Circulaire N° 2157

Paris, le 27 novembre 2017

Direction des Affaires juridiques et fiscales

Rédacteur : Nicolas ROBAUX
nicolas.robaux@coopdefrance.coop

DROIT DE L'ENTREPRISE

OBJET : LA PROTECTION DES DONNEES PERSONNELLES

- **Loi « informatique et libertés » du 6 janvier 1978,**
- **Règlement n°2012/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.**

CE QU'IL FAUT RETENIR

- Le 25 mai 2018, le règlement européen de protection des données à caractère personnel, ci-après appelé « RGPD » (pour *règlement européen sur la protection des données*), entrera en vigueur dans toute l'Union européenne.
  Il reprend toutefois de nombreuses dispositions et concepts déjà présents dans la loi du 6 janvier 1978 dite « informatique et libertés » (ci-après « I&L »).

- Alors que la loi I&L fonctionne sur la base d'une déclaration (dans la majorité des cas) des traitements de données à caractère personnel valant engagement de conformité de la part du responsable de traitement, le RGPD opte pour une démarche de responsabilisation du responsable de traitement. Cette démarche passe par des autocontrôles et une documentation de la conformité par les responsables des traitements mais elle est toutefois assortie de sanctions plus lourdes. Les formalités issues de la loi I&L ont ainsi vocation à disparaître avec l'entrée en vigueur du RGPD.

- Les grandes notions utilisées par la loi I&L (donnée à caractère personnel, traitement, fichier, consentement, responsable de traitement) proviennent déjà du droit européen. Elles ne sont modifiées qu'à la marge par le RGPD.

- Les obligations du responsable de traitement (conformité du traitement, recueil, si besoin, du consentement de la personne, information) ne sont pas modifiées. Les droits des personnes sont toutefois étendus par l'apparition de droits nouveaux.

- Les coopératives mettent en œuvre des traitements de données à caractère personnel, au moins vis-à-vis des salariés et des associés coopérateurs. Des modèles de statuts eux-mêmes découlent un certain nombre d'opérations réalisées par la coopérative sur des données à caractère personnel, chacune constituant un traitement de données à caractère personnel.

- Sont recensées ci-après les différentes opérations sur des données à caractère personnel qui découlent des statuts. Chacune prise indépendamment des autres, constitue un traitement de données à caractère personnel.

Elles peuvent être réalisées sur un outil unique (logiciel de gestion du capital social, tableur Excel…) qui dans ce cas constitue un traitement plus large de données à caractère personnel réalisé pour des finalités plus étendues.

- Les traitements liés à la gestion du sociétariat

Traitement	Source
Liste des associés coopérateurs, classés par date d'adhésion	Article R. 522-2 du CRPM + article 7.6 des modèles de statuts
Extraction des associés coopérateurs inactifs pour radiation ou exclusion	Article 11 bis et 12 des modèles de statuts
Extraction de la liste des associés coopérateurs titulaires des différentes catégories de parts sociales de la liste des associés (parts sociales d'épargne, parts sociales à avantage particulier)	Article 14 des modèles de statuts (option PSAP)
Extraction de la liste des associés non coopérateurs des associés coopérateurs	Article 7.6 des modèles de statuts (option ANC)
Liste des tiers non associés	Article 3 et 46 des modèles de statuts (option TNA)

- Les traitements liés à l'engagement coopératif

Traitement	Source
Liste des associés coopérateurs par objet ou branche d'activité	Article 3 et 8 des modèles de statuts
Traitements nécessaires à la gestion des activités de la coopérative (gestion de la collecte, de l'approvisionnement…)	Article 8 des modèles de statuts
Classement des bulletins d'adhésion, contrat de production, y compris papier	Article 8-2 des modèles de statuts Règlementation OP
Extraction de la liste des associés coopérateurs recevant le document unique récapitulatif, le cas échéant	Article 9 des modèles de statuts
Liste des associés coopérateurs membres des éventuelles organisations de producteurs (OP)	Article 10 des modèles de statuts
Extraction des associés coopérateurs appartenant à une même « branche d'activité »	Article 58 des modèles de statuts

- Les traitements liés à la gouvernance

Traitement	Source
Liste d'émargement aux éventuelles AG de groupes spécialisés	Article 10 des modèles de statuts
Liste des membres du conseil d'administration	Article 21 des modèles de statuts
Liste des membres du conseil de surveillance	Option « Directoire et conseil de surveillance »
Liste des membres du directoire	Option « Directoire et conseil de surveillance »
Liste des membres du bureau	Article 26 des modèles de statuts
Extraction des associés coopérateurs appartenant à une même « branche d'activité »	Article 58 des modèles de statuts
Liste des participants aux assemblées générales	Article 34 et suivants des modèles de statuts
Listes des associés coopérateurs et ANC rattachés aux différentes sections	Article 35 des modèles de statuts– « coopérative à sections »
Liste des délégués des différentes sections	Article 35 des modèles de statuts « coopérative à sections »
Liste des participants à l'assemblée plénière	Article 40 des modèles de statuts– « coopérative à section »
Liste des commissions ou comités non statutaires (Conseils de groupes spécialisés, conseils de filière…)	Règlement intérieur

La protection des données à caractère personnel des personnes physiques est une composante du droit à la vie privée, droit fondamental consacré par la Constitution mais également par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales.

Le régime actuel de la protection des données à caractère personnel, issu de la loi n° 78-17 du 6 janvier 1978 dite « I&L», découle aujourd'hui de textes européens transposés ces dernières décennies notamment la directive 95/46/CE du 24 octobre 1995.

Ainsi, le règlement n° 2016/679, du 27 avril 2016 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel adopté après quatre années de négociation le 14 avril 2016 (« RGPD »), n'opèrera pas une révolution totale car de nombreuses définitions ou obligations se trouvent déjà dans les textes applicables.

A compter du 25 mai 2018, le RGPD sera applicable dans tous les Etats membres de l'Union et bien que certains concepts existent déjà, la philosophie du texte en ce qui concerne la conformité diffère profondément de la loi. Là où la règlementation actuelle se base sur un engagement de conformité lors de la déclaration des traitements de données à caractère personnel, le règlement opte pour une responsabilisation des acteurs et des autocontrôles, assortis de sanctions renforcées. Il opèrera donc un renversement du mécanisme et mettra fin à l'obligation de déclaration. Cela implique que l'entreprise soit désormais le premier garant de la protection des données qu'elle traite.

Cette circulaire a donc pour objet de fournir aux coopératives un guide pratique assorti d'illustrations et d'exemples leur permettant, pour les traitements les plus courants, d'apprécier les risques et les obligations en découlant.

I) Identifier les traitements concernés

Pour se mettre en conformité avec le RGPD, la coopérative devra dans un premier temps recenser les traitements de données à caractère personnel déjà mis en œuvre.

Ces traitements peuvent être recensés dans un tableau unique qui détaille :

- Son (ou ses) responsables (la personne ou le service qui en détermine les finalités et les moyens) ;
- La personne/le service chargé de sa mise en œuvre ;
- Sa (ou ses) finalités ;
- Les données traitées (et la présence de données sensibles) ;
- Les destinataires de ces données (internes ou externes à l'entreprise) ;
- La durée de conservation des données ;
- Le fondement du traitement (consentement donné par la personne, si oui, par quel biais ? Données nécessaires à l'exécution d'un contrat ? Si oui, quel contrat ?) ;
- Les transferts hors UE éventuels.

Il est à ce titre important de cartographier l'ensemble des traitements qui peuvent être mis en œuvre, y compris ceux semblant faire « doublon ».

Exemple de cartographie de traitement :
Une telle cartographie est nécessaire pour savoir où en est la coopérative dans ses traitements et servira, ensuite, de base au registre des traitements.

Traitement	Données	Responsable	Service chargé de la mise en œuvre	Finalités	Destinataires	Durée	Fondement	Données transférées hors de l'UE ?
Liste des adhérents	Nom, prénom, contact, adresse,	Coopérative	Service adhérents	Gestion capital social Envoi des convocations AG	Service « adhérents » Direction	Adhésion + 5 ans	Règlementation (article R. 522-2 du CRPM[1]) Contrat (Engagement coop)	Non
Liste des associés collecte vente « Ovins »	Nom, prénom, contact, adresse, Données éco	Coopérative	Pôle « Ovins »	Gestion de la collecte ovins	Employés filière ovine Entreprise chargée de la collecte	Adhésion + 5 ans	Contrat (Engagement coop)	Non
Liste des associés Appro	Nom, prénom, contact, adresse, Données éco	Coopérative	Pôle « appro »	Gestion des appro	Employés service « Appro » Fournisseurs	Adhésion + 5 ans	Contrat (Engament coop)	Non
Liste des associés	Nom, Prénom, Contacts, RIB	Coopérative	Service comptabilité	Gestion de la facturation	Employés service comptabilité	Adhésion + 5ans	Contrat (Engagement coop)	Non
Collecte à destination d'organisme sanitaire	Nom, prénom, adresse, données sanitaires des associés	Coopérative	Service sanitaire	Cession d'informations à association sanitaire	Association sanitaire	Adhésion	Consentement	Non
Gestion de la paie des salariés de la coopérative	Nom, prénom, données professionnelles	Coopérative	Service RH	Gestion de la paie des employés	Employés RH	Contrat	Loi	Non

Il est également nécessaire d'identifier les traitements qui font l'objet d'une sous-traitance.

La première étape, consiste donc à identifier les traitements concernés par la loi et le règlement.

La loi I&L, de même que le RGPD, s'appliquent :

- aux **traitements automatisés de données à caractère personnel,**
- aux traitements non automatisés de données à caractère personnel contenues ou appelées à **figurer dans des fichiers,..**

… à la condition, dans le cas de la loi, que le responsable de traitement soit établi en France et, dans le cas du RGPD, qu'il soit mis en œuvre par un responsable ou un sous-traitant, établi dans l'Union européenne ou produise des effets dans l'Union européenne.

A- La notion de donnée à caractère personnel

La définition de la donnée à caractère personnel est complexe. Cette notion est vaste et englobe un grand nombre de données.

La loi I&L la définit ainsi à l'article 2 :

> *« Constitue une donnée à caractère personnel* ***toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement,*** *par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de* ***considérer l'ensemble des moyens en vue de permettre son***

[1] Code rural et de la pêche maritime

identification dont dispose ou auxquels peut avoir accès le responsable du traitement *ou toute autre personne. »*

Sont donc des données à caractère personnel les informations relatives à une personne physique :

- **Identifiée**, par le biais de son nom. Ainsi, toutes les informations qui suivent le nom d'une personne sont réputées personnelles car se rattachant à ce nom.

- **Identifiable**, directement ou indirectement, par référence à d'autres éléments. Il s'agit de la théorie du recoupement. Il est donc nécessaire, en présence de données anonymisées, de s'interroger sur la possibilité d'une identification indirecte de la personne concernée qui confèrerait un caractère personnel à ces données[2].

ILLUSTRATION : l'associé coopérateur identifiable

Une coopérative qui recense dans un fichier les parcelles exploitées par ses associés coopérateurs, mais sans les noms de ces derniers, peut être concernée.

En effet, le nom de la commune, le numéro cadastral, référencement PAC et la production réalisée sur ces parcelles peuvent, dans certains cas permettre, par déduction et recoupement, de deviner qui sont les associés coopérateurs concernés. Dans ce cas, la personne devenant identifiable et l'ensemble des données la concernant acquiert la qualification de données à caractère personnel.

Cette théorie du recoupement et de la personne physique identifiée ou identifiable est reprise également par le RGPD qui ne modifie donc pas la définition de donnée à caractère personnel.

Il la définit (article 4 RGPD) comme :

« toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable » une ***personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant,*** *tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».*

Il est également indispensable de ne pas s'arrêter à la notion de « personne physique » et de ne pas exclure, de fait, toutes les informations se rapportant à des **personnes morales.**

En effet, si les données relatives exclusivement aux personnes morales ne sont pas couvertes par ces définitions (raison sociale, adresse du siège social, numéro SIRET…), des informations relatives à des personnes physiques peuvent s'y retrouver, telles que des noms (gérants, associés, directeurs) ou autres données permettant l'identification.
Toutes les informations relatives à ces personnes physiques (adresses personnelles, poste dans l'entreprise, adresse mail) **acquièrent dès lors la qualification de données à caractère personnel.**

[2] L'analyse des circonstances du traitement (contexte et objet) est donc déterminante. Comme le notait par exemple le G29, organe consultatif européen sur la protection des données, si un nom de famille ne permet pas l'identification d'une personne à l'échelle nationale, il le permet à l'échelle d'une classe de 25 élèves.
Voir en ce sens TGI Paris, ord. réf., 22 sept. 2008 : décision d'espèce qui estime que la seule collecte de noms de famille ne suffit pas à l'application de la loi car n'est pas démontré le fait qu'une identification reste possible par le recoupement des fichiers noms et prénoms.

Ainsi, la Commission Nationale de l'Informatique et des Libertés (ci-après « CNIL ») a estimé[3], à propos d'un fichier d'entreprises qu'il convenait d'appliquer la loi de 1978 pour l'exercice du droit d'accès *« aux personnes physiques représentants légaux des entreprises, dès lors que le nom de ces personnes figure dans le fichier en tant que dirigeant, actionnaire ou associé »*, bien qu'il s'agisse en principe d'informations relatives aux entreprises.

ILLUSTRATION : associés coopérateurs sous forme sociétaire ou individuelle Les associés coopérateurs peuvent être des exploitants individuels ou des exploitants sous forme sociétaire. Le registre des associés coopérateurs que les coopératives doivent tenir à jour comporte donc des raisons sociales de sociétés, accompagnées des noms des exploitants. Quand bien même ces noms seraient des données accessibles sur Infogreffe, il n'en reste pas moins qu'elles concernent des personnes physiques et sont, de ce fait, des données à caractère personnel.

B- La notion de traitement de données à caractère personnel

La loi I&L s'applique :

- aux **traitements automatisés** de données à caractère personnel,
- aux **traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers,**

Ces notions sont définies à l'article 2 de la loi I&L :

> *Constitue un traitement de données à caractère personnel* ***toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé****, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.*
>
> *Constitue un* ***fichier de données à caractère personnel*** *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.*

La notion de traitement de données à caractère personnel est donc extrêmement large. Elle a en effet vocation à englober, aux termes des deux textes, ***« toute opération ou tout ensemble d'opérations »*** portant sur de telles données, quel que soit le procédé utilisé et vise autant la collecte par le biais d'un site internet, d'un formulaire d'inscription que la saisie de données sur un tableur informatique. La notion de traitement est polymorphe et faite pour s'adapter aux innovations technologiques.

Le RGPD prévoit, pour sa part (article 2) son application « *au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* ».

Est définie comme un traitement (article 4 du RGPD) « ***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, la cession, l'effacement… »*

[3] Délibération CNIL n° 84-28 du 3 juillet 1984, Mairie d'Arcueil et autres.

ILLUSTRATION : exemples de traitements

La compilation, l'enregistrement ou la consultation de données à caractère personnel dans :
- un tableur Excel ;
- une liste informatisée ;
- un logiciel quelconque (gestion du capital social par exemple ou un logiciel de *Customer Relationship Management* (« CRM ») ou de Gestion de Relation Clients (« GRC ») ;
- une liste de messagerie ;

constituent des traitements informatisés de données à caractère personnel.

L'usage d'un système de vidéosurveillance permettant l'identification (sur la base de l'apparence physique) de personnes constitue également un traitement de données à caractère personnel, soumis, toutefois, à une législation particulière.

La définition de fichier est également identique à celle de la loi I&L.

La qualification de traitement s'applique **dès la phase de la collecte des données**. De même, la cession de données à caractère personnel est un traitement, pour le cédant comme pour le cessionnaire.

ILLUSTRATION : exemple de cession constituant un traitement

La cession par une coopérative de la liste d'une partie de ses associés coopérateurs à un fournisseur ou un prestataire constitue un traitement de données à caractère personnel. Il est en cela soumis à la règlementation et doit respecter les principes énoncés ci-après.

La réception et l'enregistrement de ces données par le prestataire ou le fournisseur est également un traitement de données à caractère personnel.

La seule difficulté d'application de ces dispositions réside dans la notion de traitement automatisé ou non automatisé. Un traitement de données à caractère personnel peut être informatisé ou non, il est soumis à la loi dès lors que ces données sont appelées à figurer dans des fichiers.

En pratique, **la définition du fichier** implique que **toute opération qui a pour objet d'organiser la collecte, puis la gestion de données à caractère personnel par ordre alphabétique, chronologique ou thématique**, constitue un fichier.

ILLUSTRATION : classement papier constituant un fichier soumis à la règlementation

Un classement papier par ordre alphabétique ou d'adhésion de bulletins d'adhésion d'associés coopérateur est un traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans des fichiers. Un traitement de ce genre, bien que non informatisé est soumis à la loi ou au règlement.

De même, le classement papier de contrats de travail ou de candidatures est un traitement de données à caractère personnel obéissant aux mêmes règles.

C- Responsabilité du traitement et sous-traitance

Le fait que le responsable du traitement soit établi en France est également, aux termes de ses articles 2 et 5, une condition d'application de la loi I&L.

L'article 5 dispose en effet que :

> « *I- Sont soumis à la présente loi les traitements de données à caractère personnel :*
>
> *1° **Dont le responsable est établi sur le territoire français**. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;*
>
> *2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne.* »

Le responsable d'un traitement de données à caractère personnel est, quant à lui, désigné par l'article 3-I de la loi I&L.

> *« Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. (…) »*

Le RGPD (article 4), pour sa part, définit le responsable de traitement comme :

> *« 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 ».*

La détermination du responsable de traitement est importante pour de nombreuses raisons, par exemple pour déterminer l'applicabilité territoriale du règlement (définie à l'article 3 du RGPD).
En effet, ce dernier est applicable :

- aux traitements effectués dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'Union, **que le traitement ait lieu ou non dans l'Union,**
- aux traitements relatifs à des personnes concernées qui se trouvent dans l'Union européenne, mis en œuvre par un responsables du traitement qui n'est pas établi dans l'Union lorsque ces traitements sont liées :
  - A l'offre de biens ou de services destinées à des personnes concernées au sein de l'Union,
  - au suivi de comportements de ces personnes.

Ainsi, la sous-traitance sera explicitement visée dans les critères d'application de la règlementation relative aux données à caractère personnel.

1. La désignation du responsable

Le responsable de traitement est la personne, le service ou l'organisme qui répond aux questions suivantes : pourquoi ce traitement va-t-il être mis en place et comment remplir son objectif ?

Il n'est souvent pas simple de déterminer qui est le responsable de traitement. En effet, il peut s'agir de la société ou encore d'un service de la société ou d'une personne physique dans la société, ce qui est risqué en termes de sécurité juridique. Pourtant, cette désignation est extrêmement importante. Le rôle du responsable de traitement est très étendu. C'est en effet lui qui :

- gère le traitement et est chargé de sa conformité,
- est tenu de traiter les demandes d'accès et autres demandes qui en découlent.

C'est pour cette raison que le Groupe de Travail de l'article 29 (dit « Le G29 », groupe de travail chargé de la protection des personnes à l'égard du traitement des données à caractère personnel, prévu à l'article 29 de la directive de 1995, d'où il tire son nom, qui réunit l'ensemble des « CNIL » européennes) dans un avis du 20 février 2010[4] a fortement conseillé de désigner comme responsable de traitement, et donc responsable en dernier ressort de la protection des données à caractère personnel**, la société elle-même**.
Le G 29 a, dans les situations compliquées qui ne permettent pas de recourir à cette désignation, élaboré une méthode permettant l'identification du responsable de traitement :

- adopter une approche globale de la personnalité de l'entité désignée : privilégier les sociétés ou organismes plutôt que les personnes physiques,

- identifier l'origine du pouvoir de déterminer les finalités et moyens : s'agit-il d'une compétence issue d'un texte spécifique (résolution précise du Conseil d'Administration) ? Cela découle-t-il implicitement d'un texte plus général ? ou est-ce une situation de fait qui implique cette responsabilité ?

- définir éventuellement une coresponsabilité s'il n'est pas possible d'identifier un responsable unique.

ILLUSTRATION : désigner le responsable de traitement

Une coopérative polyvalente peut être organisée en différentes filières disposant de niveaux d'indépendance plus ou moins grands.
Dans ce cas, il peut arriver que les filières ou leurs organes dirigeants puissent mettre en œuvre des traitements de données à caractère personnel de manière autonome.
Dans une telle situation, il se peut que la coopérative désigne comme responsable de traitement une personne physique au sein de la filière.
Une telle pratique n'est pas conseillée. D'une part, car la nomination d'une personne physique, qui peut être amenée à quitter ses fonctions, ne répond pas à l'objectif d'identification d'un responsable fiable et univoque, gage de clarté pour les personnes concernées. D'autre part, car les responsabilités assumées par la personne physique sont importantes pour un traitement qui, au final, est assuré au nom et pour le compte de la coopérative.

2. Distinction avec la sous-traitance

Il est important de distinguer cette notion de celle de la sous-traitance. Le sous-traitant traite les données pour le compte du responsable de traitement. Il n'est, en revanche, pas responsable du traitement. Cette notion est encadrée par l'article 35 de la loi I&L ou à l'article 28 du RGPD.

[4] Avis 1/2010 du 20 février 2010.

En revanche, si une coopérative collecte des données et les traite pour son propre usage puis les cède à un organisme qui les traite également pour son propre compte, il y a dans ce cas deux traitements. Celui de la coopérative et celui du cessionnaire.

ILLUSTRATION : distinction cession/sous-traitance

Une organisation reçoit pour mission de réaliser une enquête sur la productivité par parcelle des associés coopérateurs des coopératives. Elle a besoin, pour cela, d'informations spécifiques sur les associés coopérateurs. Elle peut décider de sous-traiter la collecte des données aux coopératives. Ces dernières ne seront pas responsables de traitement. Elles ne seront que sous-traitantes car elles ne traitent pas les données collectées pour la finalité de l'enquête pour leur propre compte. Un contrat devra alors impérativement être passé entre l'organisation et les différentes coopératives.

A l'inverse, si les coopératives transmettent des données qu'elles traitent également pour leur propre compte, il n'y a pas de lien de sous-traitance. Les coopératives réalisent un traitement en transmettant les données demandées, de même que l'organisme en collectant ces données et en réalisant l'enquête.

Le statut du sous-traitant est prévu par la loi I&L. L'article 35 ne prévoit que :

- l'exigence d'un contrat passé entre le responsable et le sous-traitant,
- l'interdiction pour le sous-traitant de traiter les données sans instruction du responsable,
- l'obligation pour le sous-traitant de présenter des garanties suffisantes au regard de la loi I&L.

Le RGPD va nettement plus loin sur ce sujet. Les sous-traitants seront investis d'une véritable mission d'assistance aux responsables de traitements dans la mise en conformité. En plus du respect des conditions de régularité des traitements, le sous-traitant aura une véritable mission de conseil et d'assistance dans la documentation de conformité (étude d'impact, registres…). Ils seront également soumis aux obligations de *privacy by default* et *privacy by design* (voir infra) au même titre que les responsables.
La CNIL a publié, en septembre 2017, un guide du sous-traitant décrivant les obligations à venir et les moyens de s'y conformer.

II) Vérifier la conformité des traitements existants

Une fois identifiés les traitements de données à caractère personnel soumis à la règlementation et leurs responsables au sein de la coopérative, la deuxième étape consiste à apprécier la conformité des traitements aux obligations du RGPD et, si nécessaire, à remédier aux non-conformités.

La vérification de la conformité doit se faire au regard de trois aspects :
- le respect des **conditions de régularité** du traitement,
- la **garantie des droits** que les personnes concernées par le traitement tirent de la règlementation,
- la vérification des **fondements du traitement**.

A- La conformité aux conditions de régularité des traitements

Le traitement doit obéir à un certain nombre de principes ayant vocation à protéger les droits fondamentaux des personnes concernées contre les traitements excessifs ou les utilisations ultérieures qui pourraient être faites de leurs données.
Ces principes ne sont que très peu modifiés par le RGPD.

Article 6 de la loi I&L	Article 5 du RGPD
- Licéité et loyauté de la collecte - Finalités déterminées, explicites et légitimes - Adéquation, pertinence et caractère non excessif au regard des finalités des données collectées - Exactitude, complétude et mise à jour des données - Limitation de la durée	- Licéité, loyauté et transparence - Finalités déterminées, explicites et légitimes - Adéquation, pertinence et limitation au regard des finalités - Exactitude et mise à jour si nécessaire - Limitation de la conservation - Intégrité et confidentialité

1. Licéité et loyauté du traitement

Cette obligation à la charge du responsable du traitement implique que les données soient collectées avec le consentement, ou, le cas échéant, l'information, de la personne concernée. A contrario, est considérée comme déloyale la collecte de données à caractère personnel effectuée à l'insu de la personne, et ce, **même lorsque les personnes concernées ont accepté une certaine publicité de leurs données.**

Lorsque le consentement doit être recueilli, il est primordial qu'il soit **explicite et éclairé[5].**

Il convient donc d'être vigilant sur ce point. L'interprétation de ces principes est large et le manquement à ce devoir est pénalement sanctionné[6].

2. Principe de finalité

Tout responsable de traitement doit impérativement déterminer les finalités de son traitement, c'est-à-dire son ou ses objectifs. Cette étape est cruciale car de la détermination de la finalité découlent certaines conséquences, notamment l'applicabilité d'un régime dérogatoire, la proportionnalité ou la détermination de la durée de conservation des données. **La finalité lie par ailleurs l'exploitant qui ne peut utiliser le traitement à d'autres fins.**

[5] CE, 12 mars 2014, n° 353193, Sté Pages Jaunes
[6] Articles 226-18 et 226-24 du code pénal

La finalité du traitement **doit donc être déterminée de façon explicite**, c'est à dire **claire et non équivoque**. Cela exclut les finalités vagues (« collecte pour exploitation » ou « collecte pour tout usage ») ou inexistantes.

ILLUSTRATION : détermination des finalités du traitement

Une coopérative dispose de données collectées auprès de ses associés coopérateurs pour les finalités suivantes :

1. Gestion de la vie sociale (registre du capital, listes d'associés participants aux différentes assemblées, correspondances relatives à la gouvernance)
2. Gestion de la collecte, suivi des engagements, de l'approvisionnement, des facturations et paiements
3. Cessions à des tiers éventuels (fournisseurs, employés des sociétés chargées de la collecte) pour réalisation de la collecte, de l'approvisionnement ou de la facturation

Elle souhaite participer à l'enquête relative à la productivité des associés coopérateurs. Elle dispose des données nécessaires à l'organisme qui réalise cette enquête. Ces données n'ont toutefois pas été collectées pour cette finalité. La coopérative ne peut donc pas les céder sans recueillir à nouveau le consentement des personnes concernées.

La finalité du traitement doit également être légitime. Cela signifie que les finalités de ce traitement, lors de son élaboration et à chaque instant de sa mise en œuvre, doivent avoir reçu le consentement de la personne ou être couvertes par l'un des cas dans lequel le consentement n'est pas requis.

En dehors du cas où le traitement a reçu le consentement de la personne, il peut en effet trouver sa légitimité dans différentes législations (droit du travail, droit de la consommation…) ou dans l'exécution d'un contrat (voir infra).

Ce principe a été illustré par l'affaire de la géolocalisation. La CNIL, approuvée par la Cour de Cassation, a estimé que ce dispositif, qui constitue un traitement de données à caractère personnel, ne pouvait être justifié **que pour des finalités de sécurité des personnes et/ou des marchandises** mais l'a exclu dans un but de contrôle permanent des employés[7].

3. Proportionnalité

Les données traitées doivent, aux termes des deux textes, être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées* ».

En conséquence, **seules les données réellement et strictement nécessaires à la réalisation des finalités prévues au traitement peuvent être traitées.**

ILLUSTRATION : proportionnalité d'un traitement

Une coopérative ne peut, dans un traitement uniquement dédié à la gestion de la collecte vente, collecter des informations relatives à la vie familiale de l'associé coopérateur.
Une telle information n'ayant pas de rapport avec le traitement, elle serait considérée comme disproportionnée.

De même, il n'est pas possible de collecter les numéros de carte d'identité (ou tout autre numéro) simplement dans un but de faciliter la mise en œuvre du traitement (recherche dans le fichier, par exemple).

[7] CNIL, délib. nº 2006-066, 16 mars 2006 et Cass Soc, 3 novembre 2011.

4. Exactitude et complétude des données traitées

Les données traitées doivent être **exactes, complètes et, si nécessaire, mises à jour, effacées ou rectifiées** sans attendre que la personne concernée fasse exercice de son droit d'accès et de rectification.

Le manquement à cette obligation peut faire l'objet de sanctions administratives, voire pénales[8] lorsqu'il s'agit d'une demande d'une personne concernée qui exerce son droit d'accès et de rectification.

5. Durée de conservation des données

Le responsable de traitement est tenu d'estimer la durée de conservation nécessaire au regard des finalités fixées **et ne peut les conserver plus longtemps sous une forme permettant l'identification.** Cette obligation matérialise en partie le « droit à l'oubli ».

Ainsi, une durée de conservation doit être prévue au-delà de laquelle les données sont effectivement supprimées ou anonymisées.

Certaines normes simplifiées ou délibérations de la CNIL imposent des durées maximales.[9]

Les données permettant d'établir la preuve d'un droit ou d'un contrat peuvent être conservées selon les règles relatives à la prescription prévues par le Code civil, le Code de commerce ou le Code de la consommation.

ILLUSTRATION : conservation des données en coopérative

La prescription des créances personnelles ou mobilières est acquise par cinq ans (article 2224 du Code civil).
En cela, les données relatives à la gestion des activités de collecte vente, approvisionnement ou service ne peuvent être conservées que jusqu'à l'expiration du délai de prescription, à savoir cinq ans à compter du remboursement des parts de l'associé démissionnaire. Au-delà, la conservation devient sans objet au regard de la finalité de la collecte des données.

La loi peut également poser des limites dans certains cas spécifiques. En matière de gestion du personnel, par exemple, certains documents doivent être impérativement conservés pendant une durée définie (5 ans à compter de la date à laquelle le salarié a quitté l'établissement pour les mentions portées sur le registre unique du personnel, par exemple : article R.1221-26 du Code du travail).

Dans les autres cas, il est important de veiller à ce que la durée de conservation des données ne dépasse pas ce qui est nécessaire au regard des finalités, sous peine de sanctions pénales[10].

[8] Art. R. 625-12 du code pénal.
[9] La délibération n° 2010-229 du 10 juin 2010 relative aux traitements des organismes à but non lucratif interdit par exemple dans son article 5 la conservation des données au-delà de la démission ou la radiation de l'adhérent.
La délibération n° 2016-264 du 21 juillet 2016 relative aux traitements ayant pour objet la gestion des fichiers clients et prospects distingue, dans son article 5, selon les données.
[10] Art 226-20 du code pénal.

B- La garantie des droits des personnes concernées

Au-delà du respect de grands principes de mise en œuvre des traitements, la conformité à la règlementation passe également par la garantie des droits des personnes concernées.
Ces droits, déjà présents dans la loi I&L, sont repris dans le RGPD qui en rajoute certains.

1. Le droit à l'information

Le fait pour la personne concernée d'être informée de l'existence du traitement et de sa finalité est un corolaire du principe de loyauté du traitement. Cette obligation est prévue à l'article 32 **de la loi I&L et aux** articles 12 et suivants du RGPD**.**

a. L'information en cas de collecte directe

Lorsque les données sont collectées directement auprès de la personne concernée, que ce soit par écrit, à l'oral, lors de la création d'un espace sur un site internet ou quelle que soit la forme, la loi I&L (article 32) prévoit que le responsable de traitement informe la personne:

- de l'identité du responsable ;
- de la finalité du traitement ;
- du caractère obligatoire ou facultatif des réponses ;
- des conséquences du défaut de réponse ;
- du ou des destinataires ou catégorie de destinataire des données ;
- des droits dont elle dispose ;
- des éventuels transferts hors Union européenne ;
- de la durée de conservation.

Si la collecte est réalisée par voie de questionnaire, ce dernier doit par ailleurs obligatoirement mentionner l'identité du responsable, la finalité, le caractère obligatoire des réponses et les droits dont dispose la personne. La notion de questionnaire s'interprète largement. Un formulaire de collectes de données, qu'il soit numérique[11] ou papier est assimilé à un questionnaire.

Le RGPD impose certains éléments supplémentaires à communiquer. Aux termes de son article 13, la personne concernée est informée :

- de l'identité du responsable ;
- des coordonnées du délégué à la protection des données, le cas échéant ;
- des finalités du traitement ainsi que de son fondement juridique (consentement, contrat, base légale) ;
- de l'éventuel intérêt légitime poursuivi le cas échéant ;
- des destinataires ;
- des éventuels transferts hors Union européenne.

De plus, si cela s'avère nécessaire pour garantir un traitement équitable et transparent, la personne concernée doit également être informée :

- du délai de conservation des données ou de ses modalités de détermination ;
- de l'existence du droit d'accès, de rectification, de limitation, d'effacement et de portabilité ainsi que des modalités de son exercice ;
- de son droit de retrait du consentement, si le consentement est la condition du traitement ;
- de son droit au recours devant une autorité de contrôle ;
- des conséquences au regard d'un éventuel contrat de son refus du traitement ;
- de l'existence d'une éventuelle décision prise sur le fondement du traitement.

[11] Décision CNIL 2016/007 du 26 janvier 2016 – Facebook.

Cette information peut se faire par écrit ou tout autre moyen en des termes clairs, lisibles compréhensibles et facilement accessibles.

ILLUSTRATION : information des associés coopérateurs

Les mentions légales, dans le cas des traitements mis en œuvre dans les coopératives agricoles, peuvent figurer dans différents documents.

Elles peuvent figurer dans le règlement intérieur. Dans ce cas, elles peuvent porter sur l'ensemble des traitements mis en œuvre par la coopérative et énumérer les différents traitements et les différentes finalités. En d'autres termes, il peut s'agir, pour la coopérative, de développer sa politique générale de traitement des données à caractère personnel vis-à-vis de ses seuls associés coopérateurs, qui sont les seuls destinataires du règlement intérieur.

Sur le bulletin d'adhésion, en revanche, les mentions légales doivent porter sur les traitements concernant l'associé coopérateur destinataire du document. Quant au document unique récapitulatif, qui reprend les obligations existantes, il est recommandé d'y mentionner les mentions légales, car son émission procède d'un traitement et par ailleurs, il est un instrument de la bonne information de l'associé coopérateur.

L'information devant également se faire au moment de la collecte, si le bulletin d'adhésion, ou tout autre document adressé à l'associé, sert à collecter de nouvelles données, les mentions prévues doivent être apposées sur le document ou la page internet.

Sur le bulletin d'adhésion servant à recueillir les informations, la coopérative peut par exemple apposer la mention suivante (ces mentions sont à adapter au cas par cas) :

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par (RESPONSABLE DU TRAITEMENT) pour les finalités suivantes :

- *gestion de la collecte des produits ;*
- *gestion des approvisionnements ;*
- *partage avec les associations sanitaires partenaires de la coopérative à des fins de coordination de la politique sanitaire ;*
- *gestion de la facturation ;*
- *gestion de la vie sociale de la coopérative.*

Elles sont conservées pendant toute la durée de l'engagement de l'associé coopérateur et conformément aux textes en vigueur et sont destinées aux salariés de la coopérative et aux organismes partenaires exclusivement.
Conformément à la loi « I&L », vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant : (service ou personne en charge du droit d'accès + adresse).

L'entrée en vigueur du RGPD devra entraîner une modification de ces mentions qui devront intégrer, le cas échéant, les coordonnées du délégué à la protection des données, les fondements juridiques du traitement mais également la mention des nouveaux droits consacrés par le RGPD (portabilité, effacement).

Les mentions légales publiques constituant la « vitrine » de la conformité, des mentions légales absentes ou non conformes fournissent un signe extérieur visible du non-respect de la règlementation.

b. L'information en cas de collecte indirecte

L'obligation d'informer les personnes existe également lorsque la collecte des données est indirecte, par le biais d'une cession ou d'une compilation.

L'exploitant d'un traitement de données à caractère personnel est tenu d'un devoir d'information des personnes concernées quand bien même il aurait récupéré les données sur internet ou auprès du collecteur direct.

La loi prévoit que cette information intervient :
- au moment de l'enregistrement des données,
- si une communication à des tiers est prévue, au plus tard au moment de la première communication.

Plus précis, le RGPD prévoit que la communication des informations doit se faire :
- si une communication avec la personne concernée doit avoir lieu, au plus tard au moment de la communication,
- si les données doivent être communiquées à une autre personne, au plus tard au moment de la communication,
- sinon dans un « délai raisonnable » qui ne peut excéder un mois.

Les informations à communiquer ne varient pas par rapport à la collecte directe. Le RGPD prévoit en revanche que la source des données doit être communiquée si cela s'avère nécessaire à la garantie d'un traitement équitable et transparent vis-à-vis de la personne concernée.

2. Le droit d'accès et ses corollaires

L'information de la personne lui permet, par la suite, d'exercer les droits ci-dessous. Il est donc nécessaire pour la coopérative, de mettre en œuvre les modalités permettant de répondre effectivement aux demandes des personnes concernées. L'exercice des droits est en effet le moment ou le responsable et la personne se retrouvent dans une situation potentiellement génératrice de litiges.

a. Droit d'accès

Le droit d'accès prévu à l'article 39 de la loi I&L et à l'article 15 du RGPD, permet à toute personne physique justifiant de son identité le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue, notamment, d'être informé de l'existence d'un traitement, de sa logique et d'obtenir copie des informations le concernant.

L'interprétation que fait la jurisprudence de la notion de « personne concernée » au sens de cet article est plus large que la simple définition de l'article 2 de la loi I&L. Ainsi, les héritiers d'une personne décédée peuvent se prévaloir de la qualité de « personne concernée » pour accéder aux données à caractère personnel, si la personne initialement concernée n'a pas laissé de directives sur le sort des données après son décès[12].

Le responsable de traitement est en droit de refuser les demandes manifestement excessives et peut facturer à la personne les frais de reproduction éventuels.

L'article 12 du RGPD précise que le responsable de traitement dispose d'un mois pour répondre à la requête de la personne concernée. En cas de réponse négative, la réponse doit

[12] CE, 29 juin 2011.

préciser les motifs et informer la personne de son droit d'exercer un recours devant l'autorité de contrôle. Ce délai d'un mois peut être prolongé d'un mois supplémentaire.

ILLUSTRATION : droit d'accès par un associé coopérateur

Une coopérative responsable de traitement peut être confrontée à une demande d'accès d'un de ses associés coopérateurs.

Elle est dans ce cas tenue de répondre dans les délais prévus (deux mois actuellement et un à compter du 18 mai 2017) et, si elle accède à la demande, de communiquer l'intégralité des informations qu'elle possède sur l'associé coopérateur.

Cette communication peut se faire par courrier recommandé ou, si la masse de données est conséquente, sur un support (CD, clé USB…). Lorsque le règlement sera entré en vigueur, il sera possible, si la demande a été formulée par voie électronique, de fournir les données par voie électronique.

Si cette demande d'accès conduit à une demande de rectification ou d'opposition, il appartient à la coopérative d'en apprécier le bienfondé. La preuve de la conformité du traitement pèse sur la coopérative.

b. Droit de rectification

Le droit de rectification résulte de l'article 40 de la loi et 16 du RGPD.

Ce droit peut s'exercer lorsque les données sont inexactes, incomplètes, équivoques ou périmées. La personne concernée peut également demander l'effacement ou le verrouillage de données qui ont été illégalement collectées, conservées ou utilisées. Ce dernier point est également repris par le RGPD dans le droit à la limitation du traitement.

En cas de litige, il appartient à la personne responsable du traitement de prouver que la collecte ou l'utilisation est conforme.

Il est donc indispensable, pour un responsable de traitement, d'indiquer des coordonnées de contact permettant aux personnes concernées de se prévaloir de manière effective des droits qu'elle tire de la loi I&L.

c. Droit d'opposition

Le droit d'opposition permet à toute personne de s'opposer, pour des motifs légitimes, à ce que les données à caractère personnel la concernant fassent l'objet d'un traitement. Ce droit est consacré par l'article 38 de la loi I&L et 21 du RGPD.

Cette opposition **ne se confond pas avec le recueil du consentement**, même si l'un découle de l'autre. Le droit d'opposition est une possibilité offerte à la personne de suivre l'évolution de ses données et de s'opposer, le cas échéant, à une utilisation à laquelle la personne ne consentirait pas ou plus. Le droit d'opposition *« pour des motifs légitimes »* vaut également pour les cas dans lesquels le recueil du consentement n'est pas requis au regard de la loi ou du règlement.

Il est à noter qu'une personne n'a pas à se prévaloir d'un motif légitime lorsqu'il s'agit de fins de prospections, notamment commerciales.

d. Droit à « l'oubli »

Ce droit nouveau est consacré par l'article 17 du RGPD.

La personne concernée peut demander l'effacement de ses données, par exemple :
- lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ;
- lorsque la personne retire son consentement et qu'il n'existe pas d'autre fondement juridique au traitement ;
- lorsque le traitement est illicite ;
- lorsque la loi de l'Etat membre l'impose ;
- lorsque la personne s'oppose au traitement de ses données et qu'il n'existe pas de motif pour le responsable de s'y opposer ;
- lorsque la personne s'oppose au traitement de ses données pour des finalités de prospection commerciale.

Ce droit ne s'applique pas dans certains cas limitativement énumérés tels que les traitements nécessaires à la liberté de l'information ou rendus obligatoires par la loi de l'Etat membre ou le droit de l'Union européenne.

e. Droit à la portabilité

Il s'agit d'un autre droit nouveau consacré par l'article 20 du RGPD. Il permet à la personne concernée de demander au responsable de traitement la communication de données sous format *« structuré, couramment utilisé et lisible par machine »,* cela afin de les céder à un autre responsable de traitement.

Deux conditions cumulatives s'imposent :
- le traitement est fondé sur le consentement ou résulte de l'exécution d'un contrat,
- le traitement est automatisé.

La personne peut également demander au responsable de traitement la cession des données la concernant à un autre responsable de traitement. Le responsable de traitement doit donc, lorsque cela est techniquement possible, transférer les données au nouveau responsable.

Les données concernées sont les données que la personne a activement fournies (nom, âge, adresse, coordonnées téléphoniques, adresses électroniques…) mais également celles collectées par le responsable de traitement au cours de la relation avec la personne concernée dans le cadre de l'activité par l'utilisation du service ou du dispositif.

Sont en revanche exclues les données « construites » par le responsable de traitement, par déduction ou dérivation des données collectées. Les résultats des analyses statistiques, par exemple, ne sont donc pas concernés.

Le G29 a publié le 5 avril 2017 une circulaire relative à la mise en œuvre du droit à la portabilité (disponible en anglais uniquement).

ILLUSTRATION : mise en œuvre du droit à la portabilité en coopérative

La cession de certaines données à caractère personnel par l'associé coopérateur est fondée sur l'exécution d'un contrat, l'engagement coopératif.
Si le traitement mis en œuvre par la coopérative est automatisé, l'associé coopérateur est alors en droit de faire jouer son droit à la portabilité et, par exemple, de demander, s'il décide de changer de coopérative à la fin de sa période d'engagement, le transfert des données à

caractère personnel le concernant à la seconde coopérative (nom, adresse, production, localisation des parcelles, numéro de téléphone, RIB…).

Le délai de réponse de la coopérative en cas de demande d'exercice de ce droit est d'un mois. Cette dernière doit accéder à sa requête si cela est techniquement possible et informer l'associé. Si cela ne l'est pas, elle doit informer dans ce délai l'associé coopérateur des motifs de son refus et de la possibilité qui lui est offerte d'introduire un recours devant l'autorité de contrôle national.

f. Droit à la limitation

Le droit à la limitation du traitement, prévu à l'article 18 permet à une personne de demander au responsable de traitement que les données la concernant ne soient plus que conservées mais ne puissent plus être traitées, sauf accord de sa part, pour un usage autre que la conservation.

L'usage de ces données ne reste possible que pour l'exercice de la défense en justice, la défense des droits d'une autre personne ou un « motif important d'intérêt public ».
Le droit à la limitation est reconnu dans quatre cas :

- l'exactitude des données est contestée ;
- le traitement est illicite ;
- le responsable souhaite supprimer les données, contre la volonté de la personne concernée qui souhaite qu'elles soient conservées pour l'exercice de ses droits en justice ;
- la personne s'oppose au traitement et le responsable de traitement se prévaut d'un intérêt légitime qu'il convient de vérifier.

Cette possibilité de « verrouiller » le traitement existait déjà dans la loi I&L *via* le droit de rectification mais acquiert, par le droit à la limitation, un caractère autonome.

C- La conformité du fondement du traitement

Ce point de la règlementation est probablement le plus compliqué à gérer pour le responsable du traitement, tout particulièrement la transition avec le RGPD qui modifie à la marge la question du consentement de la personne.

En effet, si sous l'empire de la loi I&L, le recueil du consentement est au centre mais peut être assorti de dérogations, le règlement n'en fait qu'un fondement parmi d'autres.

1. Le recueil et le retrait du consentement

a. Le recueil du consentement

Le recueil du consentement de la personne concernée par le traitement est capital et découle du principe de loyauté.

L'obligation de recueillir le consentement, sous réserve du bénéfice d'une des éventuelles dérogations, est prévue à l'article 7 de la loi I&L.

Le consentement lui-même n'est pas défini par la loi. Il convient donc de s'en référer à la définition donnée par la CNIL[13] qui s'appuie sur la définition de la directive 95/46/CE du 24 octobre 1995[14] dont l'article 2.h), est repris à l'article 4 du RGPD :

[13] CNIL, dél. n° 2013-420, 3 janv. 2014, par exemple.
[14] Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

« *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Le consentement devient dans le RGPD l'un des fondements juridiques possibles du traitement.

Il faut rappeler que le recueil du consentement de la personne n'affranchit pas le responsable du traitement de respecter les autres conditions de licéité du traitement qui sont précisées à l'article 6 de la loi (voir partie II.A) de même que les dérogations à cet exigence de recueil du consentement (voir partie II.C.2). Par ailleurs, l'information ne vaut pas consentement.

Le consentement doit donc être :

- **Une manifestation de volonté**

En cela, le consentement doit être **explicite et indiscutable**. L'article 7 de la directive impose d'ailleurs que les Etats membres prévoient que le traitement ne puisse être mis en œuvre que si la personne concernée a « indubitablement » donné son consentement.

Le RGPD exige pour sa part un « acte positif clair » et déclare dans son considérant 32 qu'« *il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.* »

Une action est donc nécessaire pour matérialiser ce consentement qui ne peut découler du silence gardé. En cela, l'esprit de l'exigence du recueil du consentement **exclut l'opt-out** (possibilité de retirer son consentement réputé acquis par défaut) au profit de l'opt-in (obligation de consentir au traitement).

ILLUSTRATION : exclusion de l'opt-out

Hormis dans les cas couverts par les dérogations à l'exigence de recueil du consentement décrits ci-après (partie II.C.2), tels que l'obligation légale incombant au responsable de traitement (registre des associés, par exemple, prévu à l'article R. 522-2 du Code rural et de la pêche maritime), la coopérative qui met en œuvre un traitement est tenue de prouver qu'elle a recueilli le consentement des associés coopérateurs dont les données à caractère personnel font l'objet d'un traitement et ce **par le biais d'une manifestation de volonté explicite de leur part.**

Ainsi, si la coopérative décide de participer à une enquête et céder certaines données relatives à ses associés coopérateurs, la simple décision du Conseil d'Administration, même approuvée en Assemblée générale, ne suffit pas. La simple approbation en assemblée générale d'un nouveau traitement ne peut emporter le consentement de chaque associé coopérateur : un tel consentement ne peut être donné que de manière individuelle.

Il n'est pas non plus possible de considérer que l'absence de réponse négative à un courrier d'information vaut consentement.

- **Libre**

Le consentement ne doit pas être influencé ou son refus ne doit pas donner lieu à des conséquences défavorables pour la personne concernée. Cela vaut, par exemple, dans les cas où la personne est sous influence du responsable de traitement (relation de travail, par exemple).

- **Spécifique**

La spécificité du consentement implique qu'en cas de finalités multiples, le consentement doit être donné pour chaque finalité. Celles-ci doivent donc avoir été portées à la connaissance de la personne **de manière lisible et intelligible**. En aucun cas le consentement ne peut être recueilli de manière globale pour l'ensemble du traitement si les finalités ne sont pas clairement définies.

De même, si les finalités du traitement viennent à évoluer en cours de mise en œuvre du traitement, le consentement doit être de nouveau demandé.

- **Informé**

Il est enfin nécessaire que la personne dont les données font l'objet d'un traitement ait été informée non seulement clairement, mais également au préalable des caractéristiques de ce traitement.
La CNIL exige que l'information soit compréhensible (sans jargon, dans un caractère lisible) mais également accessible. Il ne suffit pas que l'information soit simplement disponible.

Le RGPD impose, dans son article 8, lorsque le consentement est recueilli dans le cadre d'une déclaration écrite qui concerne également d'autres questions, que « *la demande de consentement* [soit] *présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples.* »

La charge de la preuve du recueil du consentement pèse sur le responsable du traitement. En cela, un écrit reste la meilleure des preuves.

Le règlement prévoit également, dans son article 8, de nouvelles mesures de protection des mineurs. Il prévoit que le consentement des mineurs de moins de 16 ans ne peut être donné licitement, âge pouvant être aménagé jusqu'à 13 ans par les Etats membres.

ILLUSTRATION : spécificité du consentement

Une coopérative dispose de données collectées auprès de ses associés coopérateurs pour les finalités suivantes :
- gestion de la vie sociale (suivi du capital, correspondances…),
- gestion des engagements, de la collecte, de l'approvisionnement et des facturations et paiements,
- cessions à des tiers éventuels pour facilitation de la collecte, de l'approvisionnement ou de la facturation.

Elle souhaite participer à l'enquête relative à la productivité des associés coopérateurs. Elle dispose des données nécessaires à l'organisme qui réalise cette enquête. Ces données n'ont toutefois pas été collectées pour cette finalité.
Pour mettre en place ce traitement, la coopérative est tenue de recueillir le consentement spécifique des associés coopérateurs concernés.

b. Le retrait du consentement

L'article 7.3 du règlement prévoit que :

> « *3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant*

de donner son consentement. Il est aussi simple de retirer que de donner son consentement. »

Le retrait du consentement est donc désormais possible et peut servir de préalable à l'exercice du droit à l'oubli.

Il est important pour les responsables de traitement de prendre en compte la consécration de ce droit par la loi. Des précisions, sur le sujet du consentement en général et son retrait en particulier doivent intervenir par le biais d'une note du G29.

2. Les autres fondements du traitement

La loi, comme le règlement, prévoient des exceptions à la nécessité de recueillir le consentement. Mais si la loi traite ces cas comme de véritables exceptions et le recueil de consentement comme le principe, dans son article 7, le règlement diffère en ne faisant du consentement que l'un des fondements possibles du traitement parmi d'autres, à l'article 6.

En tout état de cause, identifier le fondement du traitement existant ou envisagé est nécessaire à la conformité. Ces fondements possibles sont :

- le consentement de la personne, dans les conditions définies précédemment ;
- le respect d'une obligation légale incombant au responsable du traitement.

Il s'agit du cas dans lequel la constitution d'un traitement est une obligation pour le responsable aux termes du droit national ou du droit de l'Union européenne.

Tel est par exemple le cas **de l'article** R . 522-2 du CRPM **qui dispose que :**

La qualité d'associé coopérateur est établie par la souscription ou par l'acquisition d'une ou plusieurs parts sociales de la coopérative.
Toute société coopérative agricole doit avoir obligatoirement à son siège un fichier des associés coopérateurs sur lequel ces derniers sont inscrits *par ordre chronologique d'adhésion et numéros d'inscription avec indication du capital souscrit par catégorie de parts telles que prévues à l'article R. 523-1.*

- L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

ILLUSTRATION : portée de la base légale de l'article R. 522-2 du CRPM

Les exceptions étant d'interprétation stricte, cette disposition ne concerne que le fichier des associés coopérateurs. Elle ne peut en aucun cas couvrir d'autres traitements.

Il s'agit dans ce cas **des données collectées à l'occasion de la souscription d'un contrat ou d'un service et qui ont pour finalité la réalisation de ce contrat**.

ILLUSTRATION : engagement coopératif et fondement contractuel

L'engagement coopératif comporte des obligations pour l'associé coopérateur (souscrire des parts sociales et utiliser les services de la coopérative) mais également pour la coopérative (convoquer les assemblées générales et exercer son activité avec l'associé coopérateur).
Ainsi, pour permettre à la coopérative d'accomplir ses obligations issues de l'engagement coopératif, certains traitements de données à caractère personnel sont nécessaires à cette

dernière tels que la collecte et l'utilisation de l'adresse de l'associé coopérateur, permettant l'envoi des convocations ou la collecte et l'utilisation des données nécessaires à l'activité pour lesquelles les parts ont été souscrites.
Le traitement rendu nécessaire par l'exécution par la coopérative de ses obligations ne nécessite pas de recueil du consentement.

Il n'en va pas de même avec les traitements extra-statutaires qui ne relèvent pas de l'engagement coopératif, par exemple, la cession par la coopérative de données à caractère personnel à des organismes de comptabilité.
Dans ce cas, la coopérative doit recueillir le consentement des personnes concernées.

Seuls les traitements nécessaires à l'exécution du contrat coopératif sont couverts par cette dérogation et cela ne dispense pas la coopérative du respect des autres obligations liées à la conformité que sont les conditions de licéité (voir infra : partie II.A) et l'information (voir infra : partie II.B).

Il peut en aller de même avec d'autres contrats passés par la coopérative.

- La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ;

La jurisprudence de la Cour de Justice de l'Union européenne a, sur ce point, développé des conditions. **Le traitement doit tout d'abord être nécessaire[15].**
Ce fondement n'est ensuite acceptable qu'à condition que le traitement ne viole pas les droits et libertés fondamentaux de la personne concernée. Une **mise en balance de l'intérêt du traitement au regard des impacts sur les autres libertés est alors à appliquer.**
Il est apprécié au regard du droit de l'Union ou de l'Etat membre.

- La sauvegarde de la vie de la personne concernée ;

- L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement.

En application du RGPD, le fondement du traitement est à indiquer de manière obligatoire dans les mentions légales et dans le registre des traitements. Il devient donc particulièrement nécessaire d'identifier clairement quels sont les fondements des différents traitements mis en œuvre et, le cas échéant, de s'assurer que le traitement correspond bien à son fondement.

ILLUSTRATION : identification des fondements

Une coopérative met en œuvre de nombreux traitements de données, que ce soit vis-à-vis de ses associés coopérateurs, de ses interlocuteurs externes ou de ses salariés.

Chacun de ces traitements doit disposer d'un fondement juridique qu'il conviendra de déterminer précisément.

Par exemple :
- logiciel de gestion de la paye des salariés : obligation légale ;
- collecte de données pour la vente en ligne (conditions générales de vente) : mesures contractuelles et obligations légales ;
- fichier des associés : obligation légale ;

[15] CJUE, 13 mai 2014, aff. C-131/12, Google Spain SL.

- fichier de gestion de la collecte vente : mesures contractuelles ;
- fichier de cession de données relatives aux associés coopérateurs à des associations sanitaires : consentement ;
- liste de diffusion au public d'une lettre d'actualité : consentement ;
- fichier des adresses d'envoi des convocations aux assemblées générales : mesures contractuelles ;
- listes d'émargement à l'assemblée générale : mesures contractuelles.

III) Identifier les formalités au regard des risques

Le règlement européen bouleverse principalement la philosophie des contraintes qui pèsent sur les responsables de traitement.
Alors que la loi I&L prévoit une déclaration du traitement valant engagement de conformité, le RGPD choisit la responsabilité du responsable de traitement, garantie par divers outils et assortie de contrôles et de sanctions plus lourdes.

A- Les formalités issues de la loi I&L

L'objet de la présente circulaire n'est pas la gestion des formalités par la loi I&L qui ont vocation à disparaître.
Le RGPD opte pour une politique de responsabilisation et d'autocontrôle des responsables de traitement par le biais de différents outils, tels que le registre, le délégué de protection des données ou l'étude d'impact.

En cela, les formalités actuellement prévues par la loi I&L (la déclaration, déclaration simplifiée ou l'autorisation) **disparaîtront en règle générale le 25 mai 2018.**

Toutefois, dans certains domaines, tels que les traitements nécessaires aux relations de travail (article 88 du RGPD) ou les données de santé (article 9 du RGPD), le règlement permet à l'Etat de conserver certaines dispositions supplémentaires, telles que les autorisations.

Les entreprises devront désormais tenir un registre et définir les modalités d'utilisation de leurs fichiers en fonction des risques qu'elles représentent. Elles devront donc procéder à une autoévaluation des risques et enjeux de la mise en œuvre d'un traitement de données à caractère personnel.

La loi I&L et ses textes d'application, les délibérations, ont toutefois le mérite d'offrir des pistes pour apprécier les risques qu'engendrent les traitements. Ces pistes pourront, ensuite, servir pour apprécier, dans le cadre de l'autocontrôle prévu par le RGPD, les risques des différents traitements. Il convient donc de rappeler quelles sont ces formalités qui ont vocation à disparaître.

1. Les traitements dispensés de déclaration

Le droit commun, sous la loi I&L, est la déclaration dite normale. Certains traitements sont toutefois considérés comme peu risqués et donc dispensés de cette déclaration, cela par trois biais différents.

- Les traitements visés par la loi elle-même

La loi I&L vise expressément certains traitements comme étant « non risqués » et donc exclus du champ de la déclaration.

Sont visés certains traitements mis en œuvre par certains organismes à but non lucratif, dans les conditions visées au point II de l'article 22 de la loi.

- Les traitements visés par une dispense spécifique

La loi prévoit la possibilité pour la CNIL, à l'article 24, d'adopter des dispenses visant les traitements les plus courants et qui ne sont pas susceptibles de porter atteinte à la vie privée. Ces dispenses ont fait l'objet de délibérations, publiées au Journal Officiel et sur le site de la CNIL. Elles portent sur certaines catégories de traitements et précisent :

- les finalités du traitement ;
- les destinataires ou catégories de destinataires ;
- les données à caractère personnel traitées ;
- la durée de conservation de celles-ci ;
- les catégories de personnes concernées.

Ces dispenses **doivent être appréciées de manière stricte.**

Sont par exemple dispensés de déclaration :

- les traitements mis en œuvre par les comités d'entreprise (délibération 2006-230) ;
- les traitements mis en œuvre par les organismes à but non lucratif (délibération 2010-229) ;
- les traitements relatifs à la gestion des fournisseurs (délibération 2005-005) ;
- les traitements relatifs à la gestion de la rémunération (délibération 2004-097) ;
- les traitements relatifs à la gestion de la comptabilité (délibération 1980-034) ;
- les traitements relatifs à la communication externe non commerciale (délibération 2006-138).

- Les traitements de base pour lesquels la structure a désigné un correspondant I&L

Les responsables de traitement peuvent s'ils le souhaitent, désigner un correspondant I&L (CIL) conformément à l'article 22-III.
La désignation du correspondant doit être déclarée à la CNIL. Par la suite, les traitements pour lesquels le correspondant a été déclaré sont dispensés de formalités pour les traitements les plus courants.

- Les traitements soumis à déclaration simplifiée

L'article 24 de la loi permet également à la CNIL de soumettre certains traitements à une déclaration simplifiée.

32 normes simplifiées existent actuellement. Toutes sont disponibles sur le site de la CNIL.

Sont par exemple soumis à déclaration simplifiée :

- les traitements relatifs à la gestion du personnel (Délibération 2005-002) ;
- les traitements relatifs à la gestion de la téléphonie sur le lieu de travail (Délibération 2005-19) ;
- les traitements relatifs à la gestion des biens immobiliers (Délibération 2003-067) ;
- les traitements relatifs à la géo localisation des véhicules utilisés par les employés (Délibération 2015-165).

2. Les traitements soumis à autorisation par la loi I&L

La loi prévoit également que certains types de traitement sont soumis à autorisation préalable de la CNIL. Ces traitements peuvent être soumis à cette formalité pour deux raisons.

- En raison des données à caractère personnel traitées

La loi considère certaines données comme des données « sensibles ». Ainsi, l'article 8 interdit sauf dérogations limitées prévues au même article, les traitements de données à caractère personnel « *qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.* »

Certains traitements portant sur ces données peuvent être mis en œuvre à la condition d'être autorisés et de faire l'objet d'un processus d'anonymisation à bref délai.

Doivent également être autorisés du fait des données traitées :
- les traitements portant sur des données relatives aux infractions, condamnations ou mesures de sûreté,
- les traitements comportant le numéro d'identification des personnes au registre des personnes physiques (n° de sécurité sociale),
- les traitements comportant des appréciations sur les difficultés sociales des personnes.

- En raison des finalités

La loi considère également certains traitements comme sensibles en raison des finalités qu'ils poursuivent.

Ainsi, sont soumis à autorisation les traitements qui, en raison de leur portée, de leur finalité ou de leur nature, sont susceptible d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.

ILLUSTRATION : traitements risquant de conduire à l'exclusion d'un droit

La notion de traitement risquant, en raison de sa portée, de sa nature ou de sa finalité, d'exclure une personne du bénéfice d'un droit, d'une prestation ou d'un contrat peut aussi s'appliquer aux coopératives lorsqu'elles consentent aides financières à leurs associés coopérateurs.

En effet, selon le Conseil d'Etat, tout traitement qui, en raison de sa nature ou de ses finalités, pourrait avoir pour effet d'aboutir à la création d'une « liste noire » de « mauvais payeurs », est susceptible d'exclure les personnes figurant sur cette liste du bénéfice d'un droit ou d'une prestation.

Les coopératives, notamment celles qui accordent des prêts, doivent donc être vigilantes dans le recensement des impayés ou autres incidents de trésorerie des associés coopérateurs afin que ce traitement ne puisse pas servir de base, par exemple, au refus d'un prêt par la coopérative.
Si un tel traitement devait être envisagé, il devrait être soumis à autorisation de la CNIL.

Sont également soumis à autorisation de la CNIL les traitements ayant pour objet **l'interconnexion** de fichiers relevant de personnes privées ne gérant pas un service public et dont les finalités principales sont différentes.

B- La gestion des risques dans le RGPD : l'analyse d'impact préalable

La gestion actuelle des risques au regard de la loi I&L passe donc par une nomenclature des traitements assortie de différentes formalités préalables. Ce ne sera plus le cas après l'entrée en vigueur du RGPD. Ce dernier opte pour une analyse d'impact préalable obligatoire pour les traitements à risque, facultative pour les autres.

L'analyse d'impact du traitement (ou PIA, Privacy Impact Assessment) est un outil de la conformité particulièrement développé par le RGPD et les commentaires qui l'accompagnent.

Aux termes de l'article 35 du RGPD, le responsable de traitement est tenu de réaliser une analyse d'impact *« 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 ».*

Cette analyse d'impact doit comporter certaines informations énumérées au point 7 de l'article. La CNIL a mis à disposition des modèles permettant de bâtir une étude d'impact sur son site internet.

La difficulté principale n'est pas liée au contenu de l'étude d'impact mais à la détermination de l'obligation d'en réaliser une ou non. L'article 35 précise que sont en particulier soumis à une étude d'impact préalable systématique et approfondie :

- les traitements automatisés, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire,
- les traitements à grande échelle de données sensibles,
- la surveillance systématique à grande échelle d'une zone accessible au public.

Cette liste n'est pas exhaustive et le G29 a publié, le 4 octobre 2017, des lignes directrices (disponibles en anglais uniquement) détaillant dix critères permettant de déterminer si un traitement doit, ou non, faire l'objet d'une étude d'impact. Parmi eux figurent la taille du traitement, la présence de données sensibles, l'interconnexion, l'usage de technologies non encore éprouvées, le fait que les personnes concernées sont des personnes vulnérables ou que le traitement peut aboutir à la privation d'un droit.

L'analyse démarre dans un premier temps par une analyse du « contexte » du traitement. Le responsable analysera son environnement physique (ou est-il domicilié, qui y a accès, sur quoi/qui porte-t-il…), technique (quels en sont les supports, quelles sont les technologies utilisées, quelles sont les mesures de sécurité qui lui sont applicables…) et juridique (quelles sont les finalités ? Quels sont ses fondements ? Le traitement est-il nécessaire et proportionné aux finalités ?).
Il analysera alors chaque risque (accès illégitime, modification des données non désirée, disparition / suppression des données) afin d'estimer sa vraisemblance et sa gravité, selon plusieurs éléments :

- les impacts potentiels sur les droits et libertés (ex : cambriolage, détournement de fonds, etc.),
- les données traitées (ex : coordonnées, géolocalisation, code de carte bancaire),
- les sources de risques (ex : un cybercriminel, un salarié, le BYOG (« *bring your own device* »), le télétravail),
- et les vulnérabilités des supports de données (ex : un serveur à l'étranger).

Il proposera ensuite les mesures techniques et organisationnelles nécessaires pour réduire le risque à un « niveau acceptable ». Si l'étude d'impact aboutit à la conclusion que le traitement présente un risque élevé, l'article 36 impose que le responsable de traitement consulte

l'autorité de contrôle avant la mise en œuvre du traitement. Si l'autorité de contrôle estime que le responsable n'a pas pris les mesures nécessaires pour atténuer le risque au regard de l'étude d'impact, elle le notifie par écrit au responsable de traitement.

Il est important de noter que l'étude d'impact est un outil de conformité et donc que le fait de ne pas y procéder doit être justifié en cas de contrôle.

IV) Mettre en conformité le fonctionnement interne de la coopérative

La dernière étape de la mise en conformité consiste en une organisation interne de la coopérative répondant aux exigences du règlement.

A- Privacy by design et privacy by default

Les principes de *privacy by design* et *privacy by default* sont les deux principales nouveautés du RGPD.

Ils sont prévus à l'article 25 du RGPD et consistent en la prise en compte, dès la phase de la conception du traitement, de la conformité de ce dernier.

Concrètement, le principe de *Privacy by design* impose la prise en compte du respect du RGPD et de ses conditions de licéité dès la phase de conception des produits ou services nécessitant un traitement.

ILLUSTRATION : la phase de développement du produit ou du service

Prendre en compte la conformité dès la phase de conception implique concrètement qu'au moment où la coopérative envisage, par exemple, de développer une filière ovine et donc de mettre en œuvre un traitement de données à caractère personnel lié et nécessaire à cette activité, elle doit anticiper le fait qu'elle devra collecter des données à caractère personnel et prévoir la conformité dès la phase de développement de cette activité. Elle doit pouvoir en justifier. Cette justification peut se faire par exemple par le fait de présenter des lignes directrices applicables au sein de la coopérative et chargée de régir la mise en conformité des traitements dès le début.

Ce n'est donc pas au moment de la collecte que la coopérative doit se poser la question de la conformité mais dès le moment de l'élaboration du service de collecte d'ovins.

Le principe *Privacy by default* impose l'adoption de mesures techniques et organisationnelles permettant de garantir le fait que, par défaut, seules les données nécessaires au regard de la finalité sont traitées et que seules les personnes nécessaires y ont accès sans l'intervention de la personne concernée.

Concrètement, ces mesures organisationnelles doivent être définies dans des procédures écrites, pouvant être présentées en cas de contrôle.

ILLUSTRATION : La prise en compte de la conformité dès la phase de conception

Une coopérative souhaite participer à une enquête réalisée par un opérateur tiers qui étudie la rentabilité des parcelles agricoles. Elle souhaite donc collecter des données à caractère personnel auprès de ses associés coopérateurs et les céder à cet opérateur.

Elle met donc en place un traitement nouveau de données à caractère personnel.

Le principe de *privacy by design* impose que dès la phase de conception des modalités de participation de la coopérative à l'enquête, la protection des données à caractère personnel et le respect des conditions de licéité des traitements soit prise en compte.
Ainsi, la coopérative doit étudier avec soin les finalités du traitement, vérifier la nécessité de chacune des données collectées, prévoir les modalités de recueil du consentement ou encore mettre en place des processus d'effacement.

Elle doit également mettre en place des processus internes garantissant la conformité du traitement au principe de proportionnalité mais permettant également la garantie de l'ensemble des droits des personnes concernées et ce, dès la phase de conception.

Cela peut se traduire, par exemple, par la formation des personnes en charge des traitements à la gestion des traitements, par l'élaboration de processus de signalisation des violations de données à caractère personnel, de processus d'effacement des données dont la durée de conservation a expiré, par la mise en place d'habilitations à accéder aux données ou encore par l'élaboration de processus de gestion de changements de destinataires de données.

En tout état de cause, les notions même de *privacy by design* et *privacy by default* imposent que ces processus soient mis en place **avant** la mise en œuvre des traitements.

B- Le principe de responsabilité

L'article 24 du RGPD dispose :

> *« Le responsable de traitement met en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au règlement. »*

Le responsable de traitement dispose pour cela d'outils. Ces outils, définis par le règlement, permettent de justifier, lors des contrôles, le respect de la conformité du responsable de traitement.

1. La tenue d'un registre d'activité

Les procédures de déclaration sont remplacées par la tenue d'un registre des activités de traitement défini à l'article 30 du RGPD.

Le registre de traitement n'est pas obligatoire pour les entreprises de moins de 250 salariés. Il le devient toutefois si :

- le traitement n'est « pas occasionnel », c'est-à-dire s'il est réalisé selon une récurrence précise, quand bien même cette occurrence serait très longue,
- le traitement est jugé « à risque » du fait de son ampleur ou des données traitées (s'il porte sur des données comportant des condamnations pénales ou autres données sensibles telles que définies à l'article 30§5 du RGPD ou s'il est qualifié de traitement à risque aux termes des dispositions relatives à l'analyse d'impact : voir infra, III.B).

Le seuil des 250 salariés s'analyse, dans le RGPD, au regard de la définition de l'effectif d'une entreprise prévue par la recommandation de la Commission n°2003/361/CE du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, à ses articles 5 et 6.

Dans le cas d'un groupe d'entreprise :

- Si l'entreprise est autonome, la détermination de l'effectif se fait sur la base de ses seuls comptes
- Si l'entreprise est partenaire d'une autre au sens de l'article 3 de la recommandation précitée située immédiatement en amont ou en aval, l'effectif à prendre en compte est celui de l'entreprise assorti d'un pourcentage des effectifs proportionnel au pourcentage de participation au capital ou des droits de vote (le plus élevé de ces deux pourcentages). En cas de participation croisée, le plus élevé de ces pourcentages s'applique.
- Si l'entreprise est liée à une autre au sens de l'article 3 de la recommandation précitée, sont ajoutés à ses effectifs 100 % des effectifs de l'entreprise liée.

La cartographie des traitements mis en œuvre est, en tout état de cause, un outil de conformité utile car permet d'une part de s'assurer de la conformité de l'ensemble des traitements mis en œuvre et d'en justifier en cas de contrôle et, d'autre part, de réagir efficacement en cas de demande d'une personne concernée par ces traitements.

Ces registres doivent comporter :
- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, de son représentant et de l'éventuel délégué à la protection des données ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- les destinataires des données ;
- les éventuels transferts hors UE ;
- si possible, les délais d'effacement des données ;
- les mesures techniques et organisationnelles prises pour assurer la sécurité du traitement.

Il est également possible d'y adjoindre le fondement du traitement (obligation légale, application d'une mesure contractuelle, consentement…), cela à des fins de gestion des traitements.

La CNIL a mis en ligne un modèle de tableau de registre, au format Excel. La première page consiste en une liste des traitements mis en œuvre et la seconde en un exemple de fiche applicable pour un traitement.

2. La transparence

La responsabilité du responsable de traitement passe également par la transparence qui lui est imposée, vis-à-vis des personnes concernées (mentions légales) mais également vis-à-vis des autorités de contrôle.

Ainsi, le règlement prévoit qu'en cas de violation des obligations du responsable de traitement (destruction, perte, altération, divulgation ou accès non autorisé aux données à caractère personnel), ce dernier doit :

- informer l'autorité de contrôle de l'Etat membre dans les 72h. Cette notification doit comporter un certain nombre d'informations imposées par le règlement. La CNIL a prévu de mettre en ligne un formulaire informatique de notification,

- informer directement les personnes concernées, dans certaines conditions, que leurs données ont été violées lorsque cette violation représente « un risque élevé pour les droits et libertés d'une personne physique », sauf si des mesures ont été prises pour

rendre ces données inutilisables ou si cela est matériellement impossible (perte des données, par exemple). Dans ce dernier cas, une annonce publique peut être faite.

Des procédures doivent avoir été définies en amont dans le cadre du privacy by design et privacy by default, permettant de justifier de la prise en compte de ces exigences dès la phase de conception. Elles doivent être présentées dans le cadre de la documentation de la conformité (voir infra : IV.B.6).

3. La désignation d'un délégué à la protection des données (DPD)

Les responsables de traitement doivent désigner un délégué à la protection des données si :

- le traitement est effectué par une autorité publique ou un organisme public,
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées,
- les activités de base du responsable du traitement ou du sous-traitant sont *« sensibles »* au regard du RGPD.

En dehors de ces cas, la désignation du DPD est facultative.

Les missions du DPD sont d'assurer le respect du règlement, de collaborer et d'informer les responsables de traitement et d'être le point de contact des organismes de contrôle. Ces missions et ses fonctions sont prévues par le RGPD aux articles 40 et 41 et détaillées dans des lignes directrices du G29 (en anglais uniquement). Son rôle rejoint et remplace celui du correspondant informatique et libertés (CIL), jusque-là prévu par la loi I&L et dont la désignation permettait la dispense de formalités. La CNIL elle-même désigne le DPD comme le « successeur naturel » du CIL.

4. L'adhésion à des codes de conduite et la certification

La responsabilité du responsable de traitement peut également passer par son adhésion à des codes de conduite ou la certification extérieure de ses traitements (article 40 et suivants du RGPD).

Ces articles prévoient que les Etats membres encouragent l'élaboration de codes de conduite et de certification qui peuvent ensuite être approuvés par les autorités de contrôle des Etats membres.

Le G29 élabore actuellement des lignes directrices sur ce sujet.

5. La sécurisation des traitements

Il est nécessaire de rappeler que la règlementation relative à la protection des données vise la protection de ces dernières.

La sécurisation de ces données, qui tient lieu de fil rouge de ces règlementations, passe également par une sécurisation des traitements, proportionnelle au risque du traitement.

Le RGPD précise en effet que les données à caractère personnel doivent « *être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité.)* »

Les moyens de sécurisation et les objectifs sont définis à l'article 32.

Il s'agit donc de prévoir des méthodes de sécurisations proportionnées. Si un simple mot de passe peut suffire pour un traitement peu risqué, un traitement comportant des données sensibles (les traitements relatifs aux salariés, qui peuvent comporter des données de santé, par exemple) doit impérativement être plus sécurisé. Les dossiers papiers doivent, par exemple, être dans un bureau fermant à clé.

La conformité à ces obligations doit pouvoir être démontrée et faire l'objet de procédures de procédures écrites.

6. La documentation de la conformité

La dernière étape de la mise en conformité avec le RGPD consiste dans le fait de tenir à jour une documentation relative à la conformité qui pourra être présentée en cas de contrôle car elle constitue la base du principe de responsabilité du règlement.

En règle générale, la documentation de la conformité passe par la conservation des documents suivants :

- le registre des traitements à jour ;
- les éventuelles analyses d'impact ;
- les mentions d'information ;
- les modèles de recueil du consentement des personnes concernées ;
- les preuves que les personnes ont donné leur consentement lorsque le traitement repose sur cette base ;
- les procédures mises en place pour l'exercice des droits ;
- les contrats avec les sous-traitants ;
- les procédures mises en place pour assurer la sécurité des données ;
- les procédures internes mises en place en cas de violation de données ;
- le registre des violations.