Groupe Pédagofiche

AMF69
RHÔNE ET MÉTROPOLE DE LYON - ASSOCIATION DES MAIRES ET PRÉSIDENTS D'INTERCOMMUNALITÉ

Règlement Général sur la Protection des Données

Quels changements pour les collectivités ?

Jeudi 24 mai 2018

Groupe Pédagofiche

Le contexte

De la loi « Informatique et Libertés » de 1978 au RGPD (mai 2018)

Les raisons :

- évolution des technologies
- volume des données collectées
- défaut de fiabilité / déficit de confiance
- nécessité d'harmoniser les niveaux de protection dans l'UE

Ce qui change :

- nouvelle logique de responsabilité
- DPD obligatoire
- droits des personnes renforcés ou nouveaux
- sanctions alourdies

Groupe Pédagofiche

Quelques définitions

Donnée à caractère personnel

Toute **information se rapportant à une personne physique identifiée ou identifiable** :

- **directement**
- **indirectement**, notamment par référence :

à un **identifiant**, tel que :
- un nom
- un numéro d'identification
- des données de localisation
- un identifiant en ligne

à un ou plusieurs éléments spécifiques propres à son **identité** :
- physique, physiologique, génétique, psychique
- économique, culturelle ou sociale

➔ **Définition très large** : toutes données permettant d'identifier une personne physique (nom, date de naissance, immatriculation, données GPS, adresse IP, photographie, voix…).

Groupe Pédagofiche

Traitement de données

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** :

- 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.

Le traitement peut être **informatisé ou non**.

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**. »

Dans le cadre d'une collectivité, c'est son représentant légal :

- le **maire**
- le président de l'EPCI...

Groupe Pédagofiche

Délégué à la protection des données – DPD (DPO - data protection officer)

« Chef d'orchestre »

Obligatoire

Indépendant

Son rôle :
Veiller au respect des nouvelles règles de traitement des données.

Remplace le correspondant informatique et libertés (CIL)

Groupe Pédagofiche

Une logique inversée

D'une logique de contrôle *a priori*, basée sur des formalités déclaratives auprès de la CNIL…

… à une **logique de responsabilisation** (« accountability ») basée sur un contrôle *a posteriori*.

➔ La **collectivité** devient **responsable de la protection des données** traitées.

Comment ?

Principe nouveau de **protection des données dès la conception** (*Privacy by design*) du traitement et **par défaut** (*Privacy by default*).

Groupe Pédagofiche

Une responsabilité partagée...

... avec le **sous-traitant*** qui :

- **doit respecter le RGPD**
- **doit agir selon les instructions du responsable du traitement**

https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne

*** « personne traitant des données à caractère personnel pour le compte du responsable du traitement »**

Sanctions

- **l'élu** / responsable du traitement :

  ➔ jusqu'à 20 millions € d'amendes

- le **sous-traitant** :

  ➔ 2 à 4 % du CA

Groupe Pédagofiche

Une gouvernance nouvelle

Avant le RGPD :
formalités préalables obligatoires
(régime déclaratif auprès de la CNIL)

Avec le RGPD :
gouvernance
des données personnelles

Groupe Pédagofiche

Nouvelle gouvernance : méthodologie

Protection des données « dès la conception et par défaut »

1 - Désigner un DPD

2 - Recenser les traitements existants

3 - Identifier les actions à mener en priorité pour respecter les nouvelles règles

4 - Gérer les risques propres aux sensibles (analyse d'impact)

5 - Organiser la protection 

6 - Documenter la conformité

1 - Désigner un DPD

Le DPD veille au **respect des nouvelles règles** :

- il **informe et conseille** le responsable du traitement et les agents sur les obligations et les outils disponibles

- il **contrôle le respect du RGPD**

- il est l'**intermédiaire** entre la collectivité et la CNIL

- il conseille la collectivité sur la réalisation des analyses d'impact (PIA) sur la protection des données et en vérifie l'exécution

1 - Désigner un DPD

Un niveau d'expertise et des moyens pour exercer son rôle

- **connaissances spécialisées du droit et des pratiques** en matière de protection des données

- **moyens suffisants** pour mener à bien ses missions :
  - ressources en temps, personnels et matériels
  - accès aux informations nécessaires
  - associé aux questions « Informatique et Libertés »
  - formations nécessaires

- **agir en toute indépendance** :
  - pas de conflit d'intérêts
  - pouvoir rendre compte au plus haut niveau
  - ne pas être sanctionné
  - ne pas recevoir d'instruction

1 - Désigner un DPD

DPD/DPO mutualisé

- EPCI dont la commune est membre
- structure de mutualisation informatique

Avantages

- garantir l'indépendance du DPO
- avoir un DPO aguerri
- permettre que toutes les collectivités en soient dotées

Condition

« Facilement joignable », le responsable du traitement veille à ce que les coordonnées du DPO soient disponibles et à jour.

Groupe Pédagofiche

2 – Recenser les traitements existants

Quoi ?

- Les différents traitements de DP
- Les catégories de données personnelles traitées (sensibles ou pas)

Qui ?

- Les acteurs internes et externes : responsable du traitement, DPD, responsables de services, prestataires sous-traitants…

Pourquoi ?

- Les objectifs poursuivis/finalités du traitement de données

Où ?

- Le lieu d'hébergement des données
- Les flux : origine et destination des données

Comment ?

- Les mesures de sécurité mises en place

Jusqu'à quand ?

- La durée de conservation

Groupe Pédagofiche

2 – Recenser les traitements existants

Registre

Registre des activités de traitement de
[Nom de l'organisme]

Coordonnées du responsable de l'organisme (responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)	*Ex : NOM prénom du responsable légal* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*
Nom et coordonnées du délégué à la protection des données (si vous avez désigné un DPO)	*Ex : NOM prénom du DPO* *Société (si DPO externe)* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités (exemples)
Activité 1	*Gestion de la paie*
Activité 2	*Gestion des prospects*
Activité 3	*Gestion des fournisseurs*
Activité 4	*Vente en ligne*
Activité 5	*Sécurisation des locaux*
Activité 6	
Activité 7	
Activité 8	
Activité 9	

Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre est disponible sur la page suivante.

Fiche de registre de l'activité 1

(Reprise de l'activité 1 de la liste des activités)

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de données est partagée avec un autre organisme)*	
Nom du logiciel ou de l'application (si pertinent)	

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemple : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. _____ 2. _____
3. _____ 4. _____

Catégories de données collectées

Listez les différentes données traitées

☐ *État-civil, identité, données d'identification, images (nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

☐ *Vie personnelle (habitudes de vie, situation familiale, etc.)*

☐ *Vie professionnelle (CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*

☐ *Informations d'ordre économique et financier (revenus, situation financière, données bancaires, etc.)*

- https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

Groupe Pédagofiche

3 – Identifier les actions prioritaires

- Collecter et traiter **seulement les données strictement nécessaires**
- Réviser les **mentions d'information**
- Vérifier que les **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses
- Prévoir l'exercice des **droits des personnes**
- Vérifier les **mesures de sécurité** mises en place
- Identifier **la base juridique** du traitement

Guide CNIL « la sécurité des données personnelles » :
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

Groupe Pédagofiche

4 – Gérer les risques

Traitements de DP à risques élevés pour les droits et libertés des personnes

➔ **Analyse d'impact** sur la protection des données (**PIA**)

Qu'est-ce qu'un traitement de DP à risque ?

4 – Gérer les risques

Le traitement de DP à risques élevés cumule au moins 2 des 9 critères suivants :

1. Évaluation ou notation ;
2. Décision automatisée avec effet juridique ou effet similaire significatif ;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement personnel ;
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Groupe Pédagofiche

4 – Gérer les risques

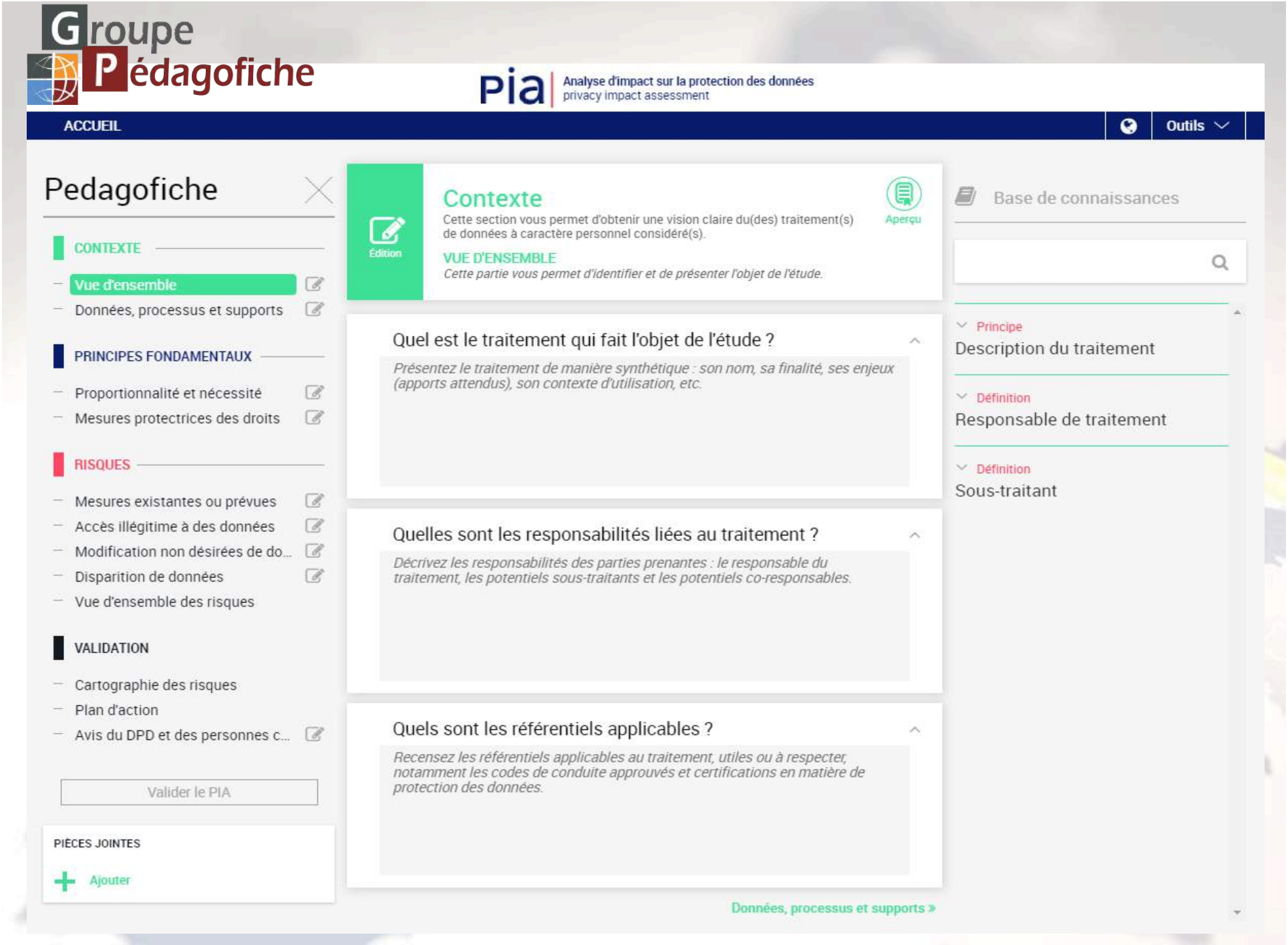
Analyse d'impact (PIA)

PIA = outil d'évaluation d'impact sur la vie privée

Respect des principes et droits fondamentaux + Gestion des risques liés à la sécurité des données = **CONFORMITÉ AU RGPD**

1. **délimiter et décrire le contexte du traitement = vision claire**
2. **analyser les mesures garantissant le respect de la vie privée**
3. **apprécier les risques et vérifier qu'ils sont convenablement traités**
4. **valider le PIA ou réviser les étapes précédentes**

Logiciel PIA (CNIL):
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil


Groupe Pédagofiche
pia
Analyse d'impact sur la protection des données
privacy impact assessment
ACCUEIL
Outils
Pedagofiche
CONTEXTE
Vue d'ensemble
Données, processus et supports
PRINCIPES FONDAMENTAUX
Proportionnalité et nécessité
Mesures protectrices des droits
RISQUES
Mesures existantes ou prévues
Accès illégitime à des données
Modification non désirées de do...
Disparition de données
Vue d'ensemble des risques
VALIDATION
Cartographie des risques
Plan d'action
Avis du DPD et des personnes c...
Valider le PIA
PIÈCES JOINTES
Ajouter
Édition
Contexte
Cette section vous permet d'obtenir une vision claire du(des) traitement(s) de données à caractère personnel considéré(s).
VUE D'ENSEMBLE
Cette partie vous permet d'identifier et de présenter l'objet de l'étude.
Aperçu
Quel est le traitement qui fait l'objet de l'étude ?
Présentez le traitement de manière synthétique : son nom, sa finalité, ses enjeux (apports attendus), son contexte d'utilisation, etc.
Quelles sont les responsabilités liées au traitement ?
Décrivez les responsabilités des parties prenantes : le responsable du traitement, les potentiels sous-traitants et les potentiels co-responsables.
Quels sont les référentiels applicables ?
Recensez les référentiels applicables au traitement, utiles ou à respecter, notamment les codes de conduite approuvés et certifications en matière de protection des données.
Données, processus et supports »
Base de connaissances
Principe
Description du traitement
Définition
Responsable de traitement
Définition
Sous-traitant

5 – Organiser la protection des données

- prendre en compte la protection des données personnelles dès la conception

- organiser la remontée d'informations

- traiter les réclamations et les demandes

- anticiper les violations de données

Groupe Pédagofiche

6 – Dossier de conformité

- la documentation sur les traitements de données
  - le registre des traitements
  - les analyses d'impacts (PIA)

- l'information des personnes
  - les mentions d'information
  - les modèles de recueil de consentement
  - les procédures d'exercice des droits

- les pièces définissant les rôles et les responsabilités
  - les contrats avec les sous-traitants
  - les procédures en cas de violation des données
  - la preuve du consentement des personnes

Groupe Pédagofiche

RGPD et Open Data

Open data :

- 7 octobre 2018
- collectivités + 3 500 habitants ou + 50 agents

Obligation de publier sur Internet leurs bases de données, sous réserve notamment d'anonymisation

Groupe Pédagofiche - CS 80005 NOHANENT - 63408 CHAMALIERES Cedex - Tél : 04 73 60 59 93 / Fax : 04 73 62 88 76
http://www.mairiexpert.fr / email : mairiexpert@pedagofiche.fr