Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'AGRICULTURE
ET DE
L'ALIMENTATION

Secrétariat général **Service de la modernisation** **délégation au numérique et à la donnée** **78, rue de Varenne** **75349 PARIS 07 SP** **0149554955**	**Instruction technique** **SG/SM/2018-227** **21/03/2018**

Date de mise en application : Immédiate
Diffusion : Tout public

Cette instruction abroge :
SG/SM/SDSI/N2006-1402 du 31/01/2006 : Les traitements de données à caractère personnel et le respect de la loi "Informatique et libertés" : organisation au sein du ministère de l'agriculture et de la pêche.
Cette instruction ne modifie aucune instruction.
Nombre d'annexes : 1

Objet : Instruction relative à la mise en œuvre du règlement (UE) n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (règlement général sur la protection des données) dans les services du ministère de l'agriculture et de l'alimentation

Destinataires d'exécution
DRAAF DAAF Directions d'administration centrale

Résumé : L'instruction présente le règlement général sur la protection des données (RGPD) et ses enjeux pour le ministère de l'agriculture et de l'alimentation (MAA).
Elle définit l'organisation mise en place pour y répondre et définit les rôles et responsabilités au sein du ministère, notamment en ce qui concerne la création et la tenue à jour d'un registre des traitements, l'intégration d'analyses préalables au titre du RGPD dans les études de cadrage des nouveaux projets informatiques et la mise en place d'une procédure de revue régulière des applications existantes articulée avec la revue exécutée au titre de la sécurité des systèmes d'information.

Elle précise en particulier que, dès le 25 mai 2018,les modalités d'informations des personnes concernées par des collectes de données personnelles doivent répondre aux exigences du RGPD et les traitements de données personnelles réalisés sous maîtrise d'ouvrage du MAA devront figurer dans le registre des traitements dont elle prévoit les modalités de constitution.

Textes de référence :règlement (UE) n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

I Présentation du RGPD – Etat des lieux

Le Parlement européen et le Conseil ont adopté le « paquet protection des données » le 27 avril 2016. Il se compose :
- d'un règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement (UE) 2016/679 dit RGPD). Ce règlement abroge la directive 95/46/CE transposée dans la loi n° 78-17 du 6 janvier 1978 modifiée et entre en application à compter du 25 mai 2018 ;
- d'une directive relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (directive (UE) 2016/680) qui ne concerne a priori pas le ministère de l'agriculture et de l'alimentation (MAA).

Un projet de loi ayant pour objet d'assurer la mise en conformité du droit national à ces nouvelles exigences et de définir les règles nationales sur quelques sujets dont le règlement prévoit qu'elles soient définies à ce niveau a été présenté en Conseil des ministres. Le débat parlementaire à venir est donc susceptible de modifier une partie de la présentation ci-après.

L'objectif principal de ce cadre juridique nouveau est de garantir aux citoyens européens la protection de leurs données personnelles, quel que soit le lieu où est réalisé le traitement de données, si celles-ci sont collectées sur le territoire européen ou destinées à la fourniture de services sur ce territoire.

Le cadre juridique relatif à la licéité des traitements et aux droits des personnes ne comprend pas d'évolutions majeures s'agissant de l'administration. Les traitements nécessaires au respect d'une obligation légale ou créés afin d'exécuter une mission de service public (et disposant d'une base juridique en définissant les paramètres) sont exclus du champ du consentement, du droit à la portabilité et du droit à l'effacement (sauf opposition). **La seule évolution réelle est l'obligation de délivrer une information relativement détaillée aux personnes concernées sur les informations recueillies et leurs finalités.**

S'agissant du droit d'opposition, le cadre juridique actuel établi par l'article 38 de la loi CNIL n'est pas modifié. Lorsqu'il concerne une obligation légale ou que l'acte établissant le traitement le prévoit, le droit d'opposition ne peut s'exercer; dans les autres cas (mission de service public sans texte), la charge de la preuve repose désormais sur le responsable de traitement qui doit démontrer son intérêt légitime à maintenir le traitement.

En cas de divulgation ou d'un accès non autorisé aux données, représentant un risque élevé pour ses droits et libertés, l'usager doit être informé, sauf si cela est susceptible de représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique (disposition du projet de loi).

S'agissant des sanctions, elles ne sont pas toutes susceptibles d'être appliquées aux administrations, et en particulier à l'État. En particulier, le règlement prévoit un montant (élevé) d'amende administrative pouvant être appliquée en cas de non respect du règlement par un responsable de traitement, mais il appartient au droit national de déterminer si cela s'applique ou pas aux autorités publiques, ce qui n'est pas le cas dans le projet de Loi.

Le RGPD prévoit la réduction des formalités préalables pour la mise en œuvre des traitements, avec le passage d'un système de contrôle *ex ante* de la Commission nationale de l'informatique et des libertés par le biais des déclarations, autorisations ou avis sur un projet d'acte, à **un contrôle *ex post* plus adapté aux évolutions technologiques et responsabilisant pour les responsables de traitement qui sont pleinement chargés de contrôler la proportionnalité du recueil des données**.

Les responsables de traitement devront donc mener une analyse d'impact afin de mesurer le risque en matière de protection des données, et, le cas échéant, consulter la CNIL lorsque le traitement présenterait un risque élevé (pour les droits et libertés de personnes physiques) malgré les mesures prises par le responsable de traitement pour atténuer le risque. Ce risque devra être apprécié par le responsable de traitement, au cas par cas. L'analyse d'impact, aussi appelée étude d'impact sur la vie privée (EIVP), est obligatoire pour les traitements présentant un risque élevé et conseillée pour tous les traitements sauf les moins risqués. La CNIL doit produire une liste de traitements pour lesquels elle est obligatoire.

L'analyse au titre de la sécurité des systèmes d'information est partie intégrante de cette EIVP dans la mesure où celle-ci comprend un pilier relatif aux droits liés aux données personnelles (respect des obligations légales) et aussi un autre portant sur les mesures techniques et organisationnelles appropriées pour protéger les données conservées (voir https://www.cnil.fr/fr/etude-dimpacts-sur-la-vieprivee-suivez-la-methode-de-la-cnil).
En conséquence, le projet de loi supprime les régimes de déclaration préalable et d'autorisation simple de la CNIL et restreint fortement le champ de l'autorisation par décret en Conseil d'État pris après avis CNIL aux traitements de données biométriques ou génétiques de l'Etat agissant dans l'exercice de ses prérogatives de puissance publique.
Il maintient aussi d'importantes protections pour certains types de données :
- il interdit les traitements qui nécessitent l'utilisation du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR), sauf s'ils figurent dans un futur décret-cadre pris après avis de la CNIL, s'il s'agit de téléservices ou de traitements statistiques (avec NIR haché).
- il conserve le régime actuel en matière de traitements de données de santé.

II Enjeux du RGPD pour le MAA

Les principales conséquences du RGPD sont ainsi de nature organisationnelle :
- outre la mise en place de l'EIVP, le responsable de traitement doit veiller à la tenue d'un registre des traitements de données personnelles et à la notification à la CNIL, et aux personnes concernées, des violations de données ;
- il est fait obligation de désigner un délégué à la protection des données (DPD) qui est chargé d'assister le responsable de traitement et ses équipes en les conseillant pour assurer la conformité au RGPD des traitements mis en œuvre.
Pour garantir l'effectivité de ses missions, le délégué doit disposer de qualités professionnelles et de connaissances spécifiques et doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.
Le délégué est indépendant (il ne reçoit aucune instruction sur ses missions et ne peut être pénalisé dans ce cadre) et fait directement rapport au niveau le plus élevé de la direction du responsable du traitement.

Ainsi, les enjeux pour le MAA sont :
- de définir l'architecture des responsabilités dans le rôle de responsable de traitement,
- de désigner un DPD et de lui donner les moyens d'exercer sa mission,
- de déterminer les procédures permettant de réaliser dans de bonnes conditions l'EIVP, d'organiser la tenue du registre des traitements et de répondre aux obligations nouvelles d'informations préalables et, le cas échéant, d'information sur les violations de données.

La présente instruction a pour objet de préciser les grandes lignes d'organisation retenues, qui ont fait l'objet d'une présentation en conseil des systèmes d'information, ainsi que les travaux préparatoires à réaliser d'ici l'entrée en vigueur du règlement.
Les procédures mises en place visent à une articulation la plus fine possible avec les procédures existantes ou dont la mise en place est liée à des enjeux complémentaires, dont la sécurité des systèmes d'information.

Elle pourra être complétée et modifiée au vu notamment du débat parlementaire sur le projet de loi.

III Organisation interne retenue

Le responsable de traitement

Le responsable du traitement est celui qui en définit la finalité et les moyens. Lorsque le traitement est instrumenté par un système d'information, le responsable du traitement est le maître d'ouvrage du système d'information. C'est donc un directeur d'administration centrale ou un chef de service du secrétariat général, éventuellement un DRAAF.

Lorsque ce traitement n'est pas instrumenté par un SI, par exemple lorsqu'il consiste en la création d'un tableau sur un logiciel bureautique, le responsable du traitement est la personne qui décide de créer ce traitement et en définit le contenu.

Dans tous les cas, le responsable du traitement doit veiller à la licéité du traitement dont il est responsable.

Il doit mettre en place les dispositifs permettant la bonne information et l'exercice des droits des personnes concernées, d'une manière proportionnée aux risques liés à ce traitement.

Le délégué à la protection des données (DPD)

Un délégué à la protection des données préfigurateur a été désigné : il s'agit de M. Romuald Oudjani, conseiller aux affaires pénales et civiles auprès de la directrice des affaires juridiques, et déjà correspondant de la CNIL.

Pour l'exercice de ses missions, le DPD reçoit à sa demande l'appui de la mission de la sécurité des systèmes d'information au sein de la sous-direction des systèmes d'information et de la délégation au numérique et à la donnée. Il a accès en permanence au registre des traitements et peut obtenir communication de tout document relatif à un traitement de données personnelles. Il est le point de contact avec la CNIL et peut être sollicité pour avis par tout responsable de traitement.

Il fait part directement aux responsables des traitements des conseils ou alertes qu'il jugera utiles, en en informant le délégué au numérique et à la donnée et le sous-directeur des systèmes d'information. Il rend compte de son action, et des éventuelles situations présentant un risque élevé, à la secrétaire générale et à la directrice des affaires juridiques.

Le délégué au numérique et à la donnée (DND)

Il est l'administrateur ministériel des données et à ce titre, chargé de coordonner au niveau ministériel la gestion des données. A ce titre, il propose les évolutions des modalités de mise en œuvre du RGPD au sein du ministère, dans le but notamment d'assurer une mutualisation des outils mis à disposition des différents responsables de traitement et une harmonisation des méthodes ; il participe aux études de cadrage des projets informatiques.

La sous-direction des systèmes d'information

Elle met à disposition l'outil permettant de gérer le registre des traitements du ministère et facilite la constitution de ce dernier en le préremplissant sur la base de sa connaissance des systèmes d'information qu'elle opère.

Elle organise les études de cadrage des projets informatiques et veille dans ce cadre, en lien avec le DND, à ce que les nouveaux projets soient conformes au RGPD.

Elle veille au maintien en condition de sécurité des systèmes d'information du MAA, ce qui inclut la vérification régulière que l'évolution des menaces ne dégrade pas la confidentialité des données personnelles ; elle et organise, le cas échéant, les évolutions nécessaires pour rétablir un niveau de sécurité satisfaisant.

IV Collecte de données personnelles

Licéité de la collecte

L'article 6 du règlement précise les conditions à remplir pour qu'un traitement de données soit licite. Dans la très grande majorité des situations, les traitements réalisés par le ministère relèveront du 6.1.e :
« le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » ,
ou éventuellement du 6.1.c :
« le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis », notamment pour le fonctionnement interne du ministère (SIRH, gestion des temps, …).
Il appartient au responsable du traitement de vérifier qu'il entre bien dans l'un de ces cas et de le justifier. Cela emporte des conséquences juridiques fortes (il n'y a alors ni droit à la portabilité ni droit à l'effacement, et le droit d'opposition est très limité).

Il pourra néanmoins arriver que le traitement relève du 6.1.a :
« la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ».
Le responsable du traitement doit alors recueillir le consentement explicite des personnes concernées, et mettre en place les moyens de respecter l'ensemble de leurs droits.

Information des personnes concernées

L'article 13 du règlement précise les informations à fournir à la personne concernée lors de la collecte des données personnelles.
Il s'agit de manière obligatoire de :
- l'identité et les coordonnées du responsable du traitement et du représentant du responsable du traitement à qui la personne doit éventuellement s'adresser,
- les coordonnées du délégué à la protection des données,
- les finalités du traitement et la base juridique du traitement,
- le cas échéant les destinataires de ces données personnelles (si ces données doivent être partagées avec d'autres structures dans le cadre de la procédure qui nécessite leur usage).

D'autres informations, citées à l'article 13.2, ne sont obligatoires que si elles sont nécessaires pour garantir un traitement équitable et transparent. A priori, les trois informations suivantes peuvent concerner un traitement opéré par le MAA :
- lorsque le traitement est fondé sur l'article 6.1.a (c'est à dire qu'il ne relève pas d'une mission de service public mais du consentement de la personne concernée), l'existence du droit de retirer ce consentement à tout moment,
- des informations sur le caractère réglementaire de la fourniture de données personnelles et sur les conséquences éventuelles de la non fourniture de ces données,
- l'existence d'une prise de décision automatisée à partir de ces données et des informations concernant la logique sous-jacente (par exemple : « les données collectées permettent de vérifier automatiquement l'éligibilité à telle aide, en application des critères qui sont précisées par tel texte »).

Il convient donc que, avant le 25 mai 2018, l'ensemble des collectes de données personnelles fasse l'objet d'une information, qui pourra prendre la forme d'une page accessible à partir du formulaire de saisie des informations, si elles font l'objet d'un téléservice, ou d'un texte inclus dans ou joint à un formulaire papier. Un exemple en est fourni en annexe. Cet exemple n'est pas applicable aux collectes réalisées sur la base du consentement, qui demanderont une élaboration au cas par cas.

V Registre des traitements

Initialisation

L'ensemble des traitements de données personnelles instrumentés par un système d'information dont le maître d'ouvrage est une structure du ministère doit figurer dans un registre des traitements.

Dans ce but, la SDSI élabore une première description des traitements de données personnelles pour les systèmes dont elle assure la maîtrise d'œuvre et qui sera implémentée dans Philae[1]. Cette première version du registre s'appuiera sur le référentiel des applications du MAA et indiquera pour chacune d'elle le traitement de données personnelles éventuellement existant et sa structure responsable, ainsi que les catégories de données personnelles concernées. Le niveau de risque lié sera également décrit par l'intermédiaire des cotations DICT (disponibilité, intégrité, confidentialité, traçabilité) du SI.

Il appartiendra aux différentes structures de :

- valider les informations relevant du quartier de SI (au sens de Philae) dont elles ont la responsabilité,

- les compléter le cas échéant par des informations sur les traitements dont la SDSI n'est pas maître d'oeuvre, notamment les éléments du SI de l'enseignement agricole qui sont gérés par le CNERTA.

Les informations initialisées par la SDSI seront disponibles dans Philae mi-mars.

---

1 Plateforme Harmonisée InterministérieLle d'Architecture d'Entreprise

Ces éléments devront être validés, ajustés ou complétés par les responsables de traitement ou leur assistance à maîtrise d'ouvrage interne pour le 15 mai 2018, avant l'entrée en vigueur effective du RGPD. Ils permettront notamment de définir la planification de la revue des traitements prévue ci-dessous.

Le point de contact des responsables de traitement sur le registre des traitements est, au sein de la SDSI, Alexandre Nguyen (alexandre.nguyen@agriculture.gouv.fr), urbaniste des systèmes d'information du ministère.

Contenu à terme

Les nouveaux traitements ainsi que les traitements existants, après qu'ils auront fait l'objet de la revue décrite ci-après, devront faire l'objet d'une description plus complète, qui sera toujours implémentée dans Philae. Un travail interministériel visant à définir les informations pertinentes et à implémenter ainsi que la possibilité de les renseigner sur Philae est en cours à cet effet.

VI Création de nouveaux traitements

Traitements mis en œuvre par un SI faisant l'objet d'un projet informatique

Les nouveaux projets informatiques du ministère font l'objet d'études de cadrage dans le cadre de la démarche PIMENT (cf circulaire SG/SM/SDSI/C2013-1401 du 10 juin 2013).

La similitude des approches dans le cadre du RGPD et de la sécurité des systèmes d'information (analyse de risque et intégration dès la conception) amène à ce que les problématiques spécifiques du RGPD soient étudiées dans le cadre de l'étude de cadrage sur la sécurité (étude ISP) de la démarche PIMENT.

Cette étude devra donc donner un diagnostic quant :

- au respect du principe de protection des données dès la conception et de protection des données par défaut, notamment le fait que seules les données à caractère personnel nécessaires à la finalité du traitement sont traitées (art 25. 2 du RGPD),

- à l'éventuelle nécessité, au vu de la sensibilité des données et des mesures techniques et opérationnelles de protection de réaliser l'analyse d'impact prévue à l'article 35 du règlement.

Le délégué à la protection des données est systématiquement destinataire de cette étude sur laquelle il peut donner un avis au responsable du traitement, avec copie au délégué au numérique et à la donnée et au sous-directeur des systèmes d'information. Si le responsable du traitement ne souhaite pas suivre cet avis, notamment dans le cas où ce dernier recommanderait une analyse d'impact, il l'indique au délégué à la protection des données en précisant les raisons qui l'y amènent, avec les mêmes destinataires en copie. Si le délégué estime la situation ainsi créée dangereuse, il en rend compte à la secrétaire générale et, le cas échéant, peut consulter la CNIL.

Si une analyse d'impact est jugée nécessaire, elle est réalisée avec l'appui de la SDSI/MSSI, qui dispose d'un marché de prestation adapté. Cette analyse est transmise au DPD dans les mêmes conditions que l'étude ISP. Il donne un avis au responsable du traitement quant à la pertinence, au vu de cette analyse, d'une consultation préalable de l'autorité de contrôle (la CNIL) telle que prévue à l'article 36 du RGPD et notamment au vu de l'article 36.1, qui prévoit une consultation obligatoire préalablement à la mise en œuvre du traitement lorsque l'analyse d'impact prévue à l'article 35 révèle que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

Lors de sa mise en service, le traitement est intégré dans le registre des traitements avec l'ensemble des informations précisées dans le paragraphe « contenu à terme » ci-dessus.

Autres traitements

Le RGPD ne couvre pas que les traitements faisant l'objet d'un développement informatique spécifique, ni même les traitements des seules données numérisées.

Néanmoins, la logique d'analyse de risque qui sous-tend le règlement amène à considérer que, sauf cas exceptionnel, un traitement qui ne nécessite pas d'être instrumenté par des outils informatiques présente un niveau de risque faible. Il est en tout état de cause absolument nécessaire de veiller à la licéité du traitement.

Par exemple, réunir dans un tableau une liste de coordonnées des contacts d'une structure est un traitement qui au sens strict relève du RGPD. Pour autant, dans la mesure où il s'agit de réunir des informations sans sensibilité particulière avec l'accord des personnes concernées dans la finalité légitime de pouvoir les contacter, sa licéité ne présente aucun doute, et si le tableau ne fait pas l'objet de transmissions ou de publication, le niveau de risque sur ces données est très faible. Ce niveau de risque devrait toutefois être analysé de manière plus approfondie si le tableau contenait aussi des données sensibles, telle qu'une appartenance syndicale (ce qui pourrait conduire à ce que le tableau soit protégé par un mot de passe par exemple).

La transmission par mail de données à caractère personnel est par contre une pratique à utiliser de manière très précautionneuse, et à éviter dès que la divulgation de ces données pourraient créer un préjudice aux personnes concernées, en raison des risques spécifiques (de mauvais adressage, de faire suivre erroné, de piratage …) lié à ce mode de transmission.

En cas de doute, le responsable des traitements peut solliciter l'avis du DPD.

VII Revue régulière des traitements

Une revue nécessaire pour prendre en compte les évolutions des menaces

La sécurité des systèmes d'information est un domaine en constante évolution technique et l'évolution des menaces peut amener un système initialement sûr à ne plus l'être. Ce sujet n'est pas spécifique aux traitements relatifs aux données personnelles, et une revue régulière de la sécurité face aux menaces nouvelles sur un rythme de l'ordre de 3 à 5 ans (indépendamment de la prise en compte au fil de l'eau des menaces nouvelles identifiées) est mise en place pour tous les systèmes informatiques pour assurer leur maintien en condition de sécurité. Lorsqu'elle portera sur des SI manipulant des données personnelles, cette revue prendra en compte les enjeux spécifiques du RGPD et servira d'actualisation de l'EIVP.

La planification de la revue des traitements existants à la date de mise en application du RGPD tiendra compte de la sensibilité des données manipulées

Les règles de fond relatives à la licéité des traitements restant globalement inchangées, il est considéré que les traitements existants respectent les exigences du RGPD. Toutefois, ils feront comme tous les traitements l'objet de la revue prévue ci-dessus, ce qui sera l'occasion de vérifier que le RGPD est bien totalement respecté ou de définir et mettre en place les mesures correctives nécessaires.

Une planification de la revue de ces traitements sera réalisée par le délégué au numérique en lien avec la SDSI et sous le contrôle du délégué à la protection des données dès que l'initialisation du registre des traitements aura été faite, en se basant notamment sur les données manipulées et le niveau de risque pour le respect de la vie privée qu'un mauvais usage de celles-ci ferait courir.

VIII Violation de données à caractère personnel

Si une violation de données à caractère personnel intervient dans l'un des systèmes d'information réalisé sous maîtrise d'ouvrage du ministère, le responsable du traitement, ou la SDSI si elle en est la première informée, en informe sans délai le DPD.

Le responsable du traitement, avec l'appui de la SDSI, prend toute mesure pour faire cesser aussi rapidement que possible la situation ayant permis cette violation, en informe la CNIL, avec copie au DPD et au DND, et définit la modalité adaptée pour informer les personnes concernées de cette violation dans les meilleurs délais, ce qui doit s'entendre comme dès que la divulgation de cette information ne sera pas susceptible d'augmenter les difficultés rencontrées, notamment en rendant publique une vulnérabilité non encore corrigée.

La secrétaire générale,

Valérie METRICH-HECQUET

Exemple de texte d'information

Collecte de données personnelles

dans le cadre de « nom de la procédure »

Dans le cadre de « nom de la procédure », le ministère de l'agriculture et de l'alimentation est amené à recueillir des informations qui peuvent avoir le caractère de données personnelles.

Le responsable du traitement est le ministère de l'agriculture et de l'alimentation - « préciser la direction du ministère ou le service du secrétariat général ». Toute demande d'information ou réclamation doit être adressée à « préciser les coordonnées du représentant du responsable du traitement, qui doit être défini par les procédures de la direction ou du service responsable du traitement ».

Le délégué à la protection des données du ministère est M Romuald Oudjani, romuald.oudjani@agriculture.gouv.fr.

Le traitement est réalisé en vue de « préciser les finalités de la procédure » , en application de « préciser les textes qui fondent la procédure », et est donc nécessaire à l'exécution d'une mission d'intérêt public dont est chargé le ministère [et/ou au respect d'une obligation légale qui pèse sur le ministère].

[Ainsi, en l'absence de fourniture de ces données, le ministère ne pourrait pas « préciser l'aide qui ne serait pas accessible » [ou vous seriez passible de « préciser la pénalité encourue »]]

[Ces données permettront de prendre une décision [en partie] automatisée, qui portera sur [la vérification de l'éligibilité, le calcul du montant, …]. « préciser la logique de la décision, dans le cas le plus fréquent, l'implémentation de règles issus de textes réglementaires à citer ». Cette décision restera comme toute décision administrative susceptible de recours.]