Atelier de sensibilisation aux enjeux du RGPD

SCALA

Février 2025

Noémie BRIANTAIS-FOFANA
CNIL

Plan de la présentation

1. Présentation de la CNIL
2. Présentation du RGPD
3. Notions clés
4. Recours à un sous-traitant et désignation d'un DPO
5. Principes du RGPD
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

Plan de la présentation

1. **Présentation de la CNIL**
2. Présentation du RGPD
3. Notions clés
4. Recours à un sous-traitant et désignation d'un DPO
5. Principes du RGPD
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

LA CNIL

Selon vous, la CNIL c'est :

1 – Un ministère ?

2 – Une autorité administrative indépendante ?

3 - Une collectivité territoriale ?

LA CNIL

Selon vous, la CNIL a pour mission :

1 – De garantir le droit à la vie privée, les libertés individuelles ou publiques et la protection des données à caractère personnel ?

2 – De recenser chaque citoyen pour les administrations françaises à partir de leur numéro d'inscription au répertoire (NIR) ?

LA CNIL

Qu’est-ce que la CNIL ?

- Créée par la loi Informatique et Libertés du 6 janvier 1978
- Autorité administrative indépendante chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papier, aussi bien publics que privés.
- **Sa mission au quotidien :** s’assurer que l’informatique soit au service du citoyen et qu’elle ne porte atteinte ni à l’identité humaine, ni aux droits de l’homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

QUI COMPOSE LA COMMISSION ?

La CNIL est composée de

18 membres

- **4** PARLEMENTAIRES (2 députés, 2 sénateurs)
- **5** PERSONNALITÉS QUALIFIÉES
- **1** REPRÉSENTANT DE LA COMMISSION D'ACCÈS AUX DOCUMENTS ADMINISTRATIFS
- **6** REPRÉSENTANTS DE HAUTES JURIDICTIONS (Conseil d’État, Cour des comptes, Cour de cassation)
- **2** MEMBRES DU CONSEIL ÉCONOMIQUE, SOCIAL ET ENVIRONNEMENTAL

LA CNIL

CHIFFRES-CLÉS

BUDGET 2024

28 millions d'€

CNIL.

RESSOURCES HUMAINES EN 2024

298 postes

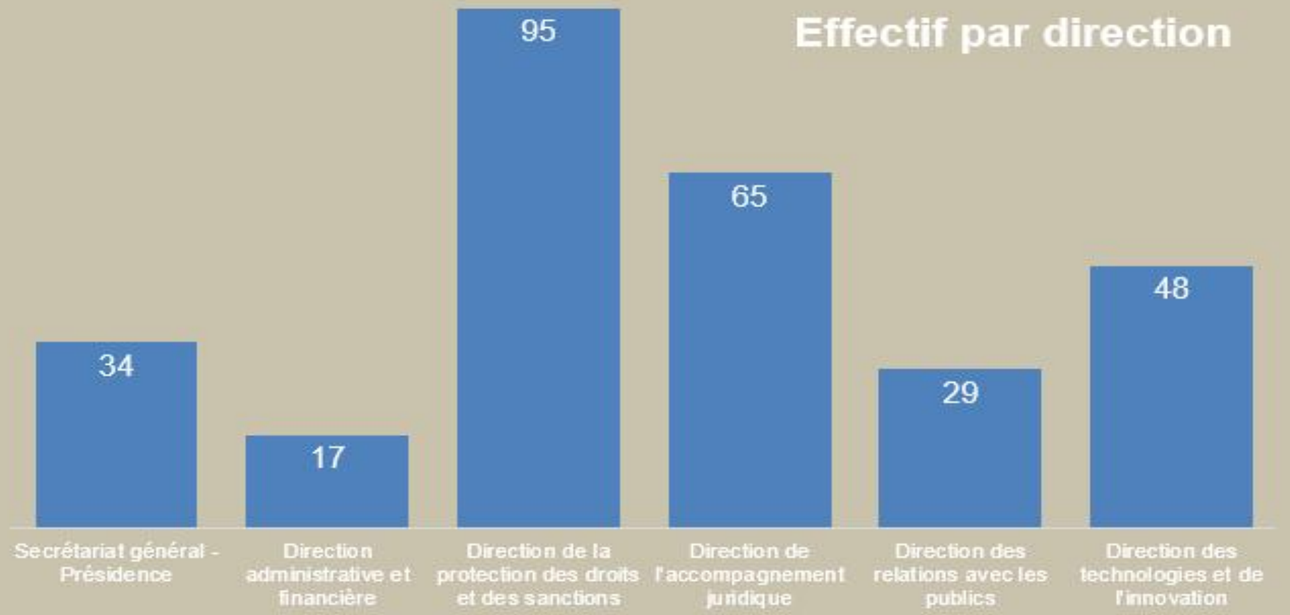
60,7% **39,3%**

39,2 ans (moyenne d'âge)

7 ans et 2 mois (ancienneté moyenne)

81,94% des postes occupés en cat. A

Effectif par direction



LA CNIL

Informer et protéger les droits

- Répondre aux demandes des particuliers et des professionnels.
- Mener des actions de communication à travers ses réseaux, les médias, le site web, les réseaux sociaux ou en mettant à disposition des outils pédagogiques.

Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits.

Accompagner la conformité et conseiller

- Aider les organismes privés et publics à se conformer au RGPD en proposant une boîte à outils adaptée à leurs tailles et leurs besoins.
- Veiller à la recherche de solutions leur permettant de poursuivre leurs objectifs légitimes dans le strict respect des droits et des libertés des citoyens.

CNIL.

Anticiper et innover

- Détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée.
- Assurer une veille dédiée.
- Contribuer au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de *privacy by design*.

Contrôler et sanctionner

- Le contrôle permet à la CNIL de vérifier la mise en œuvre concrète de la loi.
- Elle peut imposer à un acteur de régulariser son traitement (mise en demeure) ou prononcer des sanctions (amendes, etc.).

LA CNIL

La permanence téléphonique de la CNIL : 01.53.73.22.22

Plan de la présentation

1. Présentation de la CNIL
2. **Présentation du RGPD**
3. Notions clés
4. Recours à un sous-traitant et désignation d'un DPO
5. Principes du RGPD
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

PRÉSENTATION DU RGPD

Selon vous, le RGPD c'est :

1 – Un texte de droit français ?

2 – Un texte de droit européen ?

PRÉSENTATION DU RGPD

Selon vous, le RGPD implique :

1 – La réalisation de formalités préalables auprès de la CNIL avant d'effectuer un traitement de données personnelles ?

2 – La responsabilisation des acteurs qui assument les risques du traitement de données, sans besoin d'autorisation administrative ?

PRÉSENTATION DU RGPD

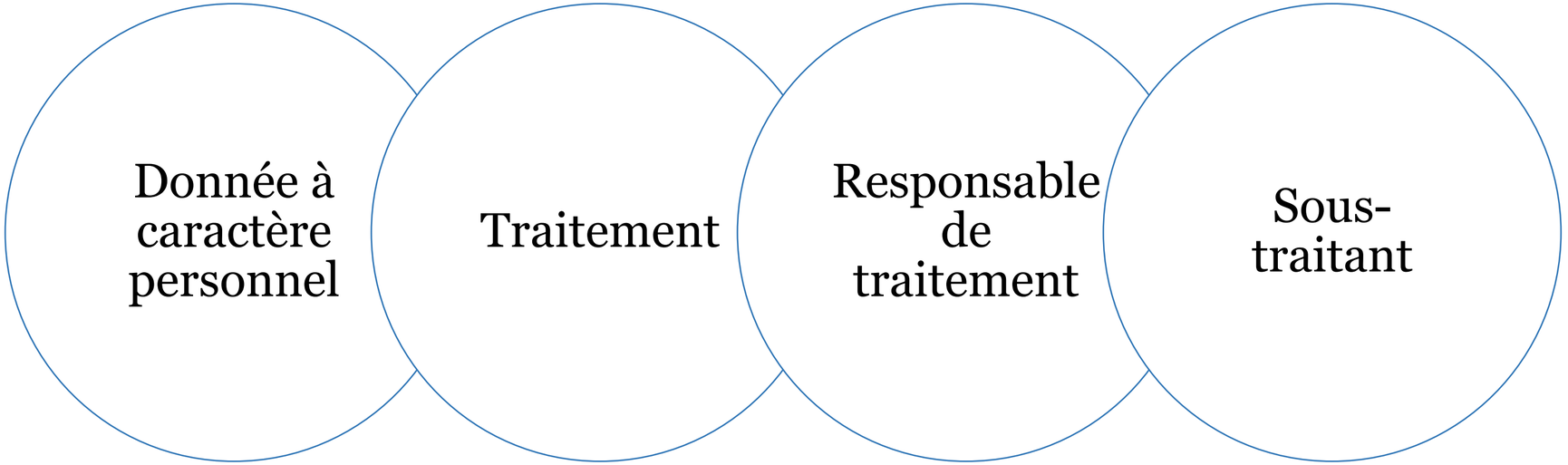
Règlement général sur la protection des données

- *L'accountability*
- Un champ d'application très large
- Renforcement des droits
- Des sanctions plus élevées

Plan de la présentation

1. Présentation de la CNIL
2. Présentation du RGPD
3. **Notions clés**
4. Recours à un sous-traitant et désignation d'un DPO
5. Principes du RGPD
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

NOTIONS CLÉS



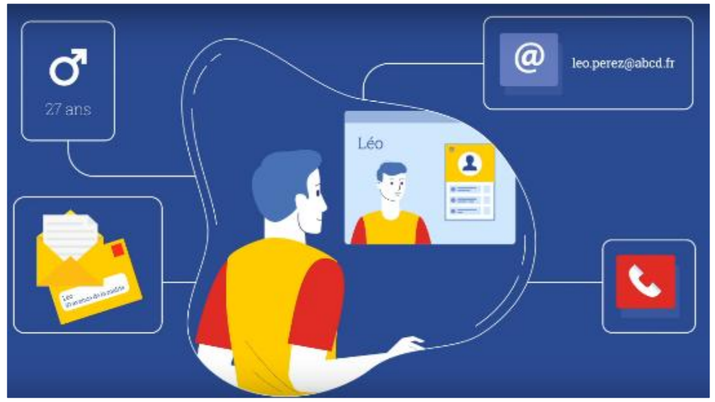
DONNÉES À CARACTÈRE PERSONNEL

➔Toute information se rapportant à une **personne physique identifiée ou identifiable**, c'est-à-dire qui peut être identifiée, **directement ou indirectement** (par le croisement de plusieurs données).

Peu importe que la donnée soit confidentielle, rendue publique, privée ou professionnelle.

- Exemples de données directement identifiantes : nom, prénom, photo, e-mail nominatif, etc.

- Exemples de données indirectement identifiantes : identifiant, numéro de téléphone, des données de localisation, un identifiant en ligne, des éléments spécifiques propres à une identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, etc.



CNIL.

DONNÉES À CARACTÈRE PERSONNEL

Un cinéma associatif souhaite réaliser des statistiques afin d'identifier comment améliorer la qualité de ses services.

Il a besoin d'analyser les données suivantes de ses abonnés :

- date de souscription à l'abonnement ;
- nombre d'enfants ;
- préférences et habitudes cinématographiques ;
- commune de résidence.

L'organisme traite t-il des données à caractère personnel ?

DONNÉES À CARACTÈRE PERSONNEL

Un cinéma associatif souhaite entretenir un fichier « listing » comprenant les coordonnées d'organismes partenaires, privés ou publics, à but non lucratif ou non. Le fichier comprend :

- Le nom de l'organisme (Compagnie A par ex.);
- L'adresse postale de l'organisme ;
- Le numéro de téléphone de son standard ;
- Un courriel générique.

L'organisme traite t-il des données à caractère personnel ?

TRAITEMENT

➔**Traitement de données à caractère personnel** : 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.

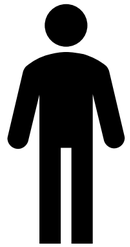
➔Le traitement de données à caractère personnel peut concerner **tout support, papier, électronique ou numérique**.

TRAITEMENT

Dans le cadre d'une campagne de recrutement d'un salarié pour l'entretien des salles, un cinéma associatif collecte le CV d'un candidat, mais ne retient finalement pas sa candidature.

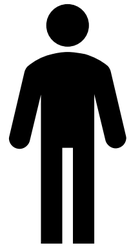
Des données à caractère personnel du candidat sont-elles traitées par l'organisme ?

LES ACTEURS DU TRAITEMENT DE DONNÉES



Le responsable de traitement

Détermine les finalités (« pourquoi ») et les moyens (« comment ») du traitement



Le sous-traitant

Traite des données personnelles pour le compte, sur instruction et sous l'autorité du responsable de traitement (ex. prestataires de services informatiques : hébergement, maintenance)

LES ACTEURS DU TRAITEMENT DE DONNÉES

Un cinéma associatif souhaite dématérialiser la vente de sa billetterie. Pour ce faire, il se tourne vers un prestataire fournisseur et hébergeur d'applications et interfaces web adaptés à la vente et à la revente de billets.

Afin d'acheter ses places, l'usager devra renseigner sur l'application ou le site web son nom et prénom, sa catégorie d'âge si nécessaire, son statut professionnel (étudiant, en recherche d'emploi) si nécessaire, son numéro de carte d'abonné et ses coordonnées bancaires.

1 – Qui est le responsable du traitement de ces données personnelles ?
2- Qui en est le sous-traitant ?

Plan de la présentation

1. Présentation de la CNIL
2. Présentation du RGPD
3. Notions clés
4. **Recours à un sous-traitant et désignation d'un DPO**
5. Principes du RGPD
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

RECOURS À UN SOUS-TRAITANT

Les **6 bonnes pratiques** à respecter dans le cadre d'une relation de sous-traitance :

- ✓ Déterminer le statut des acteurs impliqués
- ✓ Établir un contrat clair
- ✓ Documenter l'activité de sous-traitance
- ✓ Proposer des outils respectueux des données à caractère personnel
- ✓ Porter assistance pour répondre aux demandes d'exercices des droits des personnes
- ✓ Garantir la sécurité des données collectées

DÉSIGNATION D'UN DPO

Informer et conseiller

Contrôler le respect du RGPD

Coopérer avec l'autorité
Etre le point de contact

Conseils sur l'analyse d'impact
Vérifier son exécution

S'assurer de la bonne tenue de la documentation

CNIL.

DÉSIGNATION D'UN DPO

Organisme public

1. Activité de base
2. Large échelle
3. Suivi régulier et systématique

1. Activité de base
2. Large échelle
3. Données sensibles/données d'infraction

obligatoire

volontaire

Interne

Externe*

Mutualisation*

convention de mutualisation

CNIL.

DÉSIGNATION D'UN DPO

La désignation d'un DPO n'est *a priori* pas obligatoire pour les cinémas associatifs.

Quelques recommandations néanmoins :

- Mutualiser un DPO ;
- Nommer un référent RGPD veillant au bon respect des règles de conformité.

Objectifs de ces recommandations :

- Consolider des relations de confiance avec les bénévoles, les salariés et les abonnés et usagers ;
- Garantir la mise en conformité de l'organisme au RGPD, notamment pour l'information et l'exercice des droits des personnes ;
- Limiter les risques juridiques et réputationnels de l'organisme.

Plan de la présentation

1. Présentation de la CNIL
2. Présentation du RGPD
3. Notions clés
4. Recours à un sous-traitant et désignation d'un DPO
5. **Principes du RGPD**
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

PRINCIPES DU RGPD

01	Finalité	Les données personnelles contenues dans un traitement ne sont recueillies et traitées que pour **un usage déterminé et légitime, préalablement défini**
02	Base légale	Le traitement de données personnelles **doit être licite**, cad fondé sur **une base légale**
03	Minimisation	**Seules les données pertinentes et nécessaires** au regard des objectifs poursuivis doivent être traitées
04	Durée limitée de conservation	Tant qu'elles présentent un caractère identifiant, **les données ne peuvent être conservées de façon indéfinie dans les fichiers**
05	Sécurité	Le responsable du traitement doit **prendre les mesures nécessaires pour garantir l'intégrité et la confidentialité des données**
06	Droits des personnes	Toute personne dont les données sont utilisées dans un traitement disposent d'un **droit d'accès, de rectification et, selon la base légale, d'un droit d'opposition**

CNIL.

FINALITÉ DU TRAITEMENT

Cœur de la règlementation :

- Cartographie d'un traitement par finalité
- Lien entre les données, la base légale et la durée de conservation

Principe :

Les données doivent être collectées pour des finalités :

- **Déterminées**
- **explicites**
- **légitimes**

Elles ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.

FINALITÉ DU TRAITEMENT

Pour les besoins de son activité, un cinéma associatif organise des campagnes de communication afin d'obtenir davantage de bénévoles. Ensuite, il entretient un annuaire des bénévoles et organise leurs plannings. En cas de départ d'un bénévole de l'organisme, il garde ses données au cas où.

Quelles sont les finalités pouvant être poursuivies par l'organisme pour traiter des données personnelles ?

LA BASE LÉGALE

01  Le consentement

02  L’exécution du contrat

03  L’obligation légale

04  La sauvegarde des intérêts vitaux

05  La mission d’intérêt public

06  L’intérêt légitime

CNIL.

LE CONSENTEMENT

Le consentement doit être :
- libre
- spécifique
- éclairé
- univoque

Attention concernant les salariés : ils ne sont que très rarement en mesure de donner, de refuser ou de révoquer librement leur consentement, étant donné la dépendance qui découle de la relation employeur/employé. Ils ne peuvent donner leur libre consentement que dans le cas où l'acceptation ou le rejet d'une proposition n'entraine aucune conséquence sur leur situation.

LE CONSENTEMENT

Un cinéma associatif souhaite utiliser l'image de ses bénévoles afin de mettre en avant, sur papier et sur le site web, ses activités et actualités.

L'organisme peut-il fonder le traitement sur le consentement des bénévoles ?

L'EXÉCUTION DU CONTRAT

Le contrat peut valablement fonder un traitement sous réserve que celui-ci soit objectivement nécessaire à l'exécution de ce contrat.

Le recours au contrat pour fonder légalement un traitement est soumis à 3 conditions :

- il existe une relation contractuelle ou précontractuelle entre l'organisme et la personne concernée ;
- le contrat doit être valide au regard du droit applicable ;
- le contrat ne peut être retenu que si le traitement satisfait à la condition de nécessité.

L'EXÉCUTION DU CONTRAT

Dans le cadre de l'exécution du contrat d'abonnement, un cinéma associatif a besoin de traiter les données personnelles de l'abonné, afin de garantir que celui-ci puisse acheter ses places de cinéma à tarif réduit.

L'organisme réutilise les données de l'abonné pour lui communiquer par courriel une newsletter relative à ses activités.

Peut-il fonder ce dernier traitement des données sur l'exécution du contrat ?

L'OBLIGATION LÉGALE

Le recours à l'obligation légale pour fonder un traitement est soumis à plusieurs conditions :

- Le traitement doit être nécessaire à l'obligation légale qui s'impose à l'organisme ;
- L'obligation légale doit être définie par le droit européen ou national ;
- Ces dispositions doivent instituer une obligation impérative de traiter des données personnelles, suffisamment claire et précise ;
- Ces dispositions doivent au moins définir les finalités du traitement concerné
- Cette obligation doit s'imposer au responsable du traitement et non aux personnes concernées.

L'OBLIGATION LÉGALE

Exemple : lorsqu'un cinéma associatif effectue la déclaration sociale nominative pour ses salarié, il a l'obligation légale de traiter les données nécessaires (données concernant la paie du salarié, événements concernant les périodes d'activité du salarié).

L'INTÉRÊT LÉGITIME

Le recours à l'intérêt légitime de l'organisme pour fonder un traitement est soumis à plusieurs conditions :

- l'intérêt du responsable de traitement doit être légitime (licite, déterminé et réel) ;
- le traitement doit être nécessaire pour atteindre cet intérêt ;
- le traitement ne doit pas heurter les droits et intérêts des personnes dont les données sont traitées, compte tenu de leurs attentes raisonnables.

L'organisme doit opérer une pondération entre les droits et intérêts en cause, et vérifier dans ce cadre que les intérêts (commerciaux, de sécurité des biens, de lutte contre la fraude, etc.) qu'il poursuit ne créent pas de déséquilibre au détriment des droits et intérêts des personnes dont les données sont traitées, compte tenu de leurs attentes raisonnables.

L'INTÉRÊT LÉGITIME

Dans le cadre de l'exécution du contrat d'abonnement, un cinéma associatif a besoin de traiter les données personnelles de l'abonné, afin de garantir que celui-ci puisse acheter ses places de cinéma à tarif réduit.

L'organisme réutilise les données de l'abonné pour lui communiquer par courriel une newsletter relative à ses activités.

Peut-il fonder ce dernier traitement des données sur l'intérêt légitime de l'organisme ?

BASE LÉGALE

1/ Dans le cadre de la gestion de son activité, un cinéma associatif utilise les données de ses bénévoles pour organiser des formations. Quelle est la base légale permettant de fonder le traitement des données ?

2/ Dans le cadre de l'organisation de son activité, un cinéma associatif utilise les données de ses bénévoles pour gérer l'annuaire interne et l'organigramme. Quelle est la base légale permettant de fonder le traitement des données ?

3/ Dans le cadre de la gestion de son activité, un cinéma associatif souhaite collecter une photo de chacun de ses bénévoles afin de créer un trombinoscope. Quelle est la base légale permettant de fonder le traitement des données ?

PERTINENCE ET PRINCIPE DE MINIMISATION

Principe : Les données doivent être :

- **adéquates, pertinentes et non excessives** au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
- **exactes, complètes** et **mises à jour.**

PERTINENCE ET PRINCIPE DE MINIMISATION

Un cinéma associatif collecte et stocke une fiche personnelle pour chacun de ses bénévoles afin de disposer des informations nécessaires pour organiser les plannings. La fiche comprend les données suivantes :

- Identité : nom, prénom, date de naissance
- Coordonnées : e-mail, adresse postale, téléphone
- Informations personnelles : statut familial, activité professionnelle, indisponibilité pour garde d'enfants ou aide d'un proche
- Informations relatives à la santé : rendez-vous médicaux réguliers.

Toutes les données traitées sont-elles nécessaires à l'organisme pour gérer le planning des bénévoles ?

PERTINENCE ET PRINCIPE DE MINIMISATION

1/Les questions à se poser :

- Quel est mon objectif ?
- Quelles données sont indispensables pour atteindre l'objectif ?
- Ai-je le droit de collecter ces données ?
- Ai-je distingué les données obligatoires des données facultatives ?
- Ai-je besoin de toutes les données à tous les stades du traitement ?

2/ Les bonnes pratiques :

- Vérifier s'il existe une solution moins intrusive, nécessitant moins de données, pour atteindre le même objectif ;
- Ne pas collecter de données à titre préventif ;
- Favoriser la pseudonymisation si des données nominatives ne sont pas nécessaires ;
- Éviter les zones de commentaires libres et préférer les menus déroulants.

LES DONNÉES PARTICULIÈRES

DONNÉES SENSIBLES (ART. 9 RGPD)

- Données qui relèvent : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques aux fins d'identifier une personne physique de manière unique, données concernant la santé ou données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique
- Interdit par principe
- Sauf exceptions (consentement, exécution d'obligations ou exercice des droits en matière de droit du travail, etc.)

DONNÉES RELATIVES AUX CONDAMNATIONS PÉNALES ET AUX INFRACTIONS (ART. 10 RGPD ET 46 LIL)

- Données qualifiées comme telles par une autorité compétente et données collectées dans le but d'établir l'existence ou de prévenir la commission d'infractions
- Autorisé selon la qualité du professionnel (notamment les juridictions, autorités publiques et personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales + personnes morales de droit privé collaborant au service public de la justice et citées par l'article 76 du décret n° 2019-536 du 29 mai 2019)

DONNÉES RELATIVES À DES MINEURS

- Public vulnérable = poids plus important dans l'analyse de la proportionnalité
- Information renforcée

NUMÉRO DE SÉCURITÉ SOCIALE (DÉCRET « CADRE NIR » N° 2019-341 du 19 avril 2019)

LES DONNÉES PARTICULIÈRES

Exemples :

1/Lors de la conclusion d'un contrat de travail avec un salarié recruté, le cinéma associatif, en sa qualité d'employeur, a l'obligation d'accomplir certaines formalités déclaratives qui requièrent le traitement du numéro de sécurité sociale (NIR) des salariés.

2/Un cinéma associatif organise un événement pour ses membres. Afin d'organiser le repas, il a besoin de connaître les allergies alimentaires des adhérents participants. Il s'agit d'une donnée de santé, que l'organisme ne pourra collecter qu'avec le consentement des personnes concernées.

3/Un cinéma associatif accueille une classe de collégiens pour une animation, sur la demande de l'établissement scolaire. L'organisme pourrait être amené à collecter des données de mineurs. Il devra faire preuve d'une vigilance particulière pour le traitement de ces données.

CONSERVATION LIMITÉE DES DONNÉES

Principe : les données ne peuvent être conservées que pendant une durée limitée, définie en amont.

- Durée déterminée en **fonction de la finalité** de chaque traitement. Cette durée va donc **varier** selon les différents objectifs poursuivis par l'utilisation de données personnelles.
- Il s'agit de déterminer soit une durée fixe de conservation soit un critère objectif utilisé comme fait générateur pour déterminer cette durée.

CONSERVATION LIMITÉE DES DONNÉES

Cycle de vie des données :

- Conservation en **base active** : les données sont accessibles par toutes les personnes dont les missions le justifient tout le temps de l'utilisation courante des données (consultation, utilisation, exportation, modification, etc).

- **L'archivage intermédiaire** : une fois l'objectif réalisé, les données peuvent malgré tout être conservées lorsqu'une obligation légale ou un intérêt administratif l'exige.

Les données sont isolées de la base courante sur le plan physique (extraction et stockage sur un support distinct) et logique (restrictions des habilitations et droits d'accès aux données aux seules personnes dont les missions sont concernées par l'obligation légale ou l'intérêt administratif).

Seules les données nécessaires à l'objectif poursuivi par l'archivage doivent être archivées.

CONSERVATION LIMITÉE DES DONNÉES

1/Les questions à se poser :

- Jusqu'à quand ai-je besoin des données pour atteindre l'objectif fixé ?
- Suis-je soumis à une obligation légale de conserver les données ?
- Toutes les données doivent-elles être conserver pour la même durée ?
- Une fois l'objectif atteint dois-je les conserver pour d'autres impératifs ? (contentieux, délais recours justice).

2/ Les bonnes pratiques : se référer aux outils pédagogiques sectoriels proposés par la CNIL :

- Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales ;
- Guide du recrutement ;
- Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel ;
- Guide de sensibilisation au RGPD pour les associations.

CONSERVATION LIMITÉE DES DONNÉES

Exemples :

1/Un cinéma associatif utilise les données d'identité et les coordonnées d'abonnés (carte abonnement) à des fins de communication d'une newsletter et d'événements à venir (ciné clubs, expositions, etc.). L'organisme pourra conserver **en base active** les données **pendant la relation commerciale**, **puis** pour une durée de **3** ans à compter de la fin de la relation, si la personne y consent. Si la personne souhaite **retirer son consentement** avant la fin de la période des trois ans, l'organisme devra **supprimer les données immédiatement**.

2/Dans le cadre de ses activités, un cinéma associatif permet l'achat de places de cinémas sur son site web. Pour ce faire, les usagers peuvent créer un compte en ligne. Les données pourront être conservées **en base active jusqu'à la suppression du compte par l'utilisateur**. Toutefois, il est fréquent que les utilisateurs n'utilisent plus ces comptes sans pour autant les supprimer, ce qui conduirait à faire perdurer ces comptes indéfiniment. Dans ce cas, l'organisme devra prévoir de **supprimer le compte inactif au bout de 2 ans**. Il devra préalablement avertir l'usager afin de lui laisser la possibilité d'exprimer son souhait de maintenir le compte actif.

3/Dans le cadre de la gestion des bulletins de salaire de ses salariés, un cinéma associatif devra conserver ceux-ci **en base active 1 mois** puis **en archivage intermédiaire 5 ans** et **50 ans en cas de mise à disposition des fiches aux salariés par voie dématérialisée** (articles L. 3243-4 et D. 3243-8 du code du travail).

OBLIGATION DE SÉCURITÉ

Principe : prendre « *toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* »

➔ Respect de **l'intégrité** et de la **confidentialité** des données

Identification des destinataires légitimes et tiers autorisés (OPJ, administration fiscale, …).

OBLIGATION DE SÉCURITÉ

Trois principes :

- **Confidentialité** : accessibilité des données uniquement pour les personnes autorisées. L'organisme doit limiter la divulgation des données à des personnes internes ou externes qui n'ont pas besoin de les connaître.

➢ En pratique, seuls les adhérents et salariés de l'association dont les missions le nécessitent doivent pouvoir accéder aux données traitées par votre association.
➢ Avant une communication des données à un autre organisme, 3 étapes à respecter :

1. Vérifier l'existence d'un fondement légal.
2. Vérifier la source et du périmètre de la demande.
3. Sécuriser la communication des données ou les modalités d'accès.

- **Intégrité** : pas d'altération ou de modification des données.

- **Disponibilité** : les données doivent être accessibles en permanence par les personnes autorisées.

OBLIGATION DE SÉCURITÉ

Bonnes pratiques recommandées, notamment :

- **Informer et sensibiliser** les bénévoles et les salariés
- Rédiger une **charte informatique** dotée d'une force contraignante
- Prévoir des **moyens d'authentification** pour les accès électroniques (identifiant unique pour chaque utilisateur, mot de passe sécurisé,…)
- Gérer les **habilitations** (définir les profils d'habilitation pour les accès, revue et suppression annuelle des habilitations,…)
- Prévoir un **système de journalisation** (tracer les opérations)
- Prévoir une **procédure de gestion des accidents** (procédure en cas de violation de données)
- **Sécuriser les postes de travail** (antivirus, verrouillage automatique de session,…)
- **Sécuriser les sites web** (vérifier qu'aucun mot de passe ou identifiant ne passe dans les url, bandeau de consentement pour les cookies non nécessaires, canal chiffré et authentifié pour les paiements (https),…)
- **Archiver de manière sécurisée** (modalités d'accès spécifique aux données archivées)
- **Choisir des canaux sécurisés** pour l'accès ou la communication des données et vérifier qu'il s'agit du bon destinataire (éviter le recours aux clés usb non chiffrées,…)
- **Restreindre l'accès aux locaux** (verrouillage des portes, alarmes)
- **Sécuriser l'accès aux documents papiers** (tri des documents et différents rangements fermant à clés, distribution limitée des clés,…)

➔**Gérer la sous-traitance** (vigilance dans le choix du sous-traitance)

OBLIGATION DE SÉCURITÉ

Bonnes pratiques recommandées, notamment :

Voici quelques vérifications que vous pouvez déjà effectuer :

- [ ] Les accès aux locaux sont-ils sécurisés ? (ex. : alarme, système de vidéosurveillance, etc.)
- [ ] Les armoires et coffres-forts sont-ils fermés à clés systématiquement ?
- [ ] Les comptes utilisateurs sont-ils protégés par des mots de passe d'une complexité suffisante ?
- [ ] Les comptes utilisateurs sont-ils supprimés au départ d'un utilisateur ?
- [ ] Des profils distincts sont-ils prévus selon les besoins des utilisateurs pour accéder aux données ?
- [ ] Les postes de travail sont-ils sécurisés (ex. : verrouillage automatique de session, antivirus et logiciels à jour) ?
- [ ] Les membres de l'association sont-ils sensibilisés à la protection de la vie privée ? Une charte informatique est-elle signée ?
- [ ] Des mobiles multifonctions (smartphones), ordinateurs portables ou clés USB sont-ils utilisés ? Leur usage est-il encadré ?
- [ ] Des procédures de sauvegardes régulières et de récupération des données en cas d'incident sont-elles mises en place ?
- [ ] Votre site web utilise-t-il un protocole sécurisé pour les pages sur lesquelles sont affichées ou transmises des données personnelles (ex. : authentification, formulaire en ligne) ?

OBLIGATION DE SÉCURITÉ

Qu’est-ce qu’une violation de données ?

Une violation de la sécurité se caractérise par la **destruction**, la **perte**, l'**altération**, la **divulgation** non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'**accès non autorisé** à de telles données, **de manière accidentelle ou illicite (incident ou malveillance) :**

- suppression accidentelle de comptes d’utilisateurs d’un site web ;
- perte d’une clef USB non sécurisée contenant une copie de la base bénévoles d’une association;
- introduction malveillante pour détourner les paiements lors d’achats de places de cinéma sur un site web.

OBLIGATION DE SÉCURITÉ

Que faire en cas de violation de données ?

1/**Si la violation n'entraîne pas de risque** pour les droits et libertés des personnes concernées, le responsable du traitement :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- ne doit pas notifier cette violation ni à la CNIL, qui peut en revanche contrôler cette documentation interne, ni aux personnes concernées.

2/**Si la violation entraîne un risque** pour les droits et libertés des personnes concernées, le responsable du traitement :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à la CNIL, au plus tôt et dans un délai maximal de 72h.

3/**Si la violation entraîne un risque élevé** pour les droits et libertés des personnes concernées, le responsable du traitement :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à la CNIL, au plus tôt et dans un délai maximal de 72h ;
- doit communiquer la violation aux personnes concernées, au plus tôt.

➔**Dans tous les cas** : l'organisme doit identifier la cause et les conséquences de la violation de données afin de mettre en œuvre les mesures adéquates pour encadrer le risque et s'assurer que la violation ne se reproduise plus.

OBLIGATION DE SÉCURITÉ

Exemples :

1/Un cinéma associatif assure la gestion des bulletins de salaire en format papier. Il devra garantir que leur stockage soit sécurisé, notamment dans un espace (armoire, etc.) fermant à clés. Seules les membres de l'association en charge de la gestion RH des salariés pourront posséder cette clé.

2/Dans le cadre de sa politique sociale et culturelle, une municipalité demande à un cinéma associatif la liste et les coordonnées des abonnés résidant de la commune. Une commune ne peut pas demander, même lorsqu'elle accorde une subvention à une association, la liste nominative de ses adhérents. La communication de ces données constituerait un traitement illicite du cinéma associatif.

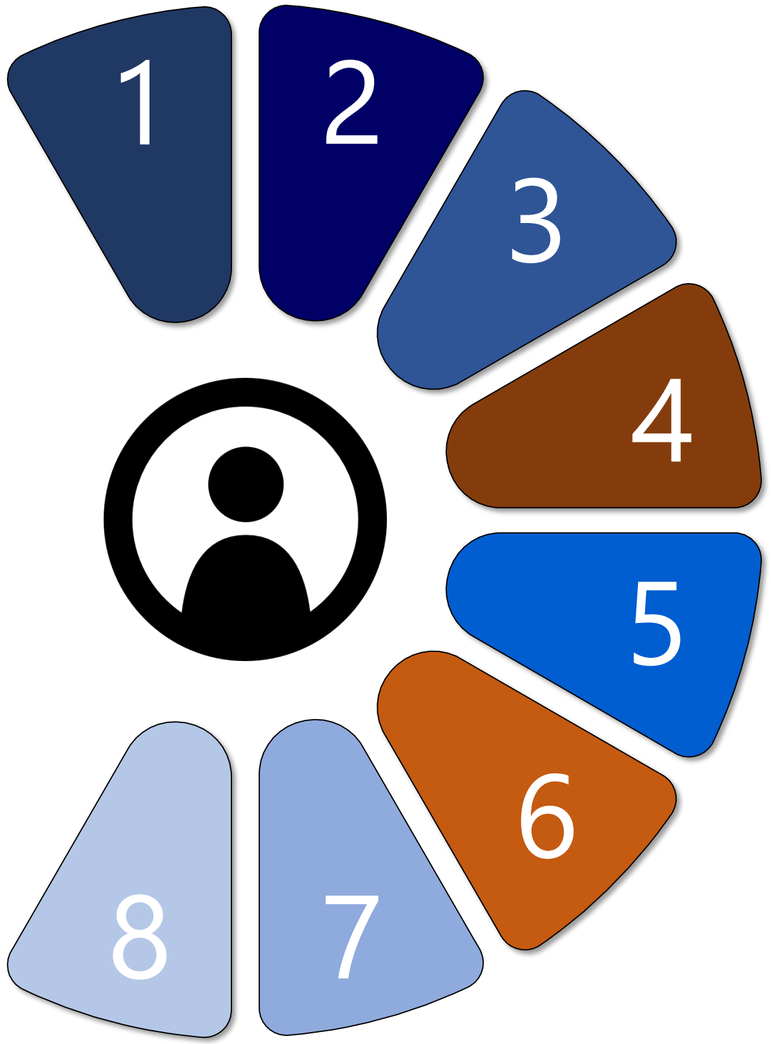
3/Dans le cadre de l'organisation de son activité, un cinéma associatif communique le planning mensuel des bénévoles dans une conversation de groupe sur un système de messagerie instantané. Il serait préférable de renvoyer les bénévoles membres de la conservation sur un espace de partage de documents sécurisé.

4/Tous les comptes utilisateurs ont fait l'objet d'un accès et d'une extraction de données (identité, coordonnées, informations bancaires) non autorisés sur le site web d'un cinéma associatif. Il pourrait s'agir d'une violation de données présentant un risque élevé (arnaques, fraudes, etc.). Dans ce cas, l'organisme devrait documenter la violation, notifier celle-ci à la CNIL et informer les personnes concernées.

Plan de la présentation

1. Présentation de la CNIL
2. Présentation du RGPD
3. Notions clés
4. Recours à un sous-traitant et désignation d'un DPO
5. Principes du RGPD
6. **Information des personnes et exercice des droits**
7. Mesures à mettre en œuvre et documentation obligatoire

DROITS DES PERSONNES



1. Information
2. Accès
3. Rectification
4. Effacement
5. Opposition
6. Limitation
7. Portabilité des données
8. Décision individuelle automatisée

L'INFORMATION DES PERSONNES

La personne concernée par un traitement de données à caractère personnel doit recevoir une **information** délivrée de **façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.**

L'INFORMATION DES PERSONNES

A quel moment le responsable de traitement est tenu d'informer les personnes concernées ?

COLLECTE DIRECTE DES DONNÉES

- **Dès que possible avant la collecte** des données,
- **Au plus tard : au moment de la collecte** des données personnelles.

COLLECTE INDIRECTE DES DONNÉES

- **Principe :**
  - Dès que possible,
  - Au plus tard dans un délai d'un mois.

- **Exceptions au délai d'un mois :**
  - Si les données sont utilisées pour communiquer avec la personne concernée : au plus tard lors de la première communication avec celle-ci ;
  - Si les informations sont communiquées à un autre destinataire : au plus tard lorsque les données sont communiquées pour la première fois.

L'INFORMATION DES PERSONNES

Quelles informations fournir aux personnes concernées ?

➢ **Dans tous les cas :**

- L'identité et coordonnées du **responsable du traitement** des données ;
- Les **finalités** du traitement ;
- La **base légale** du traitement de données ;
- Le **caractère obligatoire ou facultatif du recueil des données** et **les conséquences** pour la personne en cas de non-fourniture des données ;
- Les **destinataires** ou catégories de destinataires des données ;
- La **durée de conservation** des données (ou les critères permettant de la déterminer) ;
- Les **droits des personnes** concernées ;
- Les **coordonnées du délégué à la protection** des données de l'organisme, s'il a été désigné, ou d'un **point de contact** sur les questions de protection des données personnelles ;
- Le **droit d'introduire une réclamation auprès de la CNIL.**

L'INFORMATION DES PERSONNES

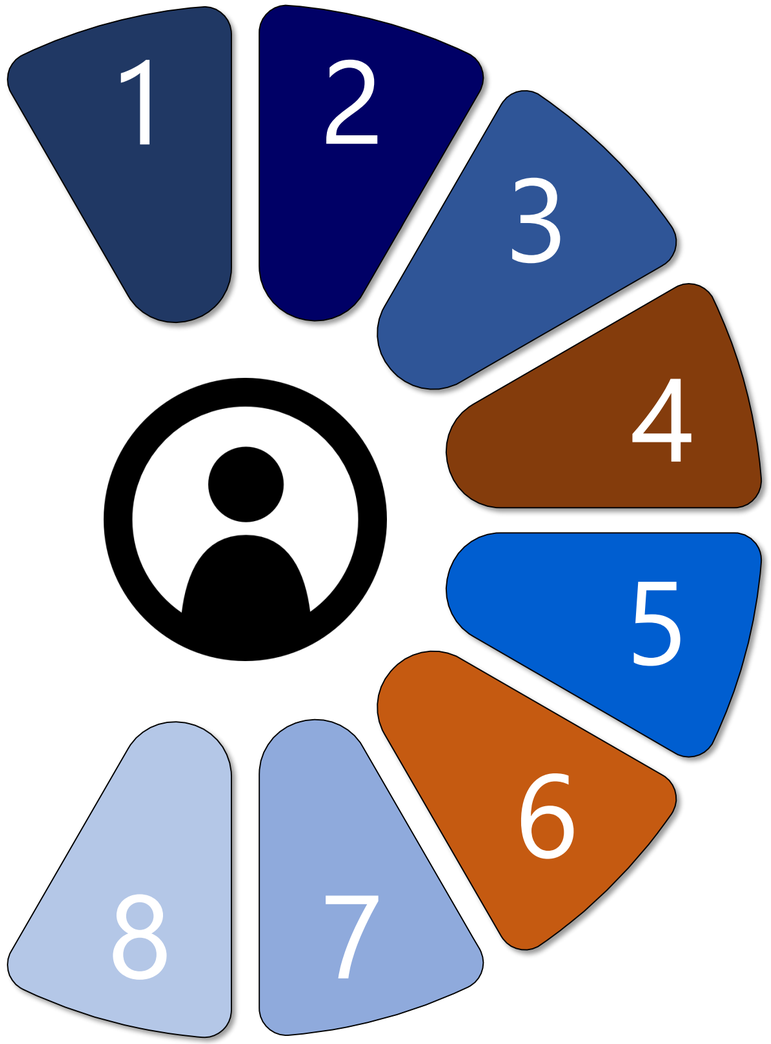
➢ **Selon les cas :**

- les intérêts légitimes poursuivis par le responsable du traitement si le traitement est fondé sur la base légale de l'intérêt légitime ;
- le fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat ;
- l'existence d'un transfert des données vers un pays hors Union européenne (ou vers une organisation internationale), les garanties associées à ce transfert et la faculté d'accéder aux documents autorisant ce transfert ;
- l'existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée ;
- le droit au retrait du consentement à tout moment, si le base légale du traitement est le consentement des personnes ;
- les autres droits applicables au traitement, en fonction de sa base légale : droit d'opposition et droit à la portabilité.

➢ **En cas de collecte indirecte :**

- les catégories de données recueillies ;
- la source des données (en indiquant notamment si elles sont issues de sources accessibles au public).

LES DROITS DES PERSONNES



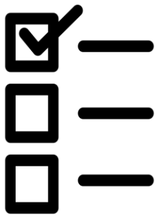
1. Information
2. **Accès**
3. **Rectification**
4. **Effacement**
5. **Opposition**
6. **Limitation**
7. **Portabilité des données**
8. **Décision individuelle automatisée**

Plan de la présentation

1. Présentation de la CNIL
2. Présentation du RGPD
3. Notions clés
4. Recours à un sous-traitant et désignation d'un DPO
5. Principes du RGPD
6. Information des personnes et exercice des droits
7. **Mesures à mettre en œuvre et documentation obligatoire**
8. Exemple pratique

LES MESURES ET LA DOCUMENTATION À METTRE EN ŒUVRE

Le registre des activités de traitement



L’analyse d’impact relative à la protection des données (AIPD)

LE REGISTRE DE TRAITEMENT

Description du traitement	
Nom du traitement	Gestion de la paie
N° / RÉF	1 - Exemple
Date de création du traitement	26/05/2018
Mise à jour du traitement	13/05/2019

Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement	Louise DUPONT	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	exemple1@ets.com
Délégué à la protection des données	Martin HENRI	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	exemple2@ets.com
Société du DPO (si celui-ci est externe)	N/A						

Finalité(s) du traitement effectué	
Finalité principale	Gestion de la paie
Sous-finalité 1	Calcul des rémunérations
Sous-finalité 2	Calcul du montant des versements adressés aux organismes sociaux
Sous-finalité 3	Ordre de virement à la banque

Catégories de données personnelles concernées	Description	Durée de conservation
État civil, identité, données d'identification, images...	Noms, prénoms, adresses	5 ans à compter du versement de la paie
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	RIB	5 ans à compter du versement de la paie
Numéro de Sécurité Sociale (ou NIR)	Numéros de sécurité sociale des salariés	5 ans à compter du versement de la paie

Catégories de personnes concernées	Description	Précisions
Catégorie de personnes 1	Salariés	

Destinataires	Type de destinataire	Précisions
Destinataire 1	Service interne qui traite les données	Dir. Administrative et Financière
Destinataire 2	Partenaires institutionnels ou commerciaux	Organismes sociaux
Destinataire 3	Destinataires dans des pays tiers ou organisations internationa	Banque d'Andorre

Mesures de sécurité	Type de mesure de sécurité	Précisions
Mesure de sécurité 1	Mesures de protection des logiciels	
Mesure de sécurité 2	Sauvegarde des données	
Mesure de sécurité 3	Contrôle d'accès des utilisateurs	

Transferts hors UE	Destinataire	Pays	Type de Garanties	Liens vers la documentation
Organisme destinataire 1	Banque d'Andorre	Andorre	Clauses contractuelles types (CCT)	Contrat en date du 23/01/2018

Retrouvez le modèle sur cnil.fr

CNIL.

LE REGISTRE DE TRAITEMENT

La tenue d'un registre est obligatoire :

- pour les organismes ayant **plus de 250 salariés/agents** ;
- si le traitement des données est susceptible de comporter un **risque pour les droits et libertés** des personnes concernées ;
- si le traitement des données n'est pas **occasionnel** ;
- si le traitement des données porte notamment sur **des catégories particulières de données** (données sensibles (santé, religion etc.) ou relatives aux infractions).

LE REGISTRE DE TRAITEMENT

A quoi sert le registre de traitement ?

- recenser les traitements ;
- disposer d'une vue d'ensemble des traitements de données personnelles dans l'organisme ;
- s'assurer de la conformité de chacun des traitements.

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Que contient une AIPD ?

1. **La description détaillée** du traitement mis en œuvre ;

2. **L'évaluation de la conformité aux principes juridiques** ;

3. **L'étude technique** des risques sur la sécurité des données, ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Dans quels cas la réaliser une AIPD ?

Obligatoire

- **Risques élevés : 2/9 critères**
  - *Évaluation/scoring*
  - *Décision automatique avec effet légal*
  - *Surveillance systématique*
  - *Données sensibles/hautement personnel*
  - *Large échelle*
  - *Croisement de données*
  - *Personnes vulnérables*
  - *Usage innovant*
  - *Blocage d'un droit/contrat*
- **Liste publiée par la CNIL**

MISE EN CONFORMITÉ : PAR OÙ COMMENCER ?

LES PREMIÈRES ACTIONS À MENER :

1. Recensez les traitements
2. Faites le tri dans les données
3. Faites preuve de transparence
4. Organisez et facilitez l'exercice des droits des personnes
5. Sécurisez les données

BOITE À OUTILS, RGPD ET TRAVAIL

- Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales ;

- Guide du recrutement ;

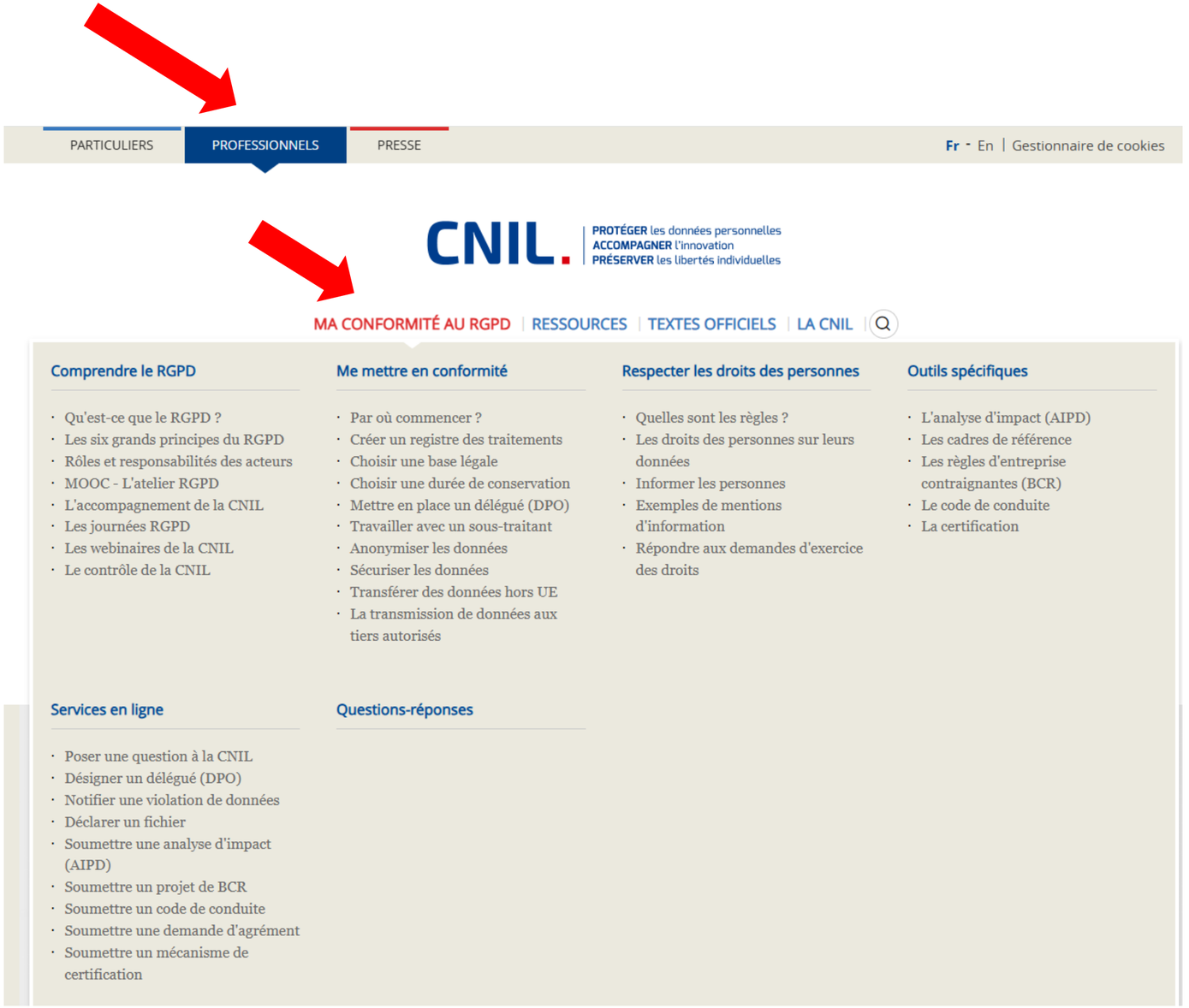
- Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel ;

- Guide de sensibilisation au RGPD pour les associations.

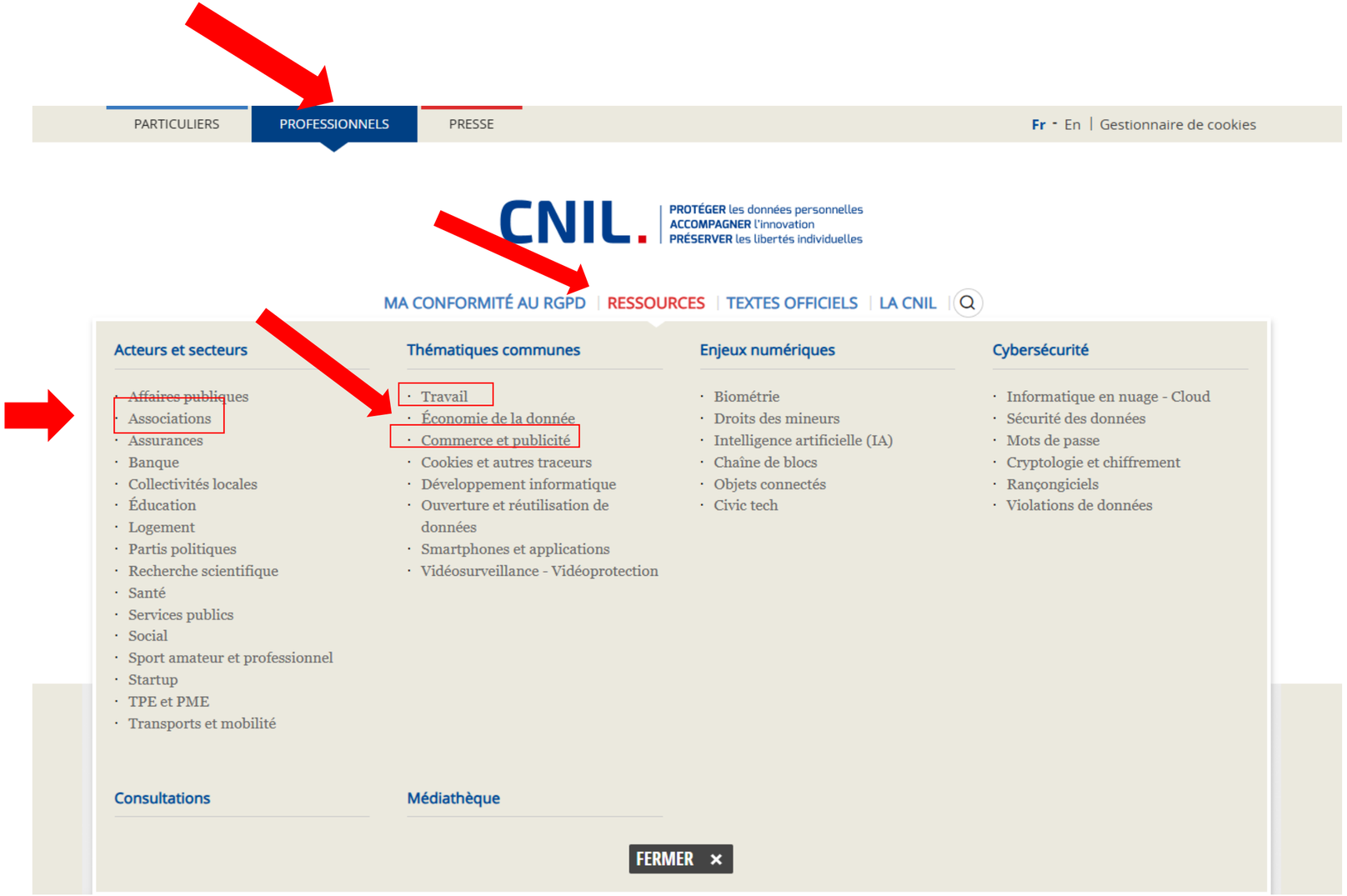
guide de la sécurité des données personnelles

➔Une formation en ligne gratuite, illimitée et ouverte à tous : **le MOOC**.

RESSOURCES


PARTICULIERS
PROFESSIONNELS
PRESSE
Fr - En | Gestionnaire de cookies
CNIL.
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles
MA CONFORMITÉ AU RGPD | RESSOURCES | TEXTES OFFICIELS | LA CNIL
Comprendre le RGPD
Qu'est-ce que le RGPD ?
Les six grands principes du RGPD
Rôles et responsabilités des acteurs
MOOC - L'atelier RGPD
L'accompagnement de la CNIL
Les journées RGPD
Les webinaires de la CNIL
Le contrôle de la CNIL
Me mettre en conformité
Par où commencer ?
Créer un registre des traitements
Choisir une base légale
Choisir une durée de conservation
Mettre en place un délégué (DPO)
Travailler avec un sous-traitant
Anonymiser les données
Sécuriser les données
Transférer des données hors UE
La transmission de données aux tiers autorisés
Respecter les droits des personnes
Quelles sont les règles ?
Les droits des personnes sur leurs données
Informer les personnes
Exemples de mentions d'information
Répondre aux demandes d'exercice des droits
Outils spécifiques
L'analyse d'impact (AIPD)
Les cadres de référence
Les règles d'entreprise contraignantes (BCR)
Le code de conduite
La certification
Services en ligne
Poser une question à la CNIL
Désigner un délégué (DPO)
Notifier une violation de données
Déclarer un fichier
Soumettre une analyse d'impact (AIPD)
Soumettre un projet de BCR
Soumettre un code de conduite
Soumettre une demande d'agrément
Soumettre un mécanisme de certification
Questions-réponses

RESSOURCES


PARTICULIERS
PROFESSIONNELS
PRESSE
Fr - En | Gestionnaire de cookies
CNIL.
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles
MA CONFORMITÉ AU RGPD | RESSOURCES | TEXTES OFFICIELS | LA CNIL
Acteurs et secteurs
Affaires publiques
Associations
Assurances
Banque
Collectivités locales
Éducation
Logement
Partis politiques
Recherche scientifique
Santé
Services publics
Social
Sport amateur et professionnel
Startup
TPE et PME
Transports et mobilité
Thématiques communes
Travail
Économie de la donnée
Commerce et publicité
Cookies et autres traceurs
Développement informatique
Ouverture et réutilisation de données
Smartphones et applications
Vidéosurveillance - Vidéoprotection
Enjeux numériques
Biométrie
Droits des mineurs
Intelligence artificielle (IA)
Chaîne de blocs
Objets connectés
Civic tech
Cybersécurité
Informatique en nuage - Cloud
Sécurité des données
Mots de passe
Cryptologie et chiffrement
Rançongiciels
Violations de données
Consultations
Médiathèque
FERMER