ACADÉMIE
DE POITIERS
Liberté
Égalité
Fraternité

Antony Barillot
Contact : dpd@ac-poitiers.fr
dpo@ac-poitiers.fr

Tous concernés

RGPD – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Règles et bonnes pratiques

Le Délégué à la Protection des Données

- **Missions du délégué à la protection des données :**
  - Veiller au respect du cadre légal
  - Alerter les responsables de traitement
  - Analyser, investiguer, auditer
  - S’assurer de l’existence d’une documentation relative aux traitements effectués
  - Assurer la médiation avec les personnes concernées
  - Accompagner et sensibiliser
  - Interagir avec l’autorité de contrôle (CNIL)

ACADÉMIE DE POITIERS
Liberté
Égalité
Fraternité

Tous concernés

Antony Barillot
Contact : dpd@ac-poitiers.fr
dpo@ac-poitiers.fr

RGPD – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Règles et bonnes pratiques

Contexte

RGPD : De quoi parle-t-on ?
- Définition d'une donnée à caractère personnel et d'un traitement
- Les droits des usagers
- Des acteurs
- Les obligations du responsable de traitement

Bonne pratique : Je respecte les 6 principes du RGPD

Outils de la société civile : Usage dans un cadre privé VS Usage dans un cadre professionnel

La sous-traitance et la sous-traitance ultérieure : Limiter les risques

Sécuriser les pratiques : Les bons réflexes

Quelques ressources

Antony Barillot
Contact : dpd@ac-poitiers.fr
dpo@ac-poitiers.fr

Règles et bonnes pratiques

pour une protection des données à caractère personnel au quotidien

Des projets impactant

https://ladigitale.dev/digiview/#/v/6399dca86a47e

https://ladigitale.dev/digiview/#/v/6399dc503298e

Contexte

Aujourd'hui la révolution numérique génère chaque jour avec les services en ligne, les réseaux sociaux, objets connectés, cloud … des milliards de données personnelles. Ce contexte d'explosion des données à caractère personnel impose des règles particulières afin de maîtriser l'impact sur les droits et libertés des personnes concernées.

Une adaptation profonde de la réglementation sur la protection des données a donc été nécessaire avec la mise en œuvre du RGPD* le 25 mai 2018.

*RGPD signifie : « Règlement Général sur la Protection des Données » ou en anglais «General Data Protection Regulation» (GDPR)

Contexte

Il en résulte :

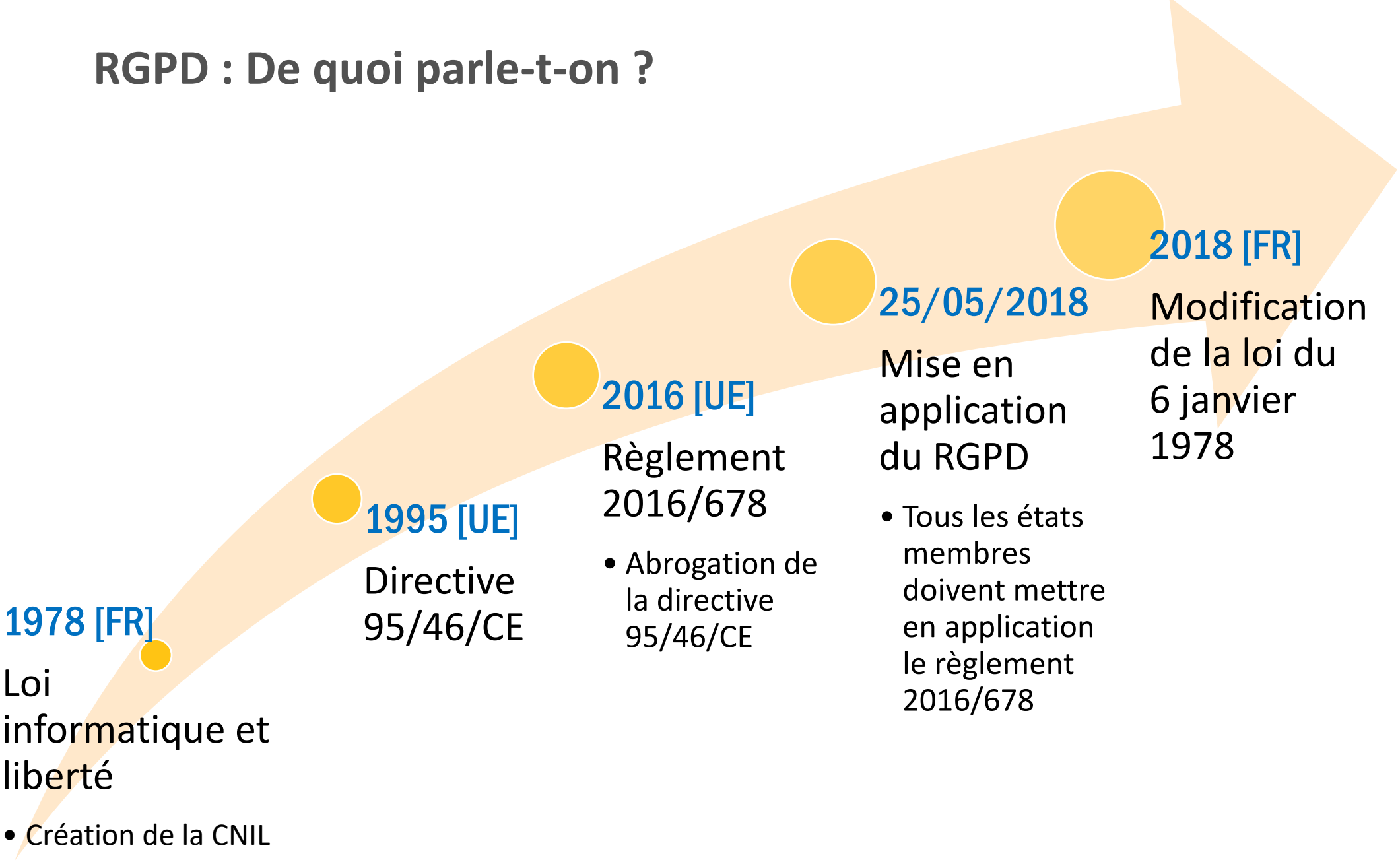
- Une harmonisation de la législation dans toute l'Europe
- Une protection des données renforcée
- Toute organisation établie sur le territoire de l'Union européenne ou dont l'activité cible directement des résidents européens doit obligatoirement respecter ce règlement.
- De nouveaux droits pour les personnes concernées

Des perspectives :

En accordant de nouveaux droits aux personnes et plus de sécurité pour leurs données, le Règlement européen renforce la confiance des personnes réticentes au digital.

Les entreprises/organisations ont ainsi plus de liberté d'innover (applications, services en ligne) et donc plus d'opportunités.

RGPD : De quoi parle-t-on ?



RGPD : De quoi parle-t-on ?

Illustration : CNIL (RGPD : de quoi parle-t-on ?)

RGPD : De quoi parle-t-on ?

RESPONSABILITE-TRANSPARENCE-CONFIANCE

Avant d'écrire mon nom sur le tableau, j'ai besoin de savoir comment vous envisagez d'utiliser ces données.

Définition d'une donnée à caractère personnel et d'un traitement

- **<u>Une donnée à caractère personnel</u>**

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

o État civil, identité, données d'identification, images : (ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)

o Données de localisation : (ex. déplacements, données GPS, GSM, …)

o Vie scolaire ou professionnelle : (ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)

o Informations d'ordre économique et financier : (ex. revenus, situation financière, données bancaires, etc.)

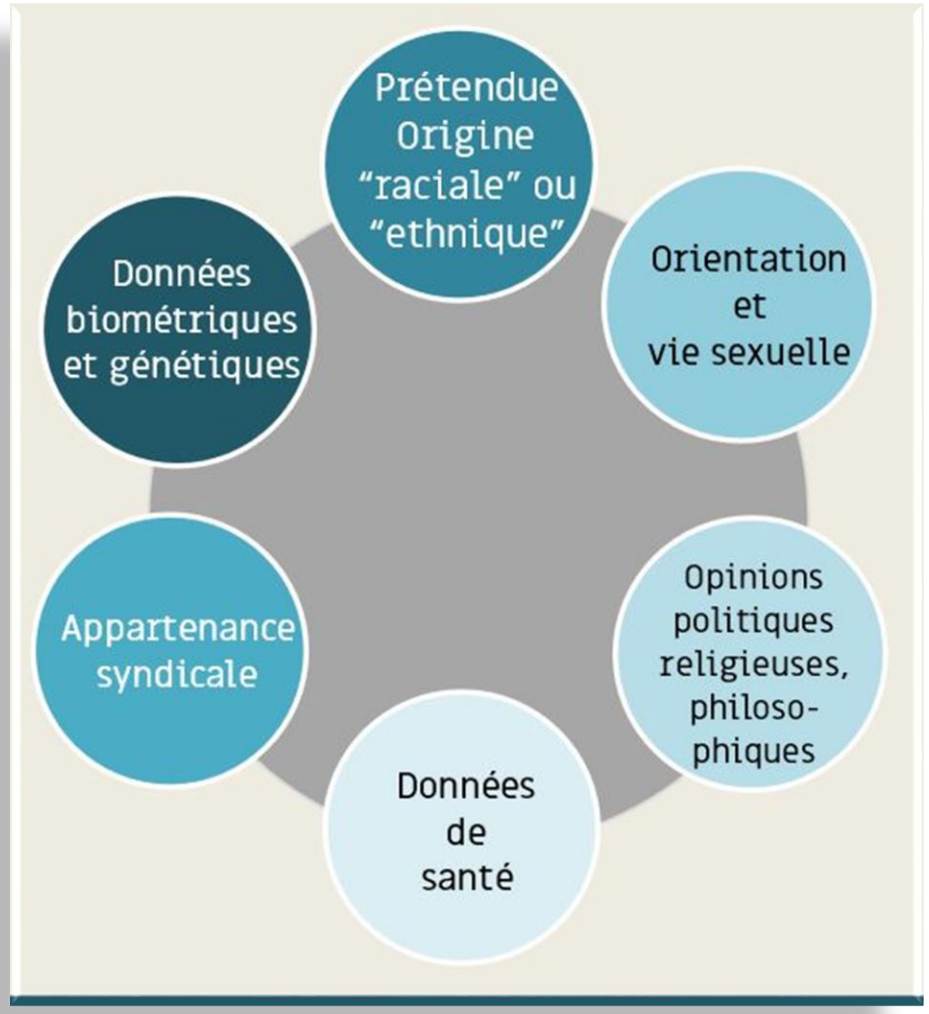
o Données de connexion : (ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

o Internet : (ex. cookies, traceurs, données de navigation, mesures d'audience …)

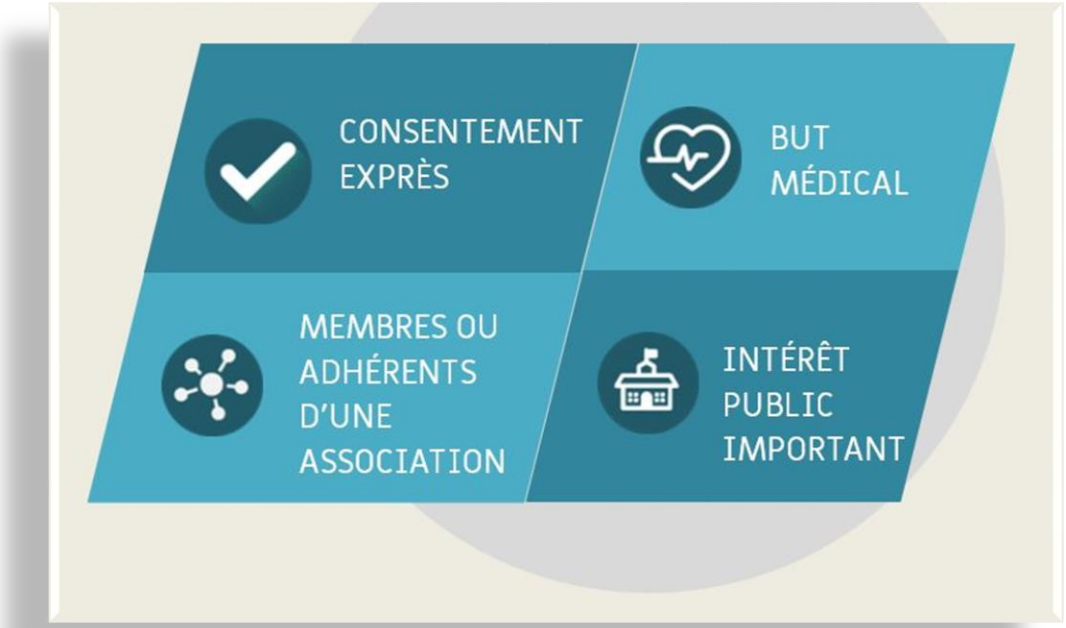
o Autres catégories de données : À préciser

Définition d'une donnée à caractère personnel et d'un traitement

Point de vigilance : Les données dites sensibles



Collecte interdite, excepté si une des conditions suivantes est remplie



Définition d'une donnée à caractère personnel et d'un traitement

- **<u>Un traitement de données</u>**

Toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé.

la consultation **la conservation** **l'extraction** **l'utilisation**

l'enregistrement **l'organisation** **la collecte** **le verrouillage**

la communication par transmission

l'adaptation pour la modification

le rapprochement ou l'interconnexion

la diffusion ou toute autre forme de mise à disposition

l'effacement ou la destruction

Définition d’une donnée à caractère personnel et d’un traitement

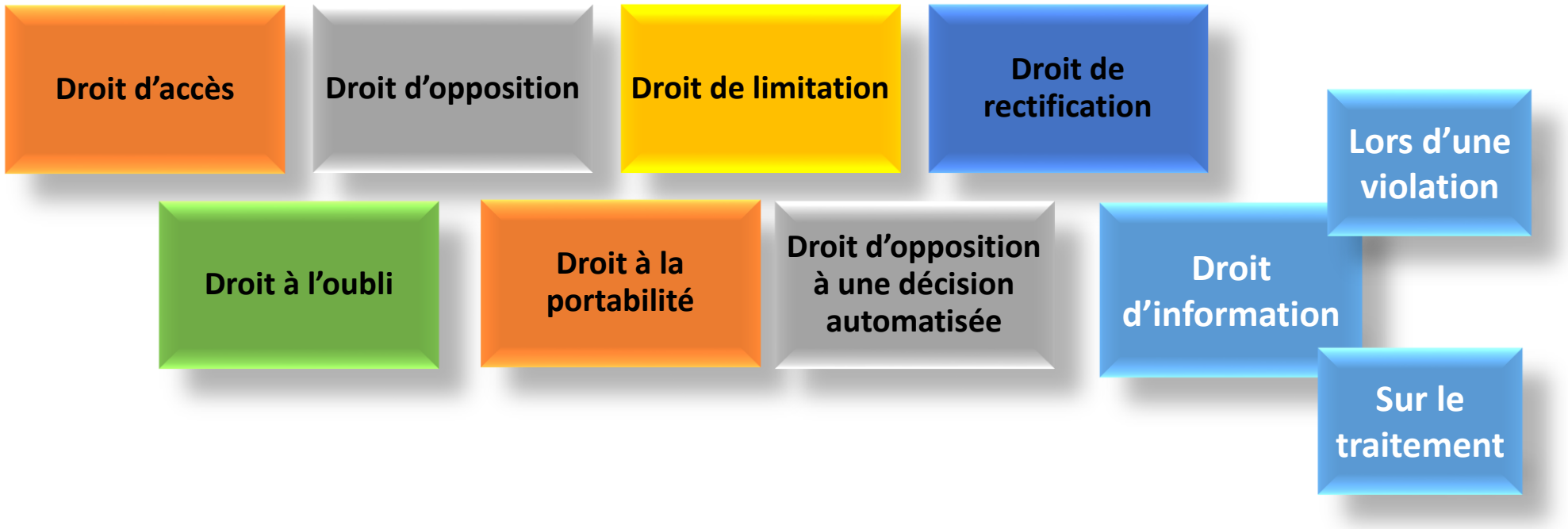
Sensibles ou non, toutes les données personnelles relèvent du RGPD !

Leurs traitements peuvent être autorisés, sous réserve que le traitement soit licite (Permis par la loi, conforme à la loi) et déclarer (Documentation de conformité).

Il convient donc de s’assurer que chaque manipulation de données à caractère personnel et toute solution/application numérique utilisée a fait l’objet d’une analyse / validation par le rectorat / la DSDEN / l’EPLE et a été déclarée au registre des traitements de la structure.

Le responsable de traitement de cette dernière étant juridiquement responsable de l’ensemble des traitements de données exécutés dans le cadre des missions qui lui incombent et qu’il a définies.

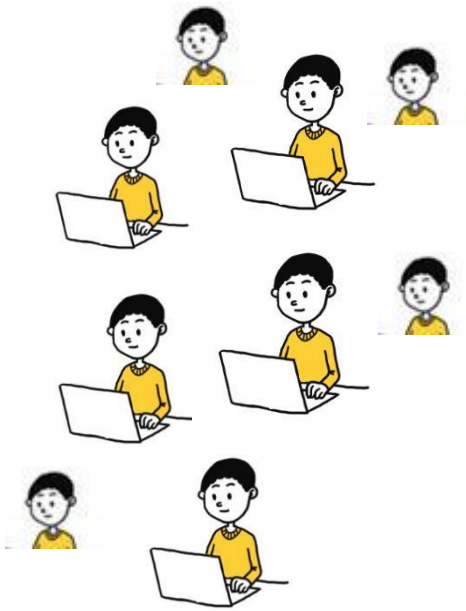
Les droits des usagers



Des acteurs

CNIL.

Tous acteurs de cette conformité



Les obligations du responsable de traitement

- Définir la finalité des traitements (base légale, licéité…) et tenir un registre
- Informer sur l'usage des DCP traitées et les droits associés
- Sécuriser les DCP et les traitements (procédures internes , contrats…)
- Contrôler les sous-traitants des traitements (Analyse d'impact…)
- Traiter les demandes des usagers (1 mois)
- Notifier les violations de DCP à la CNIL (72 heures)

Quelques questions sur le RGPD

Question N°1 : Selon vous, à quelles données s'applique le Règlement européen ?

A : Aux fichiers informatisés uniquement

B : Aux fichiers informatisés et aux fichiers papier

Quelques questions sur le RGPD

Question N° 3 : À qui le Règlement européen impose-t-il de nouvelles règles ?

A - Aux entreprises et aux organisations ?

B - Aux entreprises, aux organisations et à leurs sous-traitants ?

Quelques questions sur le RGPD

Question 4 : Le prestataire choisi est basé en dehors de l'Union Européenne, est-ce que le Règlement européen s'applique ?

A - Non, il s'applique seulement aux entreprises implantées dans l'UE

B - Oui, il s'applique, car les usagers sont européens

Bonne pratique : Je respecte les 6 principes du RGPD

- Licéité (Permis par la loi, conforme à la loi) : Ai-je le droit de traiter les données ? Quel est le cadre légal ?
- Finalité : Dans quel but je le fais ?
- Pertinence : De quoi ai-je besoin pour atteindre mon objectif ? (Minimisation de la collecte de données au strict nécessaire, données exactes et mises à jour)
- Conservation : Combien de temps ai-je le droit de conserver (DUC) ? Que dit le DUA , le service des archives du Rectorat et du Département ? Le sort final ?
- Sécurité et gestion des risques: Quelles sont les mesures de sécurité requises pour ce type de traitement ? Est-ce que je les applique ? Les risques pesant sur la vie privée des personnes concerné ont été identifiés ?
- Information (Transparence) et respect des droits : Ai-je informé les personnes sur le traitement et leurs droits ? Ai-je bien communiqué les coordonnées du DPD ?

Quelques questions sur le RGPD

Question 6 : : Je peux stocker tout type de données à caractère personnel dans les solutions proposées par l'académie ou mon établissement qui ont toutes les garanties de conformité au RGPD ?

A - Oui, quel que soit l’usage qui sera fait de cet outil numérique

B - Pour apporter une répondre, il est nécessaire de disposer de plus d’éléments sur le traitement envisagé.

Quelques questions sur le RGPD

Question 7 : Si j'utilise des pseudonymes pour identifier une personne le RGPD ne s'applique pas ?

A – Oui il s’applique, quel que soit l’usage qui sera fait des données et leurs natures.

B – Non il ne s’applique pas , car les pseudonymes ne sont pas les noms des personnes.

J’informe les personnes

Les personnes ont des droits sur leurs propres données.

AFCDP

Documenter la conformité:

Les mentions d’information…

Les Mentions

L’utilisation de Éducation est-elle sécurisée ?

Nos offres dédiées à l’éducation et aux secteurs scolaires sont conformes aux normes FERPA et COPPA. Nous sommes également signataire de l’accord américain de confidentialité des données. Nous sommes conformes aux normes RGPD, et nous proposons des contenus sûrs pour l'école.

Les Cookies


Plus de 500 partenaires
continuer sans accepter
← Sélectionner les partenaires pour
incluant son identité et le moyen de le contacter. Une fois votre paramétrage terminé, cliquez sur « Enregistrer mes choix ».
Tous les partenaires
#
1020, Inc. dba Placecast and Ericsson Emodo IAB TCF
1Agency IAB TCF
1plusX AG IAB TCF
2KDirect, Inc. (dba iPromote) IAB TCF
33Across IAB TCF
Enregistrer

Outils de la société civile : Usage dans un cadre privé VS Usage dans un cadre professionnel

1 - Le consentement dans le cas d'utilisation d'outils de la société civile :

- Dans un cadre privé: Chacun est libre d'utiliser ou non la solution en connaissance des conditions d'utilisation.
- Dans un cadre professionnel/scolaire, le consentement ne peut être la base légale retenue
  - Le consentement ne peut être libre dans le cadre d'une relation élève/enseignant, direction/personnel.
  - Des inégalités pourraient se créer.

Outils de la société civile : Usage dans un cadre privé VS Usage dans un cadre professionnel

2 - Les finalités et moyens du traitement mis en œuvre :

- Dans un cadre privé: Les finalités sont en lien avec l'intérêt légitime du prestataire/fournisseur de service.
- Dans un cadre professionnel/scolaire : Les finalités ne peuvent pas être celles du prestataire/fournisseur de service qui dans ce cadre est le sous-traitant du responsable de traitement.

Outils de la société civile : Usage dans un cadre privé VS Usage dans un cadre professionnel

/!\ Importance de la contractualisation avec ces prestataires pour :

- Avoir des garanties afin de maîtriser les données qui seront collectées pour une finalité spécifique nécessaire au Responsable de Traitement (en lien avec une mission de service public ne nécessitant pas le consentement…)
- Choisir le niveau de protection (Coût en conséquence)
- Choisir les lieux d'hébergement (UE…)
- Permettre de ne pas subir des modifications des conditions d'utilisation

Quelques questions sur le RGPD

Question 8 : DOODLE (choix de date…) WeTransfert (Transfert de fichier) ?

A - Usage compatible avec mon activité professionnelle

B - Usage non compatible avec mon activité professionnelle

Quelques questions sur le RGPD

Question 9 : Lorsque je mets à disposition de mon établissement / collègues, un tableau collaboratif stocké sur un espace personnel en ligne et recensant les noms des élèves d'une classe et leurs difficultés sociales ou familiales. Que dois-je faire ?

A - Avant toute mise en œuvre, le chef d'établissement(ou services DSDEN / Rectorat) doit être informé pour valider (vérifier si c'est légalement possible).

B - Pas de précautions particulières, car l'outil et l'espace de stockage ont été fournis par le service ou l'établissement.

Quelques questions sur le RGPD

Question 10 : Sur quoi repose la sécurité d'un traitement de données ?

A - Le sous-traitant (éditeur, intégrateur, hébergeur) avec qui un contrat a été passé
B - Les mesures techniques et organisationnelles mises en place par l'établissement (par exemple paramétrages applicatifs, procédures écrites et suivies, etc.)
C - L'usage des outils / de la solution / des données, par les utilisateurs

La sous-traitance et la sous-traitance ultérieure : Limiter les risques

Contrôler les sous-traitants des traitements

- Contractualisation obligatoire avec le ST apportant des garanties au RT.
- Avoir une vigilance concernant les contrats unidirectionnels / rapport de force non équilibré avec certains prestataires ou qui seraient les seules à détenir un outil répondant au besoin (logiciel de comptabilité …)
- Le sous-traitant (ST) est responsable des données qui lui sont confiées, car il doit traiter les données suivant les instructions du Responsable de Traitement (RT) (nouveau depuis la mise en œuvre du RGPD).
- L'adhésion à un Code de conduite peut être une garantie (en cours d'élaboration avec les entreprises de la EdTEch).

La sous-traitance et la sous-traitance ultérieure : Limiter les risques

Contrôler les sous-traitants des traitements

- Lors de la sélection d'un prestataire, la question de la réversibilité doit être posée (La question de la portabilité des données est importante, mais rarement possible).
- Les changements de sous-traitants ultérieurs doivent être portés à la connaissance du RT (RT doit être informé en temps utile pour valider ou changer de ST).
- Le sous-traitant doit faire preuve de transparence (cartographie / schéma des flux de données…)
- Le sous-traitant doit aider le responsable de traitement s'il souhaite (ou doit) mener une analyse d'impact.

La sous-traitance et la sous-traitance ultérieure : Limiter les risques

La sous-traitance et la sous-traitance ultérieure : Limiter les risques

L'hébergement des données :

Hors UE possible, mais avec des garanties :

- Le pays est adéquat (pas de mesures particulières)

- Le pays est non adéquat (close contractuelle obligatoire / règles d'entreprises contraignantes)
  - Ex : Le Privacy Shield (US) n'offre plus un niveau de garantie (invalidé depuis de mois de juillet 2020)

En UE :

- Vigilance concernant le statut du prestataire (Notamment ceux répondant à des lois de pays non européens)

Sécuriser les pratiques : Les bons réflexes

Sécuriser les pratiques : Les bons réflexes

1 - Un mot de passe fort :

Bon à savoir …

La taille et la complexité du mot de passe varient en fonction des mesures complémentaires mises en place pour fiabiliser le processus d'authentification
https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

Solution pour élever le niveau de sécurité :

L'authentification à facteurs multiples (multifacteurs) désigne une méthode de confirmation d'identité associant plus de 2 facteurs d'authentification. Ces facteurs peuvent être des informations connues par l'utilisateur (comme un mot de passe ou un code PIN), des éléments qu'il possède (tels qu'un token physique ou un smartphone, exemple de la clé OTP utilisé dans les établissements) ou une caractéristique qui lui est propre (comme une empreinte digitale).

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

2 – Le choix des outils/ressources en ligne :

- J'utilise les solutions préconisées par le Ministère de l'Éducation National, le Rectorat, ou mon établissement.

- Je propose a mon responsable de traitement de nouveaux outils/ressources :
  - ✓ En lisant attentivement les conditions d'utilisation
  - ✓ En préférant des solutions hébergées dans l'Union européenne
  - ✓ En vérifiant que les personnes concernées seront bien informées sur le traitement de leurs données
  - ✓ En vérifiant que les personnes concernées pourront exercer leurs droits

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

2 – Le choix des outils/ressources en ligne :

- Je propose a mon responsable de traitement de nouveaux outils/ressources :
  - ✓ En vérifiant l'interopérabilité avec les outils existants (ENT, outil de vie scolaire…)
  - ✓ En vérifiant que le prestataire envisagé se considère bien sous-traitant (contrat) et traitera les données uniquement dans le cadre de la finalité définie.
  - ✓ En rédigeant une fiche de traitement regroupant l'ensemble des éléments précédents et plus… (voir modèle type proposé par votre structure, le DPD / DPO)

/!\ La fiche de traitement doit permettre au responsable de traitement de prendre une décision éclairée pour la mise en œuvre, ou non, du traitement envisagé.

/!\ Le responsable de traitement associera en temps utile le Délégué à la protection des données afin qu'il puisse émettre un avis sur le traitement.

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

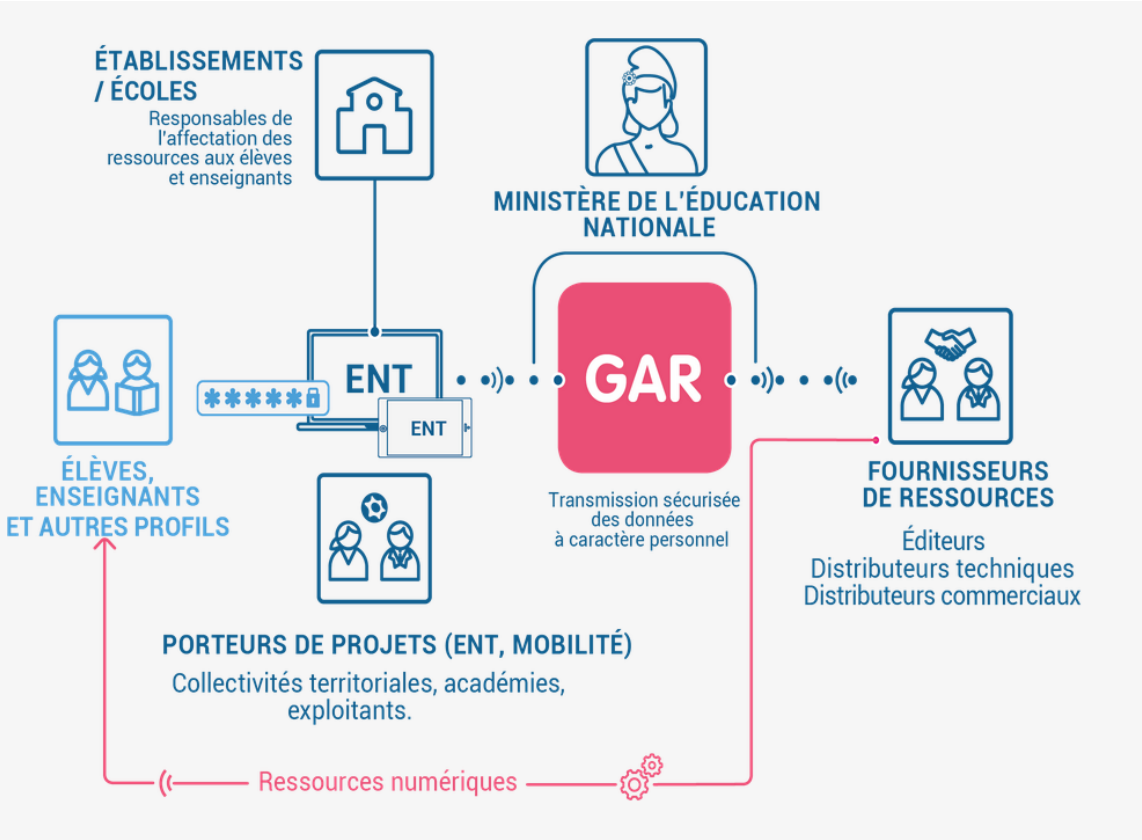
Sécuriser les pratiques : Les bons réflexes

3 – Le Gestionnaire d'Accès aux Ressources (GAR) :

Avec le GAR l'identité de l'utilisateur est transmise de l'ENT à la ressource utilisée. Le MENJS est responsable des données d'identification de l'utilisateur transmises ainsi que toutes les données personnelles produites dans la ressource. (Production, évaluation…)

Choisir une ressource compatible avec le GAR apporte une garantie concernant la protection des données.

Pas d'inscription au registre des traitements de la structure (EPLE …)



Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

éduthèque

éduthèque

éduthèque

éduthèque

éduthèque

Sécuriser les pratiques : Les bons réflexes

4 – Avoir recours à la pseudonymisation / Anonymisation :

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible.

Dans ce cas, la législation relative à la protection des données ne s'applique plus, car la diffusion ou la réutilisation des données anonymisées n'a pas d'impact sur la vie privée des personnes concernées.

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

4 – Avoir recours à la pseudonymisation / Anonymisation :

La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire.

En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.)
L'opération de pseudonymisation est donc réversible, contrairement à l'anonymisation.

La pseudonymisation constitue une des mesures recommandées par le RGPD pour limiter les risques liés au traitement de données personnelles. (C'est donc une élévation du niveau de sécurité, mais les traitements sont toujours soumis à la législation relative à la protection des données et reste sous la responsabilité du RT)

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

5 – Sécuriser les transferts de données :

- Je privilégie la solution de transfert de fichiers de l'intranet de mon académie ou des solutions proposées par le MEN (Ex avec les solutions proposées dans Apps.Education.fr qui permettent le chiffrement, avec des dispositif d'auto-destruction daté)
- Si je choisis d'autres solutions : (CF précédemment 2 - Le choix des outils/ressources en ligne :
- Je n'utilise pas de clé USB/support amovible non identifiée, trouvée ou prêtée.
- Je verrouille les fichiers avec un mot de passe ou je chiffre les documents sensibles
- J'utilise des espaces de partage avec une gestion des habilitations d'accès

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

6 – Sécuriser les collectes de données :

- Je privilégie l'utilisation de solutions académiques ou du MEN (Apps.Education.fr) de l'ENT de l'établissement, qui permettront de garantir la maîtrise des données collectées et de ne pas subir l'installation de cookies ou de traceurs.
- Si je choisis d'autres solutions : (CF précédemment 2 - Le choix des outils/ressources en ligne :

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

7 – Sécuriser les communications :

- J'utilise la messagerie professionnelle suivant les recommandations données
  Ex : redirection (IMAP /POP) (risque de stockage des données dans des messageries non maîtrisées)
- J'utilise la messagerie ou les solutions de communication de l'ENT (chat…)
- Un fichier suspect : je ne l'ouvre pas, je le signale à la DSI - Assistance (destruction de fichiers, rançongiciel…)
- Je ne réponds pas avec l'historique des documents attachés.
- Je ne réponds pas à un destinataire avec copie à tous s'il n'y a pas nécessité.
- Mailing en nombre, j'envoie en CCC (ou CCI) et non CC (copie carbone) : risque de fuite de carnet d'adresses.
- Je signale dans l'objet du message lorsque celui-ci est privé (usage personnel avec modération).

Vous êtes victime, infos, conseils et assistance sur
https://www.cybermalveillance.gouv.fr/victime/

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

8 – Sécuriser les accès internet :

- Sur mon PC ou mon téléphone portable, j'efface régulièrement mes traces (historique de navigation, cache, cookies, saisie de formulaire, stockage de mots de passe ...).
- Je paramètre mon navigateur
- Je prends le temps de configurer les cookies lors de l'ouverture des fenêtres.
- Je ne me connecte pas sur les wifis inconnus, j'évite le wifi gratuit, je ne transmets pas de données via ces réseaux non sécurisés, je déconnecte le wifi dès que je ne l'utilise plus.

Vous êtes victime, infos, conseils et assistance sur
https://www.cybermalveillance.gouv.fr/victime/

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Sécuriser les pratiques : Les bons réflexes

9 – Sécuriser les accès aux documents :

- Je travaille sur un (poste) matériel après une authentification personnelle. Je ne laisse pas de documents accessibles à tous sur un réseau (Répertoire « Transfert » ou autre).
- Je m'assure que la liste des personnes ayant accès à l'espace partagé est mise à jour.
- Poste partagé : Utiliser après authentification personnelle.
- Je ne laisse pas les documents à la photocopieuse et je supprime les documents scannés pouvant être stockés dans un dossier Scan.
- Je classe les documents papier dans les espaces prévus (armoire fermée), je ne laisse pas l'accès aux documents à des personnes non autorisées (collègues, autres services, visiteurs, prestataires…)
- Je transmets les données aux seuls destinataires autorisés et indiqués dans la fiche de traitement (présente dans le registre).
- Je détruis avec une broyeuse les documents sensibles.
- Pour mes informations privées, je stocke dans un dossier intitulé "Personnel" ou "Privé" (PC ou messagerie).

Rappel : la sécurité est une obligation pour le RT et les sous-traitants (RGPD, art.32)

Quelques ressources :

Je me forme / m’informe

- https://eduscol.education.fr/398/protection-des-donnees-personnelles-et-assistance
- DPD académique : dpd@ac-.....fr , Sites ou pages académiques (Intranet…)
- Parcours M@gistère académiques ou proposés par le MEN

J’enseigne

- https://eduscol.education.fr/574/le-referentiel-cnil-de-formation-des-eleves-la-protection-des-donnees-personnelles

Sigles

- **AIPD** : Analyse d'Impact sur la Protection des Données (= sur la vie privée des personnes)
- **CNIL** : Commission Nationale Informatique et Libertés
- **CRPA** : Code des Relations entre le Public et l'Administration
- **DCP** : Donnée à Caractère Personnel
- **DPO** : Data Protection Officer ou **DPD** : Délégué à la Protection des Données
- **DUA** : Durée d'Utilité Administrative
- **DUC** : Durée d'Utilisation Courante
- **IL** : Informatique et Libertés
- **LIL** : Loi Informatique et Libertés
- **NIR** : Numéro d'Inscription au Répertoire (national des personnes physiques = numéro Sécurité Sociale)
- **RGPD** : Règlement Général de la Protection des Données
- **RT** : Responsable de Traitement
- **ST** : Sous-Traitant

ACADÉMIE
DE POITIERS

Liberté
Égalité
Fraternité