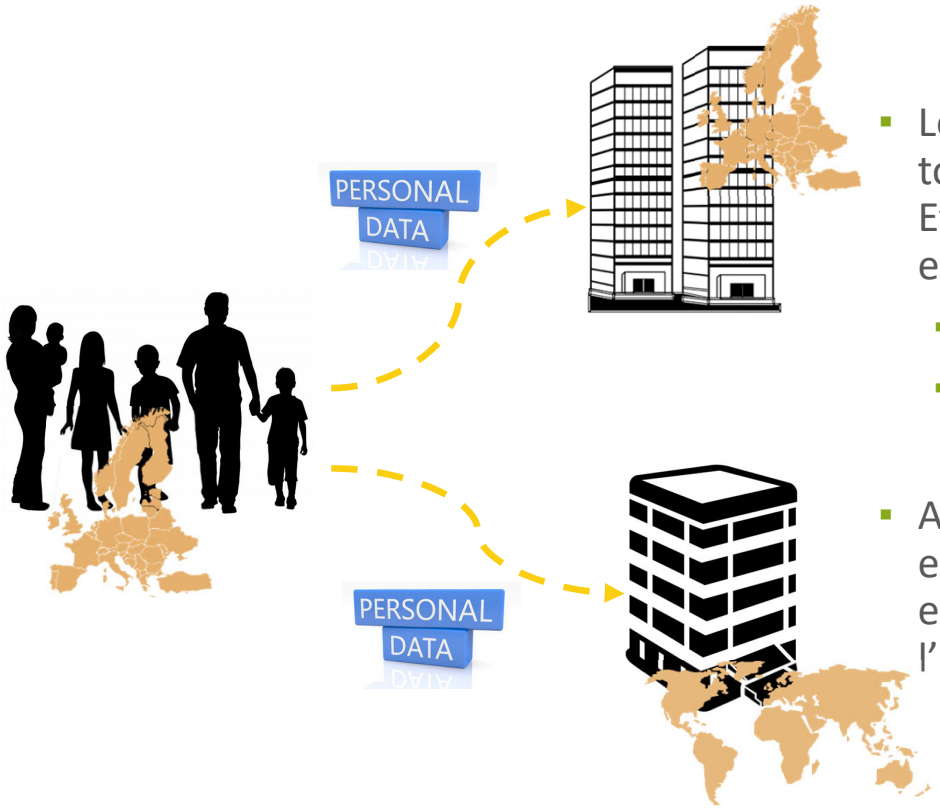
PRÉSENTATION DE LA GDPR – INTRODUCTION



- Le **GDPR** (**General Data Protection Regulation**) (RGPD - Règlement général sur la protection des données) est le nouveau règlement européen en matière **de protection des données à caractère personnel**.
- Il renforce et unifie la protection des données pour **les individus au sein de l'Union Européenne**.
- Il s'agit **d'un règlement européen**, et non pas d'une directive, le texte entrera en applic t et en même temps dans **tous les Etats n européenne**, sans transposition.

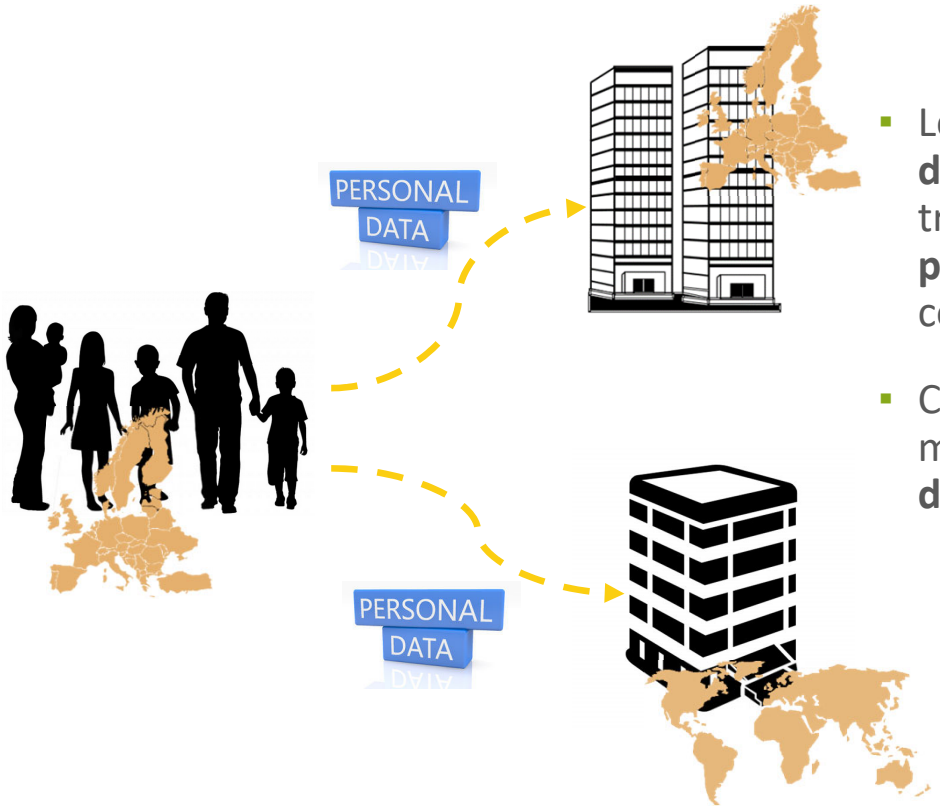


PRÉSENTATION DE LA GDPR – INTRODUCTION



- Les règles du GDPR s'appliqueront, à compter de mai 2018, à toutes les entreprises privées ou entités publiques des 28 Etats membres de l'Union européenne. Plus précisément, aux entreprises et entités:
  - Proposant **des biens et services** sur le marché de l'UE
  - **Collectant et traitant des données à caractère personnel sur les résidents de** l'UE.
- A noter que le règlement s'appliquera également aux entreprises non implantées en UE, dès lors qu'elles collectent et traitent des données personnelles sur des résidents de l'UE.

PRÉSENTATION DE LA GDPR – INTRODUCTION



- Le nouveau règlement met fin **aux obligations antérieures de déclaration** à la CNPD des traitements. Dorénavant, les traitements pourront être effectués **sans déclaration préalable** et l'autorité de contrôle CNPD pourra effectuer des contrôles à tout moment.
- Cette nouvelle disposition impose aux entités/entreprises de mettre en œuvre **un certain nombre de procédures et de documentations**, à démontrer en cas de contrôle.

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

cgi

PRÉSENTATION DE LA GDPR – DÉFINITIONS

- Les règles et obligations du GDPR s'appliquent au **traitement – automatisé ou non – des données à caractère personnel** (art. 2). L'objectif du GDPR est de renforcer l'encadrement des pratiques en matière de collecte et d'utilisation des données à caractère personnel.

- **Définition « données à caractère personnel »** (art. 4.1):
  - **toute information** se rapportant à **une personne physique identifiée ou identifiable** ». Par personne physique identifiable, il faut comprendre « une personne physique qui peut être identifiée, **directement ou indirectement**, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

PRÉSENTATION DE LA GDPR - DÉFINITIONS

- **Définition « Traitement de données » (**art. 4.2):
  - Le « traitement des données », au sens du GDPR, fait référence à **la collecte, à l'accès, au stockage, à la manipulation, à la destruction et à la consultation à distance des données**. Concrètement, une entreprise qui délègue à un prestataire la collecte et le stockage des données fait néanmoins du traitement de données dans la mesure où elle les consulte.

- **Définition « Responsable du traitement »** (art. 4.7):
  - Le « Responsable du traitement » est celui **qui prend l'initiative de (faire) collecter et tenir des données à caractère personnel**, dans le but de les traiter d'une manière ou d'une autre. Le Responsable **doit déterminer les finalités spécifiques** du traitement des données et **prouver que celui-ci repose sur une base légitime.** Il doit examiner au préalable quelles données à caractère personnel sont nécessaires à cet effet. Pour la législation, il est essentiel de ne pas collecter et traiter de données au-delà de celles qui sont strictement nécessaires pour atteindre l'objectif visé.

PRÉSENTATION DE LA GDPR – DÉFINITIONS

- **Définition « Sous-traitant »** (art. 4.8):
  - 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**. À noter que le GDPR impose également explicitement des obligations au sous-traitant. Ce n'est pas parce que vous collectez des données que vous êtes automatiquement le Responsable, mais, inversement, vous demeurez responsable en tant que donneur d'ordre, même si vous confiez la collecte des données à un sous-traitant. Pour cela, **un contrat** devra clairement indiquer quels sont **les rôles du donneur d'ordre et du preneur d'ordre** dans le traitement des données.

PRÉSENTATION DE LA GDPR – DÉFINITIONS

- **Définition « base légitime »** (art. 9):
  - Pour être licite, un traitement de données doit se fonder sur l'une **des six conditions** suivantes :
    1) Le consentement de la personne concernée (distinct pour chaque finalité). Le consentement doit être « libre, spécifique, éclairé et univoque », c'est-à-dire que la personne concernée doit avoir un véritable choix.
    2) un contrat
    3) une obligation légale (claire et précise)
    4) l'intérêt vital de la personne concernée ou d'une autre personne
    5) une mission d'intérêt public
    6) l'intérêt légitime du responsable de traitement (p. ex. à des fins de marketing, anti-fraude, traitement des données clients ou salariés, sécurité des traitements, etc.).

PRÉSENTATION DE LA GDPR – GRANDS PRINCIPES

- **Les grands principes de la GPDR (1)**
  - Principe de loyauté (art. 5.1.a):
    - les données personnelles doivent être traitées de manière loyale, licite et transparente. Obligation d'information renforcée et consentement des personnes nécessaire.
  - Principe de proportionnalité (art. 5.1.b):
    - les données personnelles ne peuvent être collectées que pour une finalité déterminée, explicite et légitime.
  - Principe de minimisation (art. 5.1.c):
    - seules les données strictement nécessaires seront collectées.
  - Principe de réactivité (art. 5.1.d):
    - les données personnelles conservées doivent être exactes, précises et actuelles. Ce qui nécessite donc de les tenir à jour.

PRÉSENTATION DE LA GDPR – GRANDS PRINCIPES

- **Les grands principes de la GPDR (2)**
  - Principe de conservation limitée (art. 5.1.e):
    - La durée de conservation doit être justifiée par la finalité du traitement. Les données qui ne sont plus utilisées doivent être supprimées.
  - Principe de sécurité (art. 5.1.f):
    - mise en place de dispositifs et procédures de sécurité, tant du côté du responsable du traitement que de ses sous-traitants.
  - Principe d'information (art. 13 – Art. 22):
    - les personnes dont les données personnelles ont été collectées disposent de droits spécifiques : accès à l'information, rectification, effacement, portabilité… Elles peuvent les faire valoir à tout moment.

PRÉSENTATION DE LA GDPR – DROITS DES PERSONNES

- **Les droits des personnes (1)**
  - Droit d'accès (art. 15):
    - Chaque personne concernée a le droit de savoir comment ses données personnelles **sont traitées et dans quel but**. Les entités/entreprises doivent donc donner aux personnes concernées davantage de contrôle sur leurs données privée. En cas de demande d'accès de la part d'un utilisateur, l'entreprise disposera **d'un délai d'un mois maximum** pour la satisfaire.
  - Consentement clair et explicite (art. 6,7,8):
    - Chaque personne doit donner son accord par un « **acte positif clair** ». Dans le cas de mineur âgé de **moins de 16 ans**, le consentement doit être recueilli **auprès du titulaire de l'autorité parentale**. Le consentement est un point central du nouveau règlement. Ce dernier impose d'obtenir **un consentement explicite à des finalités précises**.
  - Droit de rectification (art. 16):
    - La personne concernée a le droit d'obtenir du responsable du traitement, **dans les meilleurs délais**, la rectification des données à caractère personnel la contenant qui **sont inexactes**.

PRÉSENTATION DE LA GDPR – DROITS DES PERSONNES

- **Les droits des personnes (2)**
  - Droit à l'effacement (art. 17):
    - chaque personne a le droit d'obtenir **l'effacement de données** à caractère personnel la concernant, sauf si **les données sont nécessaire** (obligation légale, motifs d'intérêt public, domaine de la santé publique, fins archivistiques, fins juridiques). Les entités/entreprises disposeront d'un **délai réduit d'un mois**, pour supprimer les données à la suite d'une demande. Toutes **les copies et toutes les reproduction des données devront aussi être effacées**.
  - Portabilité des données (art. 20):
    - les personnes ont le droit **de recevoir et réutiliser** leurs données personnelles et **de les transmettre à un autre prestataire**, dans un **format structuré, lisible** par tous (par exemple en cas de changement de fournisseur).
  - Profilage et automatisation(art. 22):
    - toute personne a le droit de ne pas être soumise à une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative.

PRÉSENTATION DE LA GDPR – RESPONSABILITÉS

- **La responsabilité (accountability) (art. 24-30) (1)**
  - Le principe de l'« Accountability »(art. 24):
    - le responsable du traitement ou le sous-traitant doit mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.
  - Le principe du « Privacy By Design » (art. 25.1):
    - toutes les mesures techniques et organisationnelles doivent être mises en œuvre par le responsable du traitement et le sous-traitant, « **tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même** ».
  - Le principe du « Privacy by default » (art. 25.2):
    - le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées « **pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées** ». Ce principe s'applique non seulement à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, mais aussi à leur **durée de conservation et à leur accessibilité** (les données doivent n'être accessibles qu'aux personnes qui en ont strictement besoin en fonction de la finalité du traitement).

PRÉSENTATION DE LA GDPR – RESPONSABILITÉS

- **La responsabilité (accountability) (art. 24-39) (2)**
  - La désignation d'un **Délégué à la Protection des Données (DPO)** (art. 37):
    - un Délégué à la Protection des Données devra obligatoirement être désigné dans trois situations :
      1. Pour les traitements réalisés **par une autorité ou un organisme public** ;
      2. Pour les organismes ayant pour activité de base des opérations de traitement nécessitant le suivi **régulier et systématique des personnes à grande échelle** ;
      3. Pour les organismes ayant pour activité de base le traitement à grande échelle **de données dites « sensibles » ou relatives aux condamnations pénales et infractions**.
  - La notification des failles de sécurité (art. 33):
    - En cas de violation d'une donnée à caractère personnel, le responsable doit :
      1. **informer l'autorité de contrôle** compétente de la violation, dans un délai de **72 heures**. Cette notification doit indiquer le nom et les coordonnées du **DPO ou toute autre personne auprès de laquelle il sera possible d'obtenir des informations** ;
      2. **informer la personne concernée** de la violation des données à caractère personnel. Il s'agit donc d'être proactif car il n'est plus possible de régulariser a posteriori.

PRÉSENTATION DE LA GDPR – RESPONSABILITÉS

- **La responsabilité (accountability) (art. 24-39) (3)**
  - Le renforcement des mesures de sécurité (art. 32):
    - Les entités/entreprises sont responsables **de la sécurité** des données qu'elles traitent et doivent **mettre en place les mesures adéquates** pour la garantir (pseudonymisation des données, analyses d'impact, tests d'intrusion…).:
  - L'encadrement des sous-traitants (art. 28):
    - Les entreprises devront **choisir des sous-traitants présentant des garanties suffisantes**. En cas de faille de sécurité au niveau du sous-traitant, ce sera **l'entité/l'entreprise cliente** (= le responsable des traitements) qui sera tenue **pour responsable**. En conséquence, les entreprises devront **revoir les contrats signés avec les sous-traitants** en intégrant des clauses concernant les données à caractère personnel. Le GDPR instaure en fait un régime de co-responsabilité des sous-traitants.

PRÉSENTATION DE LA GDPR – RESPONSABILITÉS

- **La responsabilité (accountability) (art. 24-39) (4)**
  - Registre des activités de traitement (art. 30):
    - Il s'agit d'une nouveauté du règlement. Les entités/entreprises qui traitent des données personnelles sont obligées de tenir un registre des activités de traitement. Cette obligation s'applique aux grandes entreprises (qui emploient 250 personnes ou plus) et aux plus petites entreprises qui traitent régulièrement des données personnelles dans le cadre de leur activité.
    - Le registre doit mentionner toutes une série d'informations, comme le nom et les coordonnées du responsable du traitement, les finalités du traitement, les personnes concernées, les données concernées, les personnes à qui les données vont être transférées, les mesures de sécurité mises en place, etc.
    - Le registre peut se présenter sous une forme électronique.

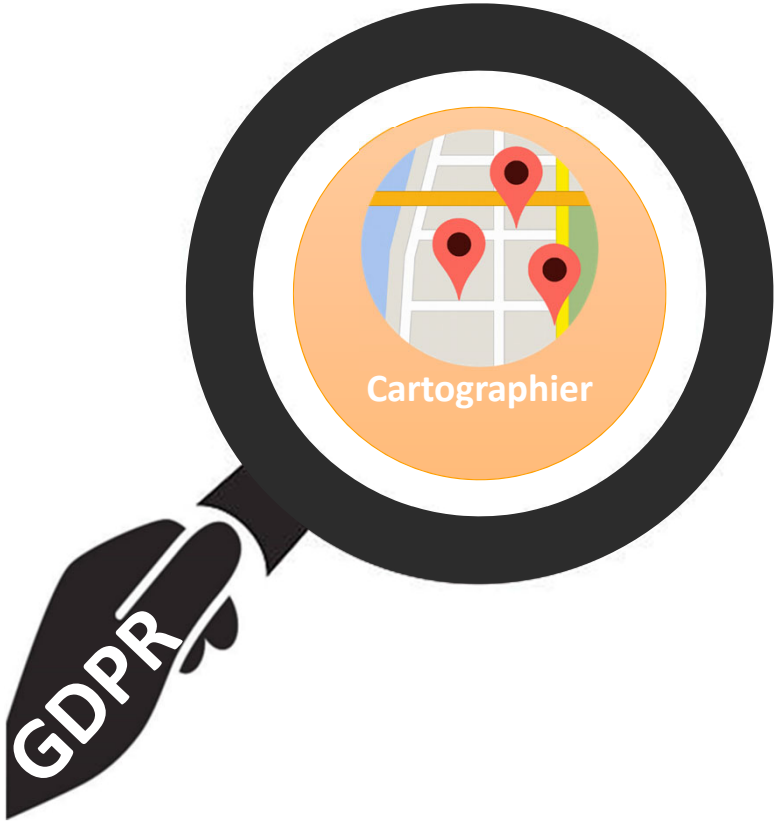
PRÉSENTATION DE LA GDPR – LES SANCTIONS

- **Les sanctions (art. 83.4 et art 83.5)**
  - Concernant les sanctions, deux seuils sont fixés en cas de non-conformité au règlement européen suivant la nature de l'infraction (l'article 79 du règlement détaille la liste des infractions pour chacun des seuils :
    - Un premier seuil à 2% du chiffre d'affaire mondial ou 10 millions d'euros (maximum des 2 valeurs) pour les infractions mineures : absence de registre des traitements, non nomination d'un DPO si elle est obligatoire ou encore non réalisation des analyses d'impact.
    - Un deuxième seuil à 4% du chiffre d'affaire mondial ou 20 millions d'euros (maximum des 2 valeurs) pour les infractions les plus graves : non recueil du consentement, non-respect des droits des personnes, transfert international illégal ou encore non-respect d'une interdiction de mise en œuvre d'un traitement.

PRÉSENTATION DE LA GDPR – COMMENT SE PRÉPARER

- **Se préparer en 6 étapes (CNIL)**
  1. Désigner un DPO
     - La désignation d'un délégué à la protection des données est obligatoire en 2018 si :
       - Vous êtes un organisme public ;
       - Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infraction.
     - Ce poste peut être occupé par un collaborateur ou confié à un prestataire externe (juriste).

PRÉSENTATION DE LA GDPR – COMMENT SE PRÉPARER

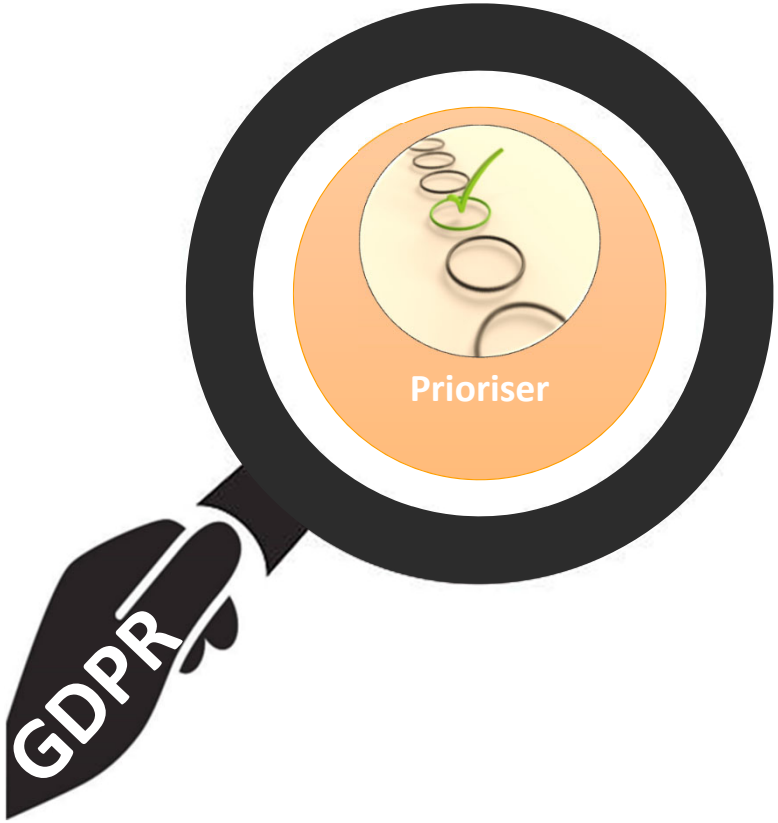


- **Se préparer en 6 étapes (CNIL)**

  2. Cartographier les traitements

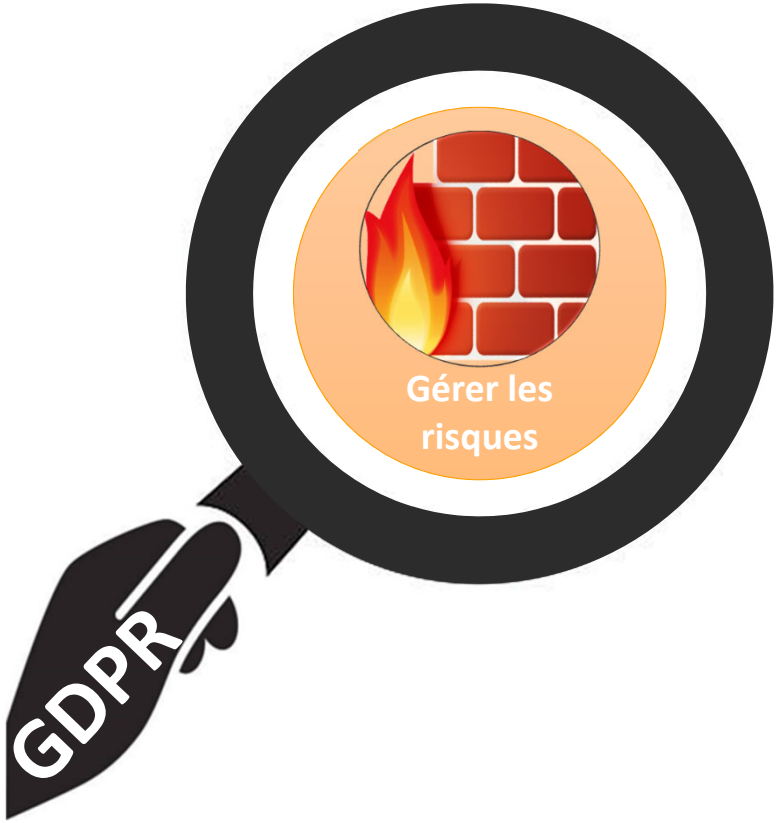
     - Dans le cadre du futur règlement, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales. Pour être en capacité de mesurer l'impact du règlement sur votre activité et de répondre à cette exigence, vous devez au préalable recenser précisément :
       - **Réaliser l'inventaire (DataReg)** de tous les traitements de données personnelles (catégories de données, leur but et la personne qui en est responsable).
       - **Évaluer et documenter vos pratiques** (gestion des réclamations et des plaintes, notification de violation de données, etc.)
       - **Identifier les risques potentiels** et prendre les mesures nécessaires à leur prévention. Plus les données sont sensibles, plus cet aspect est critique (ex: sécurisation des informations médicales ou sociales, etc.)
       - **Maintenir une documentation** assurant la traçabilité des mesures prises.

PRÉSENTATION DE LA GDPR – COMMENT SE PRÉPARER

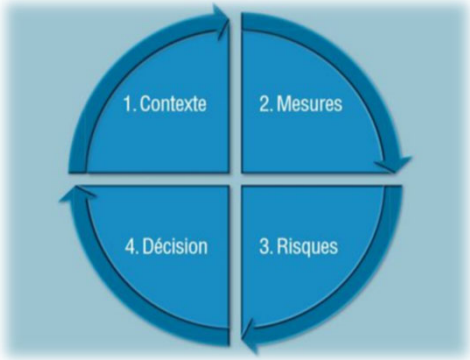


- **Se préparer en 6 étapes (CNIL)**
  3. Prioriser les actions à mener
     - Cette priorisation peut être menée au regard des risques que font peser vos traitements sur les libertés des personnes concernées. Certaines tâches seront faciles à mettre en œuvre et vous permettront de progresser rapidement:
       - Assurez-vous **que seules les données strictement nécessaires** à la poursuite de vos objectifs sont collectées et traitées.
       - **Identifiez la base juridique** sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
       - **Révisez vos mentions d'information** afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement)
       - **Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations** et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
       - **Prévoyez les modalités d'exercice des droits des personnes concernées** (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)
       - **Vérifiez les mesures de sécurité mises en place**.

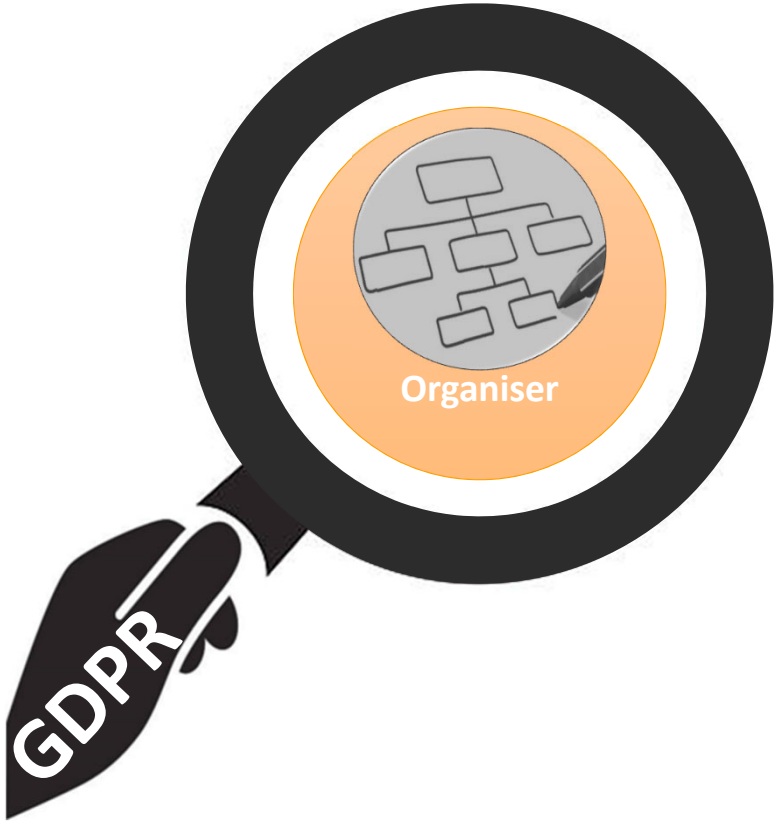
PRÉSENTATION DE LA GDPR – COMMENT SE PRÉPARER



- **Se préparer en 6 étapes (CNIL)**
  4. Gérer les risques:
     - Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (en anglais, Data protection impact assessment ou Privacy Impact Assessment).



PRÉSENTATION DE LA GDPR – COMMENT SE PRÉPARER

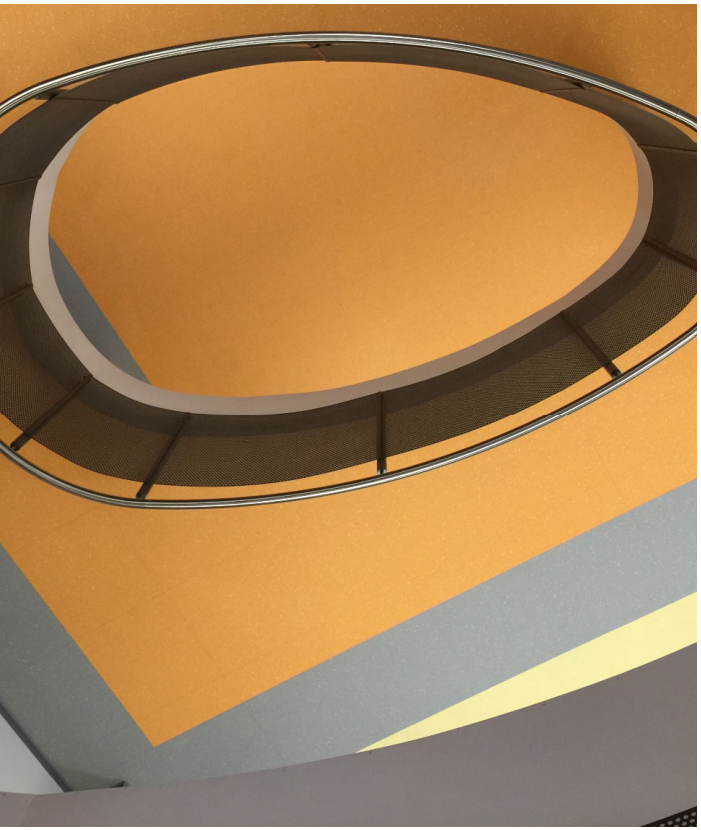


- **Se préparer en 6 étapes (CNIL)**

5. Organiser les processus internes:
   - Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

PRÉSENTATION DE LA GDPR – COMMENT SE PRÉPARER

- **Se préparer en 6 étapes (CNIL)**
  6. Documenter la conformité:
     - Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.



MERCI

GDPR.CGIE.LU
HELPDESK@CGIE.LU

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse

Centre de gestion informatique
de l'éducation