



# LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

## CE QU'IL FAUT RETENIR

À compter du 25 mai 2018, **les adhérents de la FFB n'auront plus**, sauf exception, à **déclarer leurs traitements de données personnelles à la CNIL**.

Mais **ils devront, pour assurer leur conformité** avec les exigences du RGPD **(I)** :

- ▶ **Identifier leurs traitements** (notamment grâce à **la liste des traitements courants annexée à la fiche n° 1**).
- ▶ **Les répertorier dans un registre dédié (II)** (voir modèle de la CNIL).
- ▶ **Réaliser des analyses d'impact avant de mettre en œuvre des traitements comportant un risque élevé pour les droits des individus (III)**, si le traitement envisagé réunit **au moins 2 des 9** critères dégagés au niveau européen, via le logiciel PIA développé par la CNIL, voire consulter la CNIL si l'analyse d'impact laisse apparaître un risque pour les droits des individus.

Le RGPD prévoit des **garde-fous en cas de destruction, altération, accès non autorisé, divulgation non intentionnelle, etc. (IV)**, à la charge des entreprises. Il faudra :

- ▶ Identifier et corriger la faille de sécurité sur le plan technique (en s'adressant, si besoin est au sous-traitant informatique).
- ▶ Conserver l'historique de la faille de sécurité et l'enregistrer sur un registre interne des failles de sécurité.
- ▶ Porter plainte (notamment en cas d'attaque informatique).
- ▶ Déclarer le sinistre à son assureur.
- ▶ Soit, notifier la violation à la CNIL et informer les personnes concernées.

Ces 40 dernières années, le droit des données personnelles a été relativement simple : les responsables de traitement (entreprises, syndicats, organismes publics, etc.) déclaraient simplement à la CNIL le traitement qu'ils voulaient mettre en œuvre, à charge pour eux d'informer ensuite les personnes concernées sur les modalités dudit traitement et de leurs droits en matière de protection des données.

Le règlement général sur la protection des données (RGPD) vient bouleverser cette logique : les obligations administratives (déclaration préalable, autorisation) sont quasiment toutes supprimées et sont remplacées par un principe de responsabilisation des acteurs (*accountability* en anglais)<sup>1</sup>.

**Ce principe implique l'obligation pour chaque adhérent de la FFB (responsables de traitement) de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer (et pouvoir démontrer) que le traitement est effectué dans les règles :**

- ▶ Mise en place de règles, d'outils et de bonnes pratiques pour garantir à tout instant le respect du RGPD et instauration d'audits réguliers pour en assurer l'efficacité (protection des données dès la conception et protection des données par défaut) **(I)**.
- ▶ Tenue d'un registre des traitements **(II)**.
- ▶ Réalisation d'analyses d'impact pour les traitements les plus sensibles **(III)**.
- ▶ Respect de la procédure applicable en cas de faille de sécurité **(IV)**.

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

### I. - PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PROTECTION DES DONNÉES PAR DÉFAUT

Concepts instaurés par le RGPD<sup>2</sup>, la protection des données dès la conception (*privacy by design*) et la protection des données par défaut (*privacy by default*) doivent être maîtrisées par les adhérents de la FFB afin de démontrer leur respect du principe de responsabilisation évoqué en introduction.

- ▶ **Privacy by design** : les projets menés par les adhérents (par exemple : nouveaux outils, produits, applications, services, mesures internes) doivent intégrer les exigences liées à la protection des données, **dès leur origine et tout au long de leur durée**.

Plus concrètement, chaque adhérent FFB doit :

- ▶ identifier les données personnelles strictement nécessaires à la réalisation du traitement;
  - ▶ fixer des durées maximales de conservation des données raisonnables et adaptées aux finalités poursuivies (la CNIL a fourni de nombreux exemples : voir le **tableau en annexe de la fiche n° 1**);
  - ▶ déterminer qui, au sein de la structure, a accès à quels types d'informations et dans le cadre de quelles catégories de traitements;
  - ▶ nommer, si cela est nécessaire, un délégué à la protection des données<sup>3</sup>;
  - ▶ assurer au maximum, dans le cadre de la mise en œuvre du traitement, la confidentialité et la sécurité des données (par exemple : pseudonymisation ou anonymisation des données, cryptage des ordinateurs, méthodes d'identification et d'authentification des utilisateurs, gestion des droits informatiques, mécanismes de traçabilité des accès et des traitements sur les données, mise en place d'une charte informatique et d'outils de formation du personnel, verrouillage des fichiers sensibles par un mot de passe, fermeture à clé des locaux stratégiques, sécurisation des échanges internes et externes, gestion des incidents, mise à jour des postes de travail et installation d'antivirus);
  - ▶ élaborer un cahier des charges récapitulant les exigences à respecter pour chaque projet;
  - ▶ tenir un registre des activités de traitement et réaliser des analyses d'impact (voir ci-après);
  - ▶ mettre en place des mécanismes de contrôles réguliers de l'efficacité et du respect des règles internes de protection des données;
  - ▶ appliquer en interne, si possible, un code de conduite approuvé par la CNIL<sup>4</sup>;
  - ▶ obtenir, si possible, une certification approuvée par la CNIL<sup>5</sup> (plus de détails sur les certifications existantes sur : <https://www.cnil.fr/fr/les-labels-cnil>).
- ▶ **Privacy by default** : les adhérents FFB devront également prendre les mesures organisationnelles et techniques garantissant que, par défaut, seules seront traitées les données nécessaires aux finalités du traitement.

Il faudra donc limiter au minimum :

- ▶ la quantité des données collectées (par exemple : indication des champs obligatoires sur les formulaires);
- ▶ l'étendue du traitement effectué;
- ▶ la durée de conservation des données;
- ▶ le nombre de personnes ayant accès aux données collectées.

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

**Fiche  
n° 3**

### II. - LE REGISTRE DES ACTIVITÉS DE TRAITEMENT

Comme évoqué en introduction, le RGPD a quasiment supprimé toutes les obligations déclaratives à la charge des adhérents FFB<sup>6</sup>.

En contrepartie, ces derniers (de même que leurs sous-traitants<sup>7</sup>) devront répertorier les traitements mis en œuvre dans un registre des activités de traitement<sup>8</sup> et le tenir à jour.

Le registre peut être fait sous format électronique ou papier et doit être tenu à disposition de la CNIL en cas de contrôle.

Le contenu du registre est le suivant :

REGISTRE D'UN RESPONSABLE DE TRAITEMENT	REGISTRE D'UN SOUS-TRAITANT
<ul style="list-style-type: none"> <li>▶ Nom et coordonnées du responsable de traitement.</li> <li>▶ Le cas échéant, nom et coordonnées de son représentant et de son délégué à la protection des données.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Nom et coordonnées du sous-traitant.</li> <li>▶ Le cas échéant, nom et coordonnées de son représentant et de son délégué à la protection des données.</li> </ul>
	<ul style="list-style-type: none"> <li>▶ Nom et coordonnées du ou des responsables de traitement et de leur représentant.</li> </ul>
<ul style="list-style-type: none"> <li>▶ Finalités du traitement.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Catégories de traitements.</li> </ul>
<ul style="list-style-type: none"> <li>▶ Catégories de personnes concernées (clients, employés, membres adhérents, etc.).</li> </ul>	
<ul style="list-style-type: none"> <li>▶ Catégories de données à caractère personnel.</li> </ul>	
<ul style="list-style-type: none"> <li>▶ Catégories de destinataires des données personnelles (personnes, services internes, sous-traitants, partenaires commerciaux, etc.).</li> </ul>	
<ul style="list-style-type: none"> <li>▶ Transferts des données en dehors de l'Union européenne et attestation de l'existence de garanties appropriées.</li> </ul>	
<ul style="list-style-type: none"> <li>▶ Durée de conservation des données</li> </ul>	
<ul style="list-style-type: none"> <li>▶ Description générale des mesures de sécurité techniques et organisationnelles mises en œuvre dans le cadre du traitement (<i>privacy by design</i>)</li> </ul>	

#### Quelles sont les étapes d'élaboration du registre des activités de traitement ?

1. Réaliser un audit des traitements mis en œuvre au sein de la structure de l'adhérent FFB (**voir liste des traitements les plus courants en annexe de la fiche n° 1**).
2. Élaborer un modèle de registre (voir **modèle ci-après**).
3. Déterminer en interne les modalités de remplissage du registre. Qui ? Quand ? Comment ?
4. Remplir le registre en fonction des informations obtenues dans le cadre du point 1.
5. Mettre à jour régulièrement le registre (modification d'un traitement existant ou ajout d'un nouveau traitement).

#### Les petites structures sont-elles exemptées de tenir le registre des activités de traitement ?

Le RGPD prévoit que la tenue du registre n'est pas obligatoire pour les entreprises ou organisations de moins de 250 salariés.



# LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

**Fiche  
n° 3**

## Modèle de fiche du registre

Description du traitement							
Nom / sigle							
N° / REF ref-000							
Date de création							
Mise à jour							
Acteurs							
Nom		Adresse		CP	Ville	Pays	Tel
Responsable du traitement							
Délégué à la protection des données							
Représentant							
Responsable(s) com@int(s)							
Finalité(s) du traitement effectué							
Finalité principale							
Sous-finalité 1							
Sous-finalité 2							
Sous-finalité 3							
Sous-finalité 4							
Sous-finalité 5							
Mesures de sécurité							
Mesures de sécurité techniques							
Mesures de sécurité organisationnelles							
Catégories de données personnelles concernées		Description				Délai d'effacement	
Etat civil, identité, données d'identification, images...							
Vie personnelle (habitudes de vie, situation familiale, etc.)							
Informations d'ordre économique et financier (revenus, situation financière, données de connexion (adresse IP, logs, etc.)							
Données de localisation (déplacements, données GPS, GSM, etc.)							
Données sensibles		Description				Délai d'effacement	
Données révélant l'origine raciale ou ethnique							
Données révélant les opinions politiques							
Données révélant les convictions religieuses ou philosophiques							
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 l'orientation sexuelle							
Données relatives à des condamnations pénales ou infractions							
Numéro d'identification nationale unique (NIR pour la France)							
Catégories de personnes concernées		Description					
Catégorie de personnes 1							
Catégorie de personnes 2							
Destinataires		Description		Type de destinataire			
Destinataire 1							
Destinataire 2							
Destinataire 3							
Destinataire 4							
Transferts hors UE		Destinataire		Pays		Type de Garanties	Lien vers le doc
Organisme destinataire 1							
Organisme destinataire 2							
Organisme destinataire 3							
Organisme destinataire 4							

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

### III. – L'ANALYSE D'IMPACT

#### Qu'est-ce que c'est ?

Le RGPD instaure également l'obligation pour les responsables de traitement (et donc, pour les adhérents FFB) de réaliser une analyse d'impact des traitements présentant un risque élevé pour les droits et libertés des personnes physiques.

L'analyse doit permettre d'évaluer les conséquences des traitements envisagés pour les droits et libertés des personnes physiques, les risques encourus (par exemple : atteinte au droit à la vie privée, vol, destruction, altération ou accès non autorisé aux données traitées) ainsi que les mesures destinées à réduire les risques identifiés.

L'analyse d'impact doit avoir lieu **avant** la mise en œuvre du traitement concerné.

#### Dans quels cas faut-il faire une analyse d'impact ?

Le G29 (organe consultatif représentant les autorités de contrôle des pays de l'Union européenne, dont la CNIL) a mis en place 9 critères permettant de déterminer si une analyse d'impact doit être réalisée ou non<sup>9</sup>.

Si **au moins 2 des 9** critères détaillés ci-après sont réunis, il faudra faire une analyse d'impact :

<b>1. Évaluation ou notation de la personne physique</b>	<p>Elles permettent, notamment via le profilage ou l'analyse prédictive, d'évaluer ou de noter le rendement de la personne au travail, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, sa localisation ou ses déplacements.</p> <p>Cas les plus courants : gestion des ressources humaines, profilage marketing, etc.</p>
<b>2. Prise de décision automatisée avec effet juridique ou effet similaire significatif</b>	<p>Le traitement a pour objet de prendre une décision à l'égard d'une personne (par exemple : licenciement, refus de fournir un bien ou un service, exclusion d'un groupe).</p> <p>Ce critère ne s'applique pas si la décision n'a pas ou peu d'effet pour la personne concernée.</p>
<b>3. Surveillance systématique</b>	<p>Le traitement permet d'observer, de surveiller ou de contrôler les personnes (par exemple : vidéosurveillance, géolocalisation, contrôle de l'usage des outils informatiques).</p>
<b>4. Données sensibles ou à caractère hautement personnel</b>	<p>Il s'agit :</p> <ul style="list-style-type: none"> <li>▶ des données particulières<sup>10</sup> (opinions politiques, syndicales, philosophiques, race, religion, santé, vie et orientation sexuelle...),</li> <li>▶ des données relatives aux condamnations et infractions pénales<sup>11</sup>,</li> <li>▶ des données liées à des activités domestiques et privées (par exemple : communications électroniques d'une personne), ayant un impact sur un droit fondamental de la personne concernée (par exemple : données de localisation) ou dont la violation aurait des incidences graves pour la personne concernée (par exemple : informations financières).</li> </ul> <p>Le caractère sensible peut être amoindri quand les données sont publiquement disponibles (par exemple : agendas, courriers électroniques, documents).</p>

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

<b>5. Données traitées à grande échelle</b>	<p>Le RGPD ne définit pas cette notion.</p> <p>L'adhérent FFB devra donc prendre en compte, pour déterminer si le critère est rempli ou non :</p> <ul style="list-style-type: none"> <li>▶ Le nombre de personnes concernées, en valeur absolue ou en proportion de la population considérée (par exemple : une part significative, des effectifs, des clients).</li> <li>▶ Le volume de données et/ou l'éventail des différents éléments de données traitées.</li> <li>▶ La durée ou la permanence de l'activité de traitement de données</li> <li>▶ L'étendue géographique de l'activité de traitement.</li> </ul>
<b>6. Croisement ou combinaison d'ensembles de données</b>	<p>Les données utilisées proviennent, par exemple, de différents traitements, réalisés pour des finalités différentes, par plusieurs responsables de traitement, d'une façon qui n'était pas raisonnablement prévue par la personne concernée.</p>
<b>7. Données concernant des personnes vulnérables</b>	<p>Les personnes vulnérables sont placées dans une relation déséquilibrée avec le responsable de traitement, ce qui bride leur capacité à consentir librement ou à s'opposer au traitement, ou à exercer leurs droits.</p> <p><b>Exemples</b> : enfants, employés, personnes fragiles (demandeurs d'emploi ou d'asile, malades mentaux, personnes âgées, patients, etc.) et toutes autres personnes placées dans une relation déséquilibrée avec le responsable de traitement.</p>
<b>8. Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles</b>	<p>Toute technologie innovante permettant de collecter des données.</p> <p><b>Exemples</b> : utilisation combinée de mécanismes de reconnaissance faciale et des empreintes.</p>
<b>9. Traitements qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat</b>	<p>Opérations permettant notamment d'autoriser, de modifier ou de refuser l'accès à un service ou la conclusion d'un contrat.</p> <p><b>Exemples</b> : banque passant ses clients au crible d'une base de données pour octroyer ou non un crédit; adhérent vérifiant que ses clients ne sont pas inscrits sur son registre des impayés.</p>



**La CNIL peut également dresser une liste de traitements pour lesquels une analyse d'impact est obligatoire (à ce jour, aucune liste n'a été annoncée. À surveiller néanmoins)<sup>12</sup>.**

### Dans quels cas n'est-il pas nécessaire de faire une analyse d'impact ?

Il n'est pas nécessaire de réaliser d'analyse d'impact dans les cas suivants :

- ▶ Lorsque le traitement n'est pas susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (par exemple : le traitement envisagé ne réunit pas au moins 2 des 9 critères évoqués précédemment).
- ▶ Lorsque le traitement est très similaire, en termes de nature, de portée, de contexte et de finalités, à un autre traitement ayant déjà fait l'objet d'une analyse d'impact (les résultats de l'analyse déjà effectuée serviront pour le nouveau traitement envisagé).

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

- ▶ Lorsque le traitement a déjà été soumis à la CNIL (via une déclaration ou une demande d'autorisation) et n'a pas changé depuis dans ses modalités d'exécution.
- ▶ Lorsque le traitement est réalisé en vertu d'une obligation légale.
- ▶ Lorsque le traitement figure dans la liste facultative de la CNIL des traitements n'ayant pas à faire l'objet d'une analyse d'impact (liste non encore parue).

### Qui doit faire l'analyse d'impact ?

Le responsable de traitement (dans la plupart des cas, l'adhérent FFB) doit seulement s'assurer que l'analyse d'impact est réalisée, que ce soit par lui-même ou par un tiers.

S'il en a désigné un, le responsable de traitement demande conseil à son **délégué à la protection des données (DPO)**. Les conseils du DPO sont inscrits dans l'analyse<sup>13</sup>.

Si le traitement est mis en œuvre, en tout ou partie, par un **sous-traitant** (par exemple : prestataire de services informatiques tels que l'hébergement ou la maintenance, intégrateur de logiciels, société de sécurité informatique, agence de marketing ou de communication traitant les données pour le compte de ses clients), celui-ci aide le responsable de traitement à réaliser l'analyse d'impact.

Le responsable de traitement peut également s'appuyer sur des experts indépendants (avocats, experts en informatique, experts en sécurité, etc.).

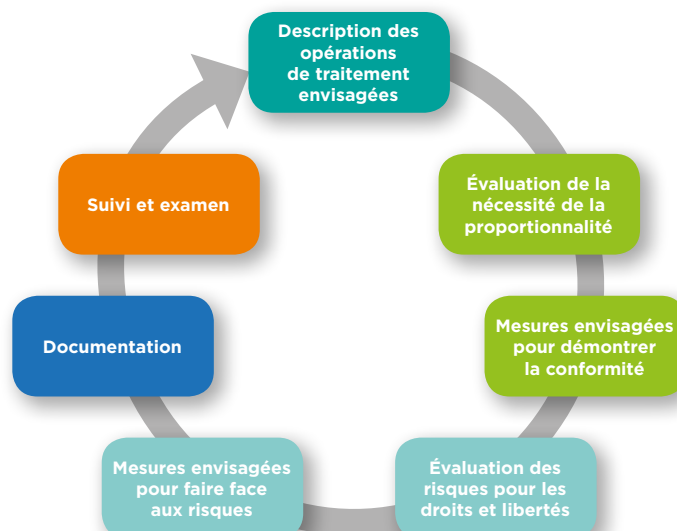
Le responsable de traitement doit, le cas échéant, demander l'avis des personnes concernées ou de leurs représentants<sup>14</sup> (par exemple : institutions représentatives du personnel). Cette consultation peut se faire par tous moyens (questionnaire, étude, enquête, etc.). S'il ne procède pas à la consultation (pour des raisons de confidentialité ou de sécurité, par exemple) ou s'il ne suit pas l'avis des personnes consultées, il faudra qu'il soit en mesure de le justifier.

### Que doit contenir une analyse d'impact ?

Le RGPD exige que l'analyse d'impact contienne au moins :

1. Une description des opérations de traitement envisagées, de leurs finalités et, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement (par exemple : lutte contre la fraude, protection des biens, des personnes et des locaux, prospection commerciale).
2. Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités.
3. Une évaluation des risques pour les droits et libertés des personnes concernées.
4. Les mesures envisagées pour faire face aux risques, y compris les garanties, les mesures et les mécanismes de sécurité visant à assurer la protection des données personnelles et à apporter la preuve du respect du RGPD.

Dans ses lignes directrices sur l'analyse d'impact, le G29 résume le processus d'élaboration de la façon suivante :



## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

### Des outils ou des modèles sont-ils disponibles ?

Oui.

Afin d'aider les structures (et notamment les TPE et les PME) à réaliser les analyses d'impact, la CNIL a élaboré un logiciel dédié, intitulé « Outil PIA ».

Cet outil est disponible – en version bêta – sur le site de la CNIL à l'adresse suivante : <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>.



### Que faire si l'analyse d'impact indique que le risque pour les droits des personnes est particulièrement élevé ?

Il faudra consulter la CNIL<sup>15</sup> et lui transmettre un dossier comprenant :

- ▶ L'analyse d'impact réalisée.
- ▶ Les responsabilités des différents acteurs du traitement envisagé (responsable de traitement, responsables de traitement conjoints et sous-traitants).
- ▶ Les finalités et les moyens du traitement envisagé.
- ▶ Les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées.
- ▶ S'il en a été nommé un, les coordonnées du DPO.
- ▶ Toute autre information requise par la CNIL.

Le logiciel PIA développé par la CNIL devrait permettre de fournir l'essentiel du contenu demandé.

La CNIL aura huit semaines pour répondre à cette consultation (prorogation de six semaines supplémentaires possible). À l'issue du délai, elle rend un avis écrit et peut user des pouvoirs qui lui sont reconnus par le RGPD (interdiction, injonction, etc.).

### Conclusion sur l'analyse d'impact :

Les adhérents FFB devront, pour être en conformité avec le RGPD :

- ▶ Réaliser un audit des traitements en cours ou à venir pour déterminer si une analyse d'impact est nécessaire.
- ▶ Déterminer les modalités pratiques de l'analyse d'impact. Qui ? Quand ? Comment ?
- ▶ Mettre en place une méthodologie appropriée pour faire face aux conséquences de l'analyse.

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

### IV. - LA GESTION DES INCIDENTS DE SÉCURITÉ

Il arrive parfois que, en dépit des précautions prises, les données personnelles soient, de façon accidentelle ou illicite, détruites, perdues, altérées ou divulguées où qu'un tiers non autorisé y ait accès.

#### Que faire dans ces cas-là ?

L'adhérent FFB doit, en principe, en sa qualité de responsable de traitement, notifier la violation des données à la CNIL<sup>16</sup>.



**Il n'est pas nécessaire de procéder à la notification si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques** (par exemple : les données n'ont pas un degré important de sensibilité ou sont illisibles en raison de la mise en place d'un procédé de cryptage).

Par contre, il faudra enregistrer la violation dans un registre dédié.

#### Que doit contenir la notification ?

Le document doit ainsi contenir :

- ▶ 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 ;
- ▶ le nom et les coordonnées du délégué à la protection des données (DPO), ou de tout contact auprès duquel des informations supplémentaires peuvent être obtenues<sup>17</sup> ;
- ▶ les conséquences probables de la violation des données personnelles ;
- ▶ les mesures prises ou que l'adhérent FFB 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.

Il peut arriver que les informations détaillées ci-dessus ne soient pas toutes disponibles au moment de la notification, c'est pourquoi le RGPD autorise à échelonner dans le temps la fourniture des informations requises.



**Il faudra également documenter, dans un registre dédié, toute violation des données à caractère personnel, en décrivant les faits et les mesures qui ont été prises afin de permettre à la CNIL de vérifier que l'adhérent FFB a bien respecté ses obligations.**

#### Existe-t-il un modèle de notification ?

Oui.

La CNIL prévoit déjà un modèle de notification sur <https://www.cnil.fr/fr/vos-demarches-en-ligne>.



**Ce modèle devrait être actualisé prochainement pour prendre en compte le RGPD.**

#### Existe-t-il un modèle de registre des failles de sécurité ?

Non. Cependant, il n'est pas à exclure que la CNIL propose prochainement ce type d'outil.

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

**Fiche  
n° 3**

### Faut-il informer les personnes concernées par les données violées ?

Oui<sup>18</sup>, sauf si :

- ▶ la violation ne présente pas un risque élevé pour les droits et libertés de la personne physique (par exemple : les données ne sont pas sensibles ou ont été cryptées);  
OU
- ▶ l'adhérent FFB a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données personnelles affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès (par exemple : chiffrement);  
OU
- ▶ l'adhérent FFB a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser;  
OU
- ▶ l'information individuelle des personnes concernées exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Dans les cas où les personnes concernées devraient être informées, il faudra au moins fournir, dans un langage clair et simple, les renseignements suivants :

- ▶ nom et coordonnées du délégué à la protection des données (DPO), ou de tout contact auprès duquel des informations supplémentaires peuvent être obtenues<sup>19</sup>;
- ▶ conséquences probables de la violation des données personnelles;
- ▶ mesures prises ou à 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.

**La CNIL peut forcer l'intéressé à procéder à l'information des personnes concernées.**



#### Quid du sous-traitant ?

L'obligation de notification à la CNIL ou d'information des personnes concernées s'imposant au responsable de traitement, le sous-traitant n'a pas à s'en charger.

Cependant, il lui incombera d'informer le responsable de traitement s'il a été victime d'une violation des données et d'aider ce dernier à accomplir ses obligations de notification ou information<sup>20</sup>.

#### Concrètement, que faire ?

- ▶ Application de la procédure interne applicable en cas d'incident :
  - ▶ identifier et corriger la faille de sécurité sur le plan technique (au besoin, s'adresser au sous-traitant);
  - ▶ conserver des renseignements sur la faille de sécurité;
  - ▶ porter plainte (notamment en cas d'attaque informatique);
  - ▶ déclarer le sinistre à l'assureur;
  - ▶ notifier la violation, le cas échéant, à la CNIL;
  - ▶ informer, le cas échéant, les personnes concernées (si besoin est, privilégier des supports de communication de type « communiqué de presse »).
- ▶ Enregistrement de l'incident dans le registre interne des failles de sécurité.

## LA RESPONSABILISATION DES ACTEURS DU TRAITEMENT

Fiche  
n° 3

1. Articles 24, 25, 33 à 39 du RGPD.
2. Article 25 du RGPD.
3. La nomination d'un délégué à la protection des données n'est obligatoire que dans certains cas listés à l'article 37 du RGPD. Cependant, rien n'empêche d'en désigner un de façon volontaire.
4. Article 40 du RGPD. Les codes de conduite doivent encore être réalisés.
5. Article 42 du RGPD.
6. À noter cependant que le projet de loi relatif à la protection des données supprime certes le régime de déclaration, mais instaure une formalité préalable pour les traitements nécessitant l'utilisation du numéro de sécurité sociale.
7. Un sous-traitant, au sens de l'article 4 du RGPD, est la personne physique ou morale, l'autorité publique, le service ou tout organisme qui traite des données à caractère personnel pour le compte du responsable de traitement (par exemple : expert-comptable, fournisseur de solutions logicielles RH ou de relations clients, hébergeur informatique). Voir la fiche n° 4 pour plus de détails.
8. Article 30 du RGPD.
9. Voir lignes directrices du G29 sur l'analyse d'impact, disponibles sur <https://www.cnll.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia>.
10. Données listées à l'article 9 du RGPD.
11. Voir l'article 10 du RGPD.
12. Point 4 de l'article 35 du RGPD.
13. Voir la fiche n° 5 pour en savoir plus sur le rôle du DPO.
14. Point 9 de l'article 35 du RGPD.
15. Article 36 du RGPD.
16. Article 33 du RGPD.
17. D'où l'importance de désigner en interne un référent pour tout ce qui concerne les problématiques de traitement de données personnelles.
18. Article 34 du RGPD.
19. D'où l'importance de désigner en interne un référent pour tout ce qui concerne les problématiques de traitement de données personnelles.
20. Article 28 du RGPD.