Le RGPD
en 6 étapes…

dane BESANÇON

académie Besançon

Région académique
BOURGOGNE-FRANCHE-COMTÉ

dpd Délégué à la protection des données

Région académique
BOURGOGNE-FRANCHE-COMTÉ

Le règlement général sur la protection des données (RGPD)

LES OBJECTIFS

Responsabiliser les professionnels sur le traitement des données à caractère personnel.

Renforcement des **Droits des citoyens**.

Respect des textes **tout au long du cycle de vie des données**.

CNIL
Réduction du contrôle,
Renforce des pouvoirs de sanction,

Mise à disposition de **nouveaux outils** pour les responsables de traitement (registre, analyse d'impact, ..)

Nomination d'un **délégué à la protection des données** (DPD).

Nouveau mode de régulation
Précision et complément par la loi du 20 juin 2018 sur la protection des données.

RGPD
Règlement Général sur la Protection des Données

Région académique
BOURGOGNE-FRANCHE-COMTÉ

ÉVOLUTION RÈGLEMENTAIRE

Loi informatique et liberté - loi n° 78-17 (LIL) du 6 janvier 1978 :
Définition des principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles.

Convention pour la protection des données du 28 janvier 1981
à l'égard du traitement automatisé des données à caractère personnel.

Directive européenne 95/45/CE du 24 octobre 1995
Elle constitue le socle européen de la protection des données à caractère personnel.

Loi n °2004-801 du 4 août 2004
relative à la protection des données physiques à l'égard des traitements de données à caractère personnel?

Directive européenne 2000/31/CE du 8 juin 2000
sur le commerce électronique et sur certaines dispositions de la **Directive du 12 juillet 2002** sur la protection de la vie privée dans le secteur des communications électroniques.

Loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004
L'objectif est de donner une nouvelle impulsion au commerce électronique et à la sécurité des transactions électroniques.

Loi pour une république numérique du 7 octobre 2016
Objectifs : libérer les innovations ; créer un cadre de confiance, construire une république numérique ouverte et

RGPD - Règlement général sur la protection des données du 25 mai 2018
Renforcer la responsabilisation de ceux qui traitent les données, accroitre les droits des citoyens

Loi n° 2018-493 du 20 juin 2018 du 20 juin 2018
relative à la protection des données personnelles – modifie la LIL de 1978

RGPD
Règlement Général sur la Protection des Données

R
G
P
D

1

COMPRENDRE

Comprendre les concepts essentiels dans le domaine de la protection des données :

- Données personnelles : *informations permettant d'identifier directement ou indirectement une personne physique.*

- Responsable de traitement : *personne, autorité, service, ou organisme déterminant les finalités et moyens mis en place pour un traitement.*

- Traitement : *désigne les manipulations (collecte, stockage, consultation, suppression...) faites à une donnée.*

- Sous traitant : *personne physique ou morale qui traite les données à caractère personnel pour le compte du responsable de traitement.*

Extrait de l'article 4 du RGPD.

Région académique
BOURGOGNE-FRANCHE-COMTÉ

LES DONNÉES À CARACTÈRE PERSONNEL

Les données personnelles des enseignants et des élèves

Nom, prénom,
date de naissance,
adresse,
Numéro d'identification de l'Education nationale (NUMEN)
Structure de rattachement,
historique de ses postes,
références bancaires,
appartenance syndicale,
contenu de ses cours,
données de connexion ENT,
etc. …

enseignant

Nom, prénom,
date de naissance,
Adresse,
Admission, radiation,
classe, niveau, activités périscolaires, sorties scolaires, restauration scolaire, fiche élève,
données de connexion,
etc. …

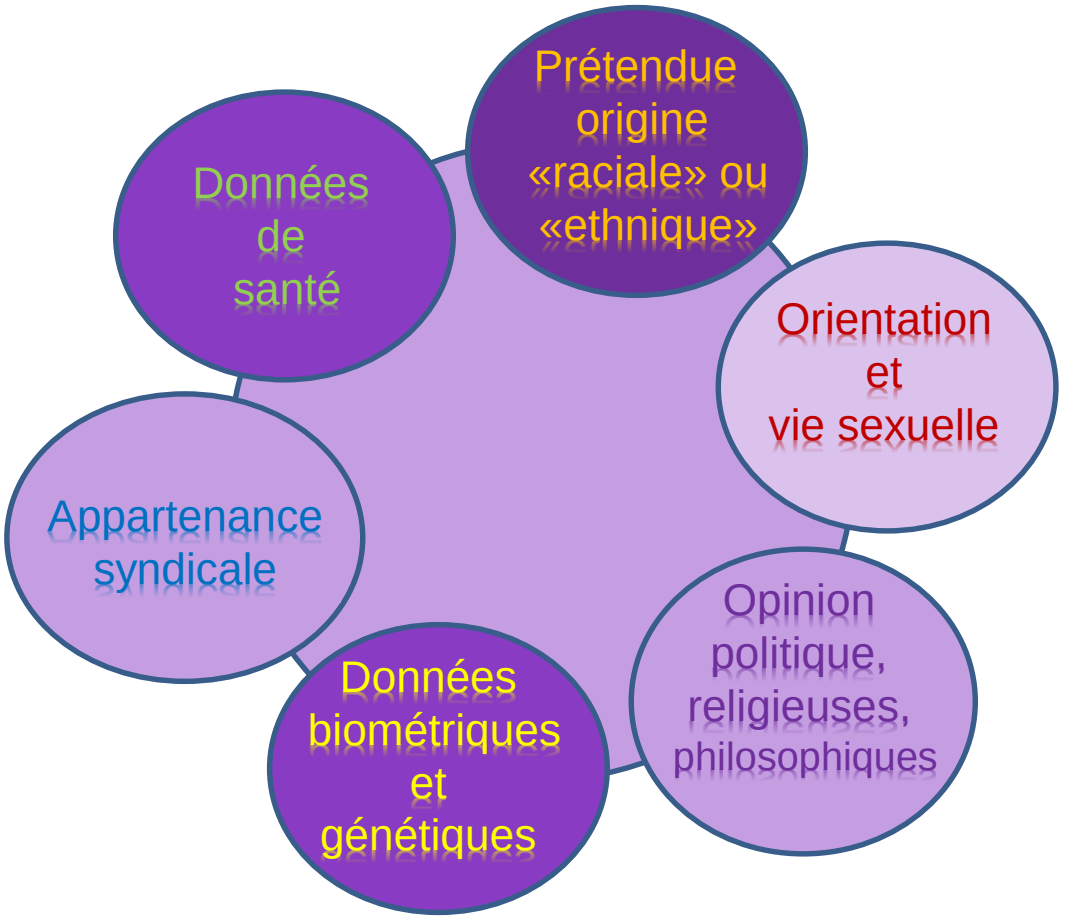
élève

RGPD
Règlement Général sur la Protection des Données

Région académique
BOURGOGNE-FRANCHE-COMTÉ

La nature d'une donnée sensible

UNE DONNÉE dite SENSISBLES



sauf ...

- Consentement
- But médical
- Intérêt public important
- Membre ou adhérents association

RGPD
Règlement Général sur la Protection des Données

Région académique
BOURGOGNE-FRANCHE-COMTÉ

Une donnée
dite SENSISBLE

Et dans le contexte de l'école ?

État vaccinal obligatoire à jour de l'enfant

Pas une donnée sensible

fiche sanitaire (infirmerie)

Format papier obligatoirement, transmise par les représentant légaux sous enveloppe cachetée.

Handicap, PAI ou PPS

Impossibilité de collecter la nature du handicap ou la pathologie mais seulement les mesures de prise en charge

RGPD
Règlement Général sur la Protection des Données

R G P D

2

RÉPERTORIER

Répertorier les différents traitements de données à caractère personnel et les inscrire dans le registre de traitement tenu.

Article 30 du RGPD :

« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité.
Ce registre comporte toutes les informations suivantes :

a) le nom et les coordonnées du responsable du traitement ;
b) les finalités du traitement ;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
e) le cas échéant, les transferts de données ;
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ».

Région académique
BOURGOGNE-FRANCHE-COMTÉ

FICHE DE TRAITEMENT

1ère partie

nom du fichier :	Fiche registre :
Fiche de registre Aix-Marseille.xlsx	
IDENTIFICATION	
Traitement n°	
Nom du traitement	
Mise en œuvre par (Registre principal concerné)	
Base légale	
traitement de référence	
Etat du traitement	
Perimetre du traitement	
Référence déclarative du traitement si formalité CNIL	
Date de création	
Dernière mise à jour	
ACTEURS	
Responsable de traitement	
Responsable(s) conjoint(s)	
Service encharge de la mise en œuvre	
Délégué à la protection des données	
Impact sur la vie privée	
Transfert Hors UE	
Données Sensibles	
Population Vulnérable	
Profilage	
Décision automatique avec effet légal	
Surveillance systématique	
Large échelle	
Croisement de données	
Usage Invovant	
Blocage d'un droit/contrat	
DPIA Obligatoire	
Ref DPIA	
Niveau de gravité et de vraisemblance	
Téléservices de l'administration	
Le traitement est un téléservice de l'administration	
Homologation RGS	
Date homologation	

Traitement : 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, telles que **la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction**

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement;

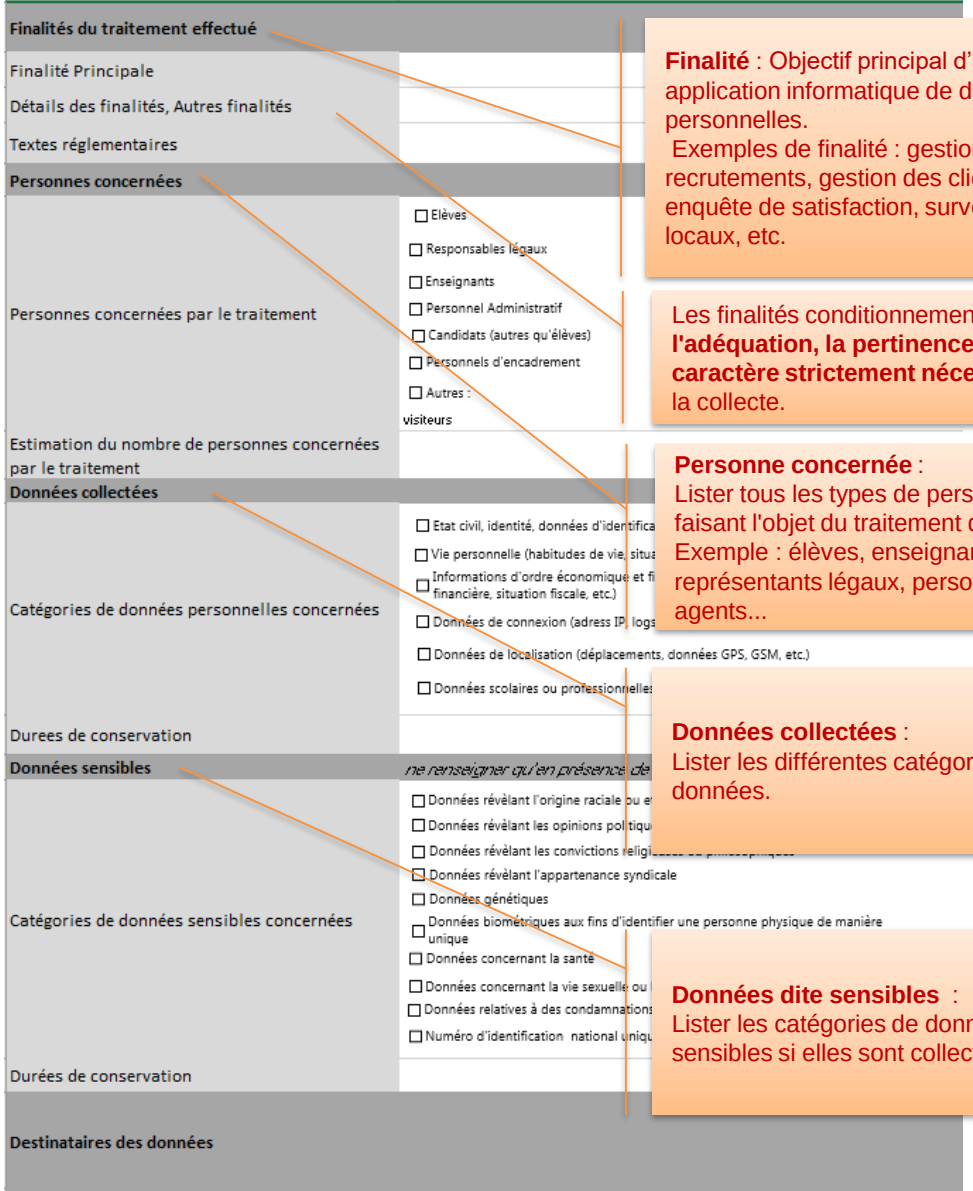
Impact sur vie privée : En tant que responsable d'un traitement de données, vous devez prendre des mesures pour garantir une utilisation de ces données respectueuse de la vie privée des personnes concernées. (PERTINENCE, TRANSPARENCE, RESPECT DES DROITS, MAÎTRISE, GESTION DES RIQUES, SÉCURITÉ

Téléservice :

Région académique
BOURGOGNE-FRANCHE-COMTÉ

FICHE DE TRAITEMENT

2ème partie



Finalités du traitement effectué	
Finalité Principale	
Détails des finalités, Autres finalités	
Textes réglementaires	
Personnes concernées	
Personnes concernées par le traitement	☐ Elèves ☐ Responsables légaux ☐ Enseignants ☐ Personnel Administratif ☐ Candidats (autres qu'élèves) ☐ Personnels d'encadrement ☐ Autres : visiteurs
Estimation du nombre de personnes concernées par le traitement	
Données collectées	
Catégories de données personnelles concernées	☐ Etat civil, identité, données d'identifica ☐ Vie personnelle (habitudes de vie, situa ☐ Informations d'ordre économique et fi financière, situation fiscale, etc.) ☐ Données de connexion (adress IP, logs ☐ Données de localisation (déplacements, données GPS, GSM, etc.) ☐ Données scolaires ou professionnelles
Durees de conservation	
Données sensibles	*ne renseigner qu'en présence de*
Catégories de données sensibles concernées	☐ Données révélant l'origine raciale ou et ☐ Données révélant les opinions politiqu ☐ Données révélant les convictions religi ☐ Données révélant l'appartenance syndicale ☐ Données génétiques ☐ Données biométriques aux fins d'identifier une personne physique de manière unique ☐ Données concernant la santé ☐ Données concernant la vie sexuelle ou ☐ Données relatives à des condamnations ☐ Numéro d'identification national uniqu
Durées de conservation	
Destinataires des données	

Finalité : Objectif principal d'une application informatique de données personnelles.
Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.

Les finalités conditionnement la **licéité, l'adéquation, la pertinence et le caractère strictement nécessaire** de la collecte.

Personne concernée :
Lister tous les types de personnes faisant l'objet du traitement de données.
Exemple : élèves, enseignants, représentants légaux, personnels, agents...

Données collectées :
Lister les différentes catégories de données.

Données dite sensibles :
Lister les catégories de données sensibles si elles sont collectées.

Région académique
BOURGOGNE-FRANCHE-COMTÉ

FICHE DE TRAITEMENT

3ème partie

RGPD
Règlement Général sur la Protection des Données

Transfert Hors UE	
Présence de transfert Hors UE	
Organisme(s) destinataire(s) et données concernées	
Pays de tranfert	
Type de garantie	
Modalité d'information des personnes concernées du transfert hors UE	
Respect des droits des personnes	
Fonction et coordonnées (personne ou service) pour l'exercice du droit d'accès	
Modalités d'informations des personnes	☐ formulaire de collecte ☐ mention sur site ☐ remise document ☐ voie affichage papier ☐ oralement lors premier échange ☐ sans information ☐ Autre :
Modalités d'exercice des droits des personnes	☐ Directement sur place ☐ Auprés du DPD (courrier ou courriel) ☐ par courrier postal auprés du service ☐ par courriel auprés du service concerné ☐ au travers du site web ☐ Autre :
Modalités de recueil du consentement	☐ Sans consentement explicite ☐ Case à cocher sur le site ☐ Consentement oral lors du premier con ☐ Consentement écrit
Mesures en vue d'assurer la sécurité des données	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	
Sous traitance	
nom du sous-traitant	
Contrat/convention comportant les clauses « Informatique et liberté » visée par le DPD	
date échéance contrat/convention	
Mises à jour - Evolutions	
détail des mises à jour ou évolutions	

Transfert hors UE : si les données sont transférer en dehors de l'union européenne , veuillez donner des garantes.

Droits des personnes : veuillez décrire les actions pour la mise en place des droits (**Le droit à l'information , le recueil du consentement , le droit d'opposition, les droits d'accès et de rectification)**

Mesures de sécurité : Pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins.

Sous-traitant :
Indiquer les coordonnées et les références de contrat ou convnetion.

Mise à jour : veuillez indiquer le délais pour le suivi et la mise à jour de cette fiche.

Région académique
BOURGOGNE-FRANCHE-COMTÉ

Le registre de traitement (le document)

LE REGISTRE DE TRAITEMENT

Actualiser le registre

Nom du traitement	Lien vers fiche (pour mise à jour du traitement)	Registre Principal	Responsable traitement	Finalité	Périmetre	Personnes concernées	Catégories	Données sensibles	transfert Hors UE	Sous-traitant	mise à jour

RGPD
Règlement Général sur la Protection des Données

R
G
P
D

3

RESPECTER

Respecter, pour chaque traitement, les 6 principes de la protection des données :

- Licéité
- Finalité
- Pertinence
- Exactitude
- Durée de conservation
- Sécurité

Article 5 du RGPD :

« Les données à caractère personnel doivent être :

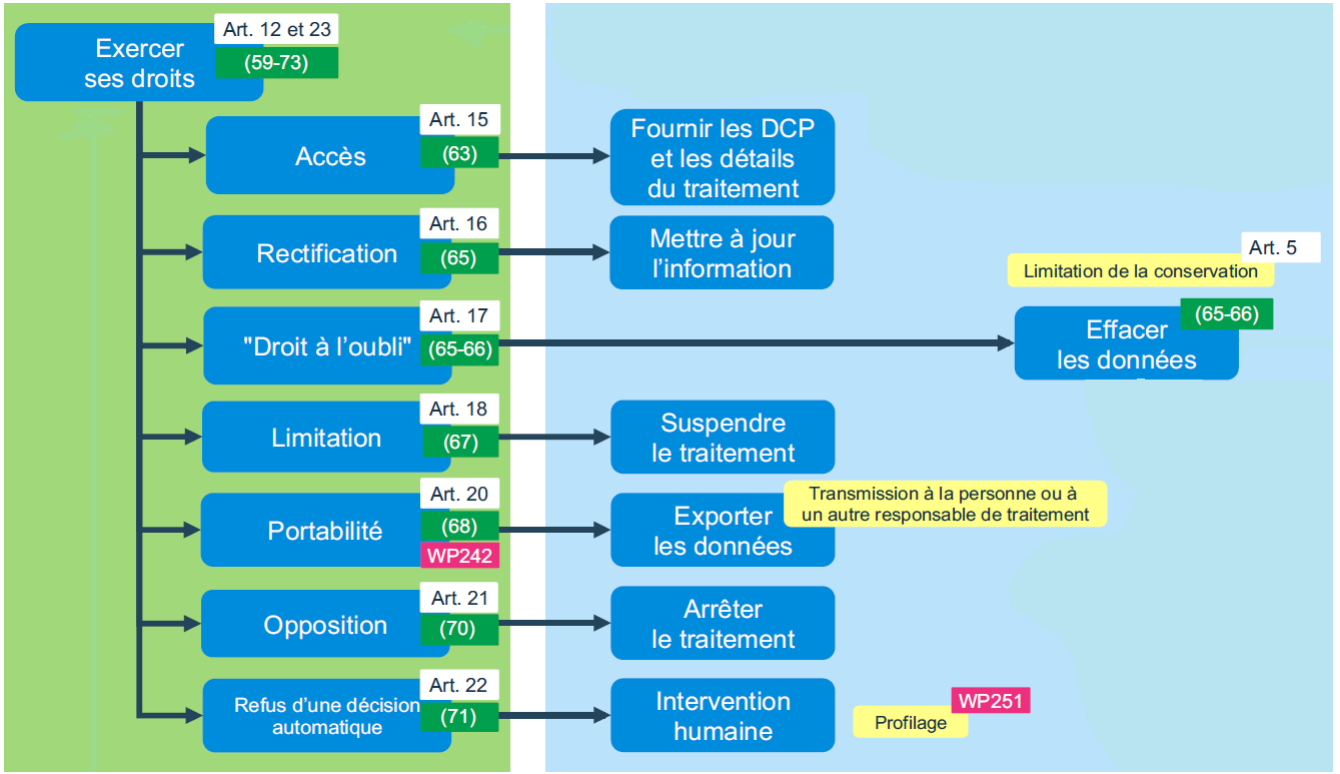
a) traitées de manière licite, loyale et transparente au regard de la personne concernée ;
b) collectées pour des finalités déterminées, explicites et légitimes ;
c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités ;
d) exactes et, si nécessaire, tenues à jour ;
e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités ;
f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel ».

R G P D

4

METTRE EN PLACE

Mettre en place des processus pour garantir l'exercice des droits des personnes.



R G P D

5

VÉRIFIER

Vérifier, dans la mesure du possible, les contrats passés avec les sous-traitants pour s'assurer du respect des règles émanant du RGPD.

Article 28 du RGPD :

« 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 ».

RGPD

6

EFFECTUER

Effectuer des études d'impact sur la vie privée (EIVP ou PIA) pour les traitements présentant des risques pour les droits et libertés des personnes concernées.

Article 35 RGPD :

« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

académie Besançon

Région académique
BOURGOGNE-FRANCHE-COMTÉ

L'ANALYSE D'IMPACT

AIPD

Analyse d'Impact relative à la Protection des Données

RGPD
Règlement Général sur la Protection des Données

DOIS-JE FAIRE UNE AIPD ?

Tout traitement de données personnelles susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées doit faire l'objet d'une analyse d'impact (AIPD).

L'analyse d'impact est un outil important de responsabilisation et de conformité qui permet de garantir le respect des principes du RGPD de façon opérationnelle et de pouvoir le démontrer.

Mon traitement est-il sur la liste des cas pour lesquels une AIPD est obligatoire ?

Consultez la liste

Oui

Non

Combien de critères mon traitement remplit-il parmi les suivants ?

1. *Évaluation/scoring (y compris le profilage)*
2. *Décision automatique avec effet légal ou similaire*
3. *Surveillance systématique*
4. *Données sensibles ou hautement personnellles (santé, géolocalisation, etc.)*
5. *Collecte à large échelle*
6. *Croisement de données*
7. *Personnes vulnérables (patients, personnes âgées, enfants, etc.)*
8. *Usage innovant (utilisation d'une nouvelle technologie)*
9. *Exclusion du bénéfice d'un droit/contrat*

Au moins deux critères

OU

Un critère mais je considère que mon traitement présente un risque élevé

Aucun critère

AIPD REQUISE

La CNIL vous propose une **boîte à outils** pour réaliser votre analyse d'impact.

Vous pouvez tout d'abord consulter **les questions/réponses** ainsi que les **guides pratiques et les catalogues de bonnes pratiques.**

Enfin, la CNIL met à votre disposition un **logiciel open source** pour faciliter la conduite et la formalisation de votre analyse.

AIPD NON REQUISE

Même non soumis à AIPD, les traitements doivent **respecter les principes de protection des données** et **les droits des personnes concernées.**

CNIL.

VIOLATION DES DONNÉES

Les violations de données personnelles susceptibles d'engendrer un risque pour les droits et libertés des personnes doivent être notifiées à la CNIL. Quatre mois après l'entrée en application du RGPD,

Article 33 - Notification à l'autorité de contrôle d'une violation de données à caractère personnel

1.En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, **72 heures au plus tard après en avoir pris connaissance**, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.
2.Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.
3.La notification visée au paragraphe 1 doit, à tout le moins:
a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
c) décrire les conséquences probables de la violation de données à caractère personnel;
d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
4.Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.
5.Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

Région académique
BOURGOGNE-FRANCHE-COMTÉ

LES VIOLATIONS DE DONNÉES

Les notifications de violation

Tout incident de sécurité, d'origine malveillante ou non, se produisant de manière intentionnelle ou non, et ***compromettant l'intégrité, la confidentialité ou la disponibilité de données personnelles.***

- ✓ La **destruction**, la **perte** ou **l'altération non désirée** de données à caractère personnel.
- ✓ La **divulgation non autorisée** de données à caractère personnel.
- ✓ L'**accès non autorisé** à des données à caractère personnel transmises, conservées ou traitées d'une autre manière.

› *https://www.cnil.fr/fr/les-violations-de-donnees-personnelles*

Effectuées par le responsable de traitement, les notifications doivent parvenir à la CNIL

› **72h au plus tard** après avoir eu connaissance de la violation et doit comprendre :

- **la nature de la violation** de données et **le nombre approximatif** de personnes concernées,
- les **coordonnées de la DPD**,
- les **conséquences probables** de la violation de données,
- les **mesures prises** ou que le responsable de traitement propose de prendre pour remédier à la violation de données.

› **Information des personnes concernées** (sous certaines conditions)

› **Information de la DPD**

La violation de données se caractérise principalement par **la perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite**

RGPD
Règlement Général sur la Protection des Données

Merci pour votre attention …