Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

SECRÉTARIAT GÉNÉRAL
DÉLÉGATION AUX SYSTEMES D'INFORMATION

BATIMENT COLBERT - TELEDOC 322
139, RUE DE BERCY
75572 PARIS CEDEX 12

18 mai 2018

Affaire suivie par : Gérard Dufour
Mél : gerard.dufour@finances.gouv.fr
Tél : 01.53.18.61.08
Réf. : -ASI/2018/0518

Instruction pour la mise en œuvre de la nouvelle réglementation de protection des données personnelles à compter du 25 mai 2018

Cette instruction a pour objectif de préciser les adaptations de la gouvernance interne aux ministères économiques et financiers qui s'appliquent en matière de protection des données à compter du 25 mai 2018

Le terme « réglementation relative à la protection des données (ci-après la réglementation)» recouvre les règles édictées par :

- Le règlement général sur la protection des données (règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ci-après RGPD).

- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée ; sa réforme en voie d'adoption vise d'une part à préciser les marges de manœuvre offertes aux Etats-membres par le RGPD précité et d'autre part à transposer la directive (directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ci-après la directive).

- l'ensemble des textes relatifs à la protection des données que le Gouvernement aura en charge, par ordonnance, de rassembler au sein d'un même texte dans les 6 mois de la promulgation de la loi de 1978 modifiée.

Cette instruction s'attachera notamment à indiquer les différences avec l'existant. Elle présentera successivement les acteurs (1) et leurs rôles puis le processus d'examen et de suivi d'un nouveau traitement depuis sa conception jusqu'à la fin de son utilisation (2). Elle indiquera enfin la part de l'existant maintenu (3) et les prochaines actions (4) à mener pour mieux intégrer le cycle de vie des projets et en particulier l'homologation de sécurité qui est connexe à la protection des données personnelles.

1. LES ACTEURS.

Le dispositif de protection des données s'articule autour de deux acteurs principaux, le responsable de traitement (ci-après RT) et le Délégué à la protection des données (ci-après DPD).

Le responsable de traitement est l'acteur principal en matière de protection des données ; de façon générale et sur le plan juridique, c'est le ministère qui assume ce rôle. En pratique le rôle de responsable de traitement opérationnel (RTO) sera assumé par la maîtrise d'ouvrage du traitement concerné.

Le DPD est un nouvel acteur ministériel du dispositif et, en conséquence, ses attributions doivent être définies. Au sein des MEF, c'est le Délégué aux Systèmes d'Information, qui exercera la fonction de DPD.

1.1 Le Délégué à la protection des données (DPD) et son réseau de référents.

Compte tenu de l'étendue de l'organisation des MEF, les directions et structures qui leur sont rattachées, ont été sollicitées pour désigner des « référents protection des données » afin de relayer l'action du délégué auprès des RTO. Ces référents DPD ne devront pas être parallèlement RTO.

Compte tenu de son rôle de délégué à la protection des données, le DSI ne signera plus les formalités préalables (résiduelles) par délégation du du ministre. Il appartiendra aux structures en charge de la gestion opérationnelle du traitement de déterminer le meilleur niveau de signature pour ce faire. Les modalités pratiques d'instruction des dossiers seront précisées par le DPD avec le réseau des référents.

1.1.1 Informer et conseiller.

Le premier rôle du DPD est « d'informer et conseiller le responsable du traitement sur les obligations qui lui incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données. ».

Cette compétence pourra s'exercer à l'initiative du DPD ou à la demande du RTO.

Ponctuelle ou générale, elle s'étendra en éventail du conseil ponctuel lors de la conception d'un traitement à la mise en place de programmes généraux de formation en collaboration avec les organismes concernés.

Pour démultiplier le conseil et l'information, des dispositifs de formation sont en cours de préparation avec l'IGPDE.

1.1.2 Contrôler dès la conception du traitement.

Le DPD a pour rôle essentiel de « contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ... en matière de protection des données à caractère personnel, y compris en ce qui concerne les audits s'y rapportant ».

Il s'agira également de « dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ».

Ce point est évidemment déterminant par son ampleur et son impact sur les processus existants de gestion de projets. Le DPD ne pourra mener à bien cette mission qu'au prix d'échanges constants qu'informels avec les RTO via le réseau des référents DPD.

Ce dialogue devra se réaliser aux étapes clés de la vie du traitement. Cette question sera illustrée au point 2 relatif au processus d'examen et de suivi d'un nouveau traitement.

1.1.3 Le DPD, point de contact pour l'autorité de contrôle.

Le DPD fait « office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet ».

Le DPD constitue le contact privilégié de la CNIL et coopère avec ses services et ce de façon très générale.

1.1.4 Le DPD, point de contact des personnes concernées.

Une personne concernée par un traitement peut choisir de contacter le RTO ou le DPD afin d'exercer ses droits.

Là aussi un partage d'informations doit intervenir ; le DPD passe par l'intermédiaire du référent (comme aujourd'hui pour les plaintes). Toutefois le délai de réponse a été raccourci à un mois.

La référence de la demande sera mentionnée au le dossier de conformité à la protection des données personnelles du traitement (DC-POD).

1.1.5 Le réseau des référents DPD.

Les rôles respectifs du DPD et des référents feront l'objet d'une formalisation progressive au fur et à mesure de la montée en puissance du dispositif.

Dans un premier temps, le DPD sera systématiquement associé dès la conception du traitement et ce, jusqu'à la définition d'une hiérarchisation des traitements.

A l'occasion des premiers travaux, l'annexe 1 précise la constitution au 25 mai du réseau des référents DPD des ministères économiques et financiers.

1.2 Le responsable de traitement opérationnel.

Le RTO est cité plus de 400 fois dans le RGPD ; il ne s'agira ici que d'évoquer ses principales obligations.

L'obligation majeure qui renverse la logique préexistante est que le RTO doit être en mesure de démontrer que le traitement est effectué conformément à la réglementation. Dans ce but, le RTO doit mettre en œuvre des mesures techniques et organisationnelles appropriées. L'étude d'impact fait partie de ces techniques. Elle sera évoquée au point 2 avec la protection dès la conception.

1.2.1 Le registre des traitements.

Le RTO tient un registre des activités de traitement effectuées sous sa responsabilité. Ce registre comporte un certain nombre d'informations obligatoires prévues par le RGPD. Il constitue évidemment une pièce essentielle de la documentation probatoire puisque tous les traitements doivent y figurer.

Au sein des MEF, le registre a fait l'objet d'une structuration qui répond à un double objectif :

- Disposer d'une structure de registre unique au plan ministériel qui permettra d'agréger les registres des RTO au sein de leur structure d'appartenance au niveau des référents du DPD puis au niveau ministériel du DPD.

- Le registre intègre les traitements existants et comporte donc toutes les rubriques aujourd'hui obligatoires pour les formalités préalables d'un traitement, y compris celles non prévues par le RGPD ou la directive.

Le registre reprend au 25 mai les traitements existants. Sa mise au point initiale est effectuée en collaboration entre les RTO et les référents DPD.

A compter de cette date, un nouveau traitement ou une modification substantielle de traitement ne seront intégrés au registre qu'après validation contradictoire associant le DPD et le RTO et ce, avant la mise en exploitation.

1.2.2 : Le registre des violations.

Le RTO doit documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée doit permettre à la CNIL de vérifier le respect de cette obligation.

Contrairement au registre des traitements qui regroupe les traitements opérationnels, cette obligation ne concerne que les violations intervenant à partir du 25 mai 2018.

Le registre doit s'inscrire dans une structure unique au plan ministériel et intègre les informations prévues par la réglementation.

En cas de violation, le RTO dispose de 72 heures au plus après en avoir pris connaissance pour informer la CNIL (à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques).

Il importe donc que le RTO informe son référent DPD dès qu'il a connaissance de l'incident pour échanger sur le sujet. Cet échange préalable aura également lieu si c'est le réseau DPD ou un RSSI qui ont connaissance de la violation le premier ; ce sera le cas notamment si le DPD est saisi par une personne concernée.

Les éventuels sous-traitants (ST) doit aussi être intégrés dans le circuit. Le ST doit informer le RTO dans les meilleurs délais après avoir pris connaissance de la violation.

1.2.3 : Les autres obligations.

La plupart d'entre elles relèvent d'une logique de mise en place progressive dans la mesure où leur réalisation ne saurait être immédiate.

Il s'agit de :

- La facilitation de l'exercice de leurs droits par les personnes concernées.
- L'amélioration des mesures de sécurité notamment transversales.
- La coordination avec les sous-traitants.
- La réalisation d'audits.
- Le programme de suivi triennal des traitements.

Ces obligations donneront lieu à des groupes de travail ministériels pour partager progressivement les bonnes pratiques et parvenir à une cohérence de traitement ministérielle notamment vis-à-vis des usagers.

Il faut noter que les RTO pourraient être amenés à faire face dans l'immédiat aux problématiques nouvelles du droit d'opposition, de la limitation du traitement subséquente et du recueil du consentement.

1.3 Les autres acteurs.

1.3.1 : La maitrise d'œuvre.

La maîtrise d'œuvre intervient à la demande d'un ou plusieurs RTO ; elle peut intervenir en intermédiaire vis-à-vis de prestataires et a donc un rôle de conseil auprès du RTO pour l'aider à assumer ses obligations de conformités réglementaires concernant la protection des données personnelles.

1.3.2 : Le RSSI.

Sa mission et les modalités de son intervention sont assez parallèles à celles du DPD . Tous deux partagent largement une même méthode d'analyse des risques et aussi des moyens identiques pour minimiser les risques identifiés.

Pour autant les risques pris en compte ne sont pas les mêmes puisque le DPD se focalise sur les risques encourus par les personnes concernées par le traitement ; le DPD vérifie en outre la licéité du traitement

et la prise en compte des principes du RGPD.

L'objectif est donc de coordonner les interventions du RSSI et du DPD vis-à-vis des RTO et pour cela d'ouvrir le dossier de conformité des traitements (DC POD) aux RSSI.

1.3.3 : Les sous-traitants.

Ces derniers ont des obligations nouvelles plus importantes dans la nouvelle réglementation.

Ils sont d'abord responsables du traitement pour la partie qu'ils ont en charge sur le plan pénal et pour son ensemble sur le plan civil.

Un écrit doit donc matérialiser les responsabilités et les engagements de chacun et comporter des informations que la réglementation impose.

Dans le cadre des marchés publics, la mise à niveau des documents de référence devrait être effectuée dans les meilleurs délais au sein de l'application ORME et comporter un article spécifique « protection des données » ; compte tenu des exigences du RGPD, cet article devra faire l'objet de compléments par le donneur d'ordre.

1.3.4 : Les autres RTO.

La réglementation a introduit la notion de « responsable conjoint » de traitement; parallèlement les échanges de données entre administrations se multiplient ainsi que les traitements s'appuyant sur des API. La question se pose de la répartition des responsabilités entre les différents intervenants concernés par ces échanges de données. Cette question qui se pose notamment en contexte interministériel a sera traité à ce niveau.

2. PROCESSUS relatif aux TRAITEMENTS :

Ce dispositif a vocation à s'appliquer à la création de nouveaux traitements, aux modifications de traitements existants ayant un impact sur la protection des données et à la veille triennale sur l'ensemble des traitements.

2.1 Le DC-POD (Dossier de Conformité en matière de PrOtection des Données à caractère personnel).

Outre les échanges informels entre le RTO et le réseau du DPD, chaque traitement donnera lieu à l'établissement d'un DC-POD qui répond à plusieurs principes :

- Le DC POD est unique pour un traitement ; il a vocation à documenter tout ce qui concerne la protection des données.

- Il accompagne le traitement tout au long de sa vie et de ses modifications.

- Le DC-POD est rédigé à partir d'un modèle ministériel établi par le réseau DPD et des RTO. Il s'adapte au risque présenté par le traitement et à sa complexité. Sa structure reprend pour la partie « étude d'impact » celle retenue par le G29 (groupe des autorités de contrôle européennes) et la CNIL.

- Il permet d'alimenter le registre des traitements et y est référencé.

- Le DC POD comporte un historique qui intègre notamment :

    - Les références des violations de données figurant au registre correspondant ;

    - Les références des demandes des personnes concernées avec leur origine (RT ou DPD) ;

    - Les références des audits menés sur le traitement ;

    - Les relations avec le sous-traitant et la référence du document qui les lie.

Le DC POD a vocation à être partagé a minima entre le RTO, le référent DPD de sa direction et le DPD. Il servira de base d'échanges si la CNIL demande des éléments sur un traitement donné.

En pratique, l'identifiant d'un DC-POD sera composé du sigle de la structure suivi d'un numéro séquentiel complété, à titre informatif, du nom du traitement.

Le DC-POD comprendra a minima une fiche de description du traitement, la justification du respect du RGPD ainsi que la procédure choisie et sa justification.

2.2 Le parcours du DC-POD :

2.2.1 : Initialisation : Le RTO doit initialiser le DC-POD dès le début de la phase de cadrage et d'expression des besoins.

Le référent DPD et le DPD doivent être consultés a minima avant que soit prise la décision de lancement du projet.

2.2.2 : Le choix de la procédure :

Au cours de la phase de conception et au plus tard lors de la rédaction des spécifications fonctionnelles, le choix de la procédure de protection des données à suivre est arrêté dès que le DC-POD contient suffisamment de précisions pour permettre ce choix.

Ce choix fera l'objet d'un avis du DPD et d'une décision formalisée du RTO historisés au DC POD.

2.2.2.1 : Régime juridique :

De manière assez analogue à l'existant, il convient de déterminer quel instrument s'applique au traitement. Ce choix est bien évidemment structurant pour la suite.

Il peut s'agir soit du RGPD, soit de la directive soit du domaine qui échappe à la compétence de l'Union européenne (sûreté de l'Etat, renseignement...)

Ce choix ne peut s'effectuer qu'au cas par cas et dépend tant du RTO, que de la finalité et des données traitées.

Dans certains cas et, en l'absence de jurisprudence, ce choix sera source d'incertitude sur le plan juridique. Il s'avérera en tout cas déterminant pour la suite de la procédure.

2.2.2.2 : Obligation d'une consultation de la CNIL :

En l'état du processus législatif, les traitements relevant de la directive font l'objet d'une consultation obligatoire de la CNIL et nécessiteront la réalisation d'une étude d'impact.

2.2.2.3 : Obligation d'une étude d'impact :

La CNIL doit publier une liste des traitements qui feront obligatoirement l'objet d'une étude d'impact.

2.2.2.4 : Analyse de risque :

Pour tous les traitements qui ne relèvent pas des points 2.2.2.2 et 2.2.2.3, le RTO doit effectuer une analyse de risque basée sur les neuf critères établis par le G29 dans son avis WP-248 du 4 avril 2017 modifié le 4 octobre.

Il s'agit, de façon simplifiée, des traitements :

- ayant recours à l'évaluation, la notation ou le profilage des individus ;
- utilisant la décision automatisée se traduisant par un effet juridique ou significatif pour la personne concernée ;
- pratiquant la surveillance systématique des personnes ;

- comportant des données sensibles (particulières au sens du RGPD mais aussi d'infractions);
- à grande échelle pour la population visée (mais aussi pour le nombre de données, la permanence ou l'étendue géographique) ;
- effectuant des croisements de données entre traitements aux finalités différentes ;
- qui concernent des personnes vulnérables (enfants...) ou en relation inégale avec le RT ;
- qui font appel aux nouvelles technologies ;
- qui empêchent la personne concernée d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Si deux critères sont remplis, le RTO doit effectuer une étude d'impact.

2.2.3 : Etude d'impact (DPIA):

Quand le RTO a l'obligation de réaliser une étude d'impact, celle-ci peut aboutir à un risque élevé pour les personnes concernées. Dans ce cas, la CNIL doit être consultée.

La DPIA est effectuée sous la responsabilité du RTO et avec l'appui du réseau du DPD.

Elle s'intègre dans le DC POD.

La DPIA fait mention in fine de l'avis du DPD.

Elle donne lieu à un choix explicite et motivé de mise en œuvre par le RTO (sous l'aspect protection des données personnelles) ; ce choix peut différer de l'avis du DPD.

La structure de la DPIA s'inspire naturellement de celle adoptée par le G29 et la CNIL.

La DPIA s'articule autour de deux piliers :

- Le premier permet de justifier du respect des principes de la protection des données ainsi que des mesures prise pour faciliter l'exercice des droits des personnes concernées.

- Le second traite de l'étude des risques courus par les personnes concernées et de leur maitrise.

2.2.3.1 : Premier pilier, respect des principes de la protection des données :

Le respect du premier pilier est nécessaire dans tous les cas, qu'il y ait étude d'impact ou non.

Une description systématique du traitement est fournie avec :

- La nature, la portée, le contexte et les finalités du traitement ;
- Les données à caractère personnel concernées, les destinataires et la durée de conservation ;
- une description fonctionnelle du traitement ;
- Les ressources tant humaines que matérielles et techniques mobilisées.

La nécessité et la proportionnalité sont évaluées :

- Les mesures envisagées pour assurer la conformité doivent être détaillées ;
- Des justifications doivent prouver que les finalités sont déterminées, explicites et légitimes, que le traitement est licite, que les données sont adéquates, pertinentes et limitées à ce qui est nécessaire et que les durées de conservation sont limitées.

Description des mesures contribuant aux droits des personnes concernées:

- Informations fournies à la personne concernée ;

- Droit d'accès et droit à la portabilité des données ;

- Droit de rectification et droit à l'effacement ;

- Droit d'opposition et droit à la limitation du traitement ;

- Relations avec les sous-traitants ;

- Garanties entourant le ou les transferts internationaux ;

- Recueil du consentement.

Description des mesures de sécurité portant sur les données : chiffrement, anonymisation, cloisonnement des données (par rapport au reste du SI), contrôle des accès logiques, traçabilité, contrôle d'intégrité, archivage, sécurité des documents papier.

Description des mesures générales de sécurité : sécurité de l'exploitation, lutte contre les logiciels malveillants, gestion des postes de travail, sécurité des sites web, sauvegardes, maintenance, sécurité des canaux informatiques (réseaux), surveillance, contrôle d'accès physique, sécurité des matériels, éloignement des sources de risques, protection contre les sources de risques non humaines.

Description des mesures organisationnelles (gouvernance) : organisation, politique (gestion des règles), gestion des risques, gestion des projets, gestion des incidents et des violations de données, gestion des personnels, relations avec les tiers, supervision.

2.2.3.2 : Deuxième pilier, l'étude de risque :

Le deuxième pilier consiste en une étude des risques :

- La méthode est basée sur EBIOS ; elle est donc très comparable à celle utilisée dans le cadre de l'homologation de sécurité.

- Les moyens de maîtrise et de diminution des risques sont les mêmes que ceux utilisées dans le cadre de l'intégration de sécurité dans les projets (ISP).

- Les risques sont par contre différents d'une étude RSSI et ne concernent que ceux courus par les personnes concernées. Dans ce domaine, l'apprentissage permettra de roder voire de standardiser le processus. C'est pourquoi il sera important de capitaliser l'expérience dans les premiers mois au niveau ministériel voire interministériel.

Plus généralement un **risque** est un **scénario** hypothétique qui décrit comment des **sources de risques** pourraient exploiter les **vulnérabilités** (**vraisemblance**) des **supports de DCP** au moyen de **menaces** et permettre à des **événements redoutés** de survenir sur les **DCP** et ainsi provoquer **des impacts (gravité) sur la vie privée** des personnes concernées.

Ces risques pour les droits et libertés des personnes concernées (vus de façon extensive par le groupe de l'article 29) doivent être gérés de façon spécifique ; il s'agit notamment à travers des accès illégitimes à des données, des modifications non désirées de données, des disparitions de données et de l'indisponibilité du traitement de mesurer l'impact potentiel pour les personnes concernées.

Conformément à la méthode EBIOS, les risques concernant la protection des données personnelles seront gérés dès la conception.

Cela permet le cas échéant d'orienter la conception et la réalisation, et de faire des choix en amont ayant un meilleur rapport efficacité/coût.

Dans les premières phases du cycle de vie du projet, seule une étude sommaire est possible. La réflexion doit s'affiner au fur et à mesure de l'avancement des travaux et de la progression de la description du traitement.

Dans un premier temps, il s'agira de dégager les grands enjeux puis d'affiner la description du sujet. L'étude des risques de protection des données personnelles sera effectuée au long du cycle de vie du projet le cas échéant par itérations successives.

Au cours des études d'opportunité et de faisabilité du traitement, il sera possible d'étudier son contexte, d'identifier les enjeux, de déterminer les fonctionnalités, d'établir leurs besoins de sécurité, d'estimer les impacts et d'identifier des sources de menaces.

Lors de la conception générale et de la conception détaillée, les grandes fonctionnalités seront décomposées en fonctions plus fines et en données traitées, les supports seront identifiés, les besoins et les impacts précisés, les sources de menaces développées et consolidées, les menaces et les vulnérabilités étudiées, les risques appréciés, les objectifs identifiés, les mesures de sécurité déterminées et les risques résiduels mis en évidence.

Lors de la phase de réalisation, l'ensemble de l'étude pourra être réajustée en fonction des mesures de sécurité et des risques résiduels.

En phase d'exploitation et jusqu'à la fin de vie du système, les évolutions du contexte (supports, sources de menaces, vulnérabilités...) permettront de gérer les risques en continu.

Il est essentiel que des échanges interviennent entre le RTO et le réseau DPD tout au long du processus afin d'éviter d'éventuelles impasses et d'économiser de futurs coûts de développement. Le réseau DPD devra notamment être associé au choix des mesures prises pour traiter les risques (évitement, transfert, partage, prise).

L'avis du DPD est recueilli formellement in fine et le RTO formalise sa décision de mise en œuvre du traitement.

L'étude d'impact peut aboutir à l'élaboration d'un plan de mesures de correction ou d'amélioration qui feront l'objet d'un suivi.

3. LES DISPOSITIONS INCHANGEES.

Un certain nombre de compétences continueront à être assumées par le DSI.

3.1 Les formalités de « l'article 26 ».

Les traitements qui relèvent du champ de la directive continueront à faire l'objet des formalités définies à l'article 26 de la loi.

Le DPD aura toujours la charge de les transmettre au commissaire du Gouvernement auprès de la CNIL puis à la CNIL mais ceux-ci devront être signés par la structure concernée. Contrairement à l'existant, tous les dossiers devront donc être transmis a priori pour avis à la DSI sous forme dématérialisée.

3.2 Les avis de la CNIL sur des projets d'actes législatif ou réglementaire.

Lorsque qu'un texte prévoit l'avis de la CNIL, le DSI demeure l'étape obligatoire pour l'examen et la transmission du dossier au commissaire du Gouvernement auprès de la CNIL puis à la CNIL.

3.3 Le point de contact unique du commissaire du Gouvernement auprès de la CNIL.

Le DPD est le point de contact du commissaire du Gouvernement.

Il lui transmet en avance de phase les dossiers importants relatifs à la protection des données, si nécessaire avant la saisine de la CNIL.

Le DPD assure les échanges avec les structures concernées des MEF, notamment l'examen des projets de délibération CNIL avant les séances plénières.

Il sert de relai au commissaire lors du visa des textes soumis à la publication au journal officiel.

3.4 Les plaintes des personnes concernées.

Comme aujourd'hui, la CNIL transmet au DPD les plaintes qu'elle reçoit ; le DPD saisira le référent concerné en tant que de besoin.

4. ETAPES ULTERIEURES.

L'objectif sera d'intégrer davantage le process « protection des données personnelles » d'une part (et par ailleurs le process d'homologation de sécurité informatique) au cycle de vie des projets.

Toutefois étant donnés les changements en matière de protection des données personnelles nécessitant une phase d'apprentissage dans les mois à venir, l'existence de cycle de vie adapté à chaque direction et intégrant pour certaines déjà l'homologation de sécuritélil est raisonnable de stabiliser d'abord ces nouvelles démarches avant une nouvelle étape d'intégration. A cette fin, le réseau des référents DPD capitalisera les retours d'expérience pendant les 6 prochains mois.

4.1 Le suivi des risques et la remise en conformité des traitements existants

La réglementation « protection des données » prévoit un suivi des risques soulevés par un traitement ; la jurisprudence de la CNIL considère que ce suivi doit s'effectuer a minima tous les trois ans.

Dans la mesure où les traitements existants n'ont pas fait l'objet ni d'une analyse de risques POD au sens du point 2.2.2.4 ni d'une analyse d'impact (DPIA), il est nécessaire au sein de chaque structure et en prenant l'avis du DPD d'élaborer une programmation triennale en la matière.

L'ordre de priorité sera naturellement fonction de l'ampleur des traitements, de leur aspect stratégique et de leur sensibilité « apparente » en matière de protection des données.

4.2 L'amélioration de l'exercice des droits des personnes concernées.

L'exercice de ces droits a jusqu'ici été traité à façon et au cas par cas. Les demandes étaient quantitativement modérées et s'inséraient souvent dans des processus de gestions courants.

Compte tenu de la dimension médiatique du sujet, l'hypothèse d'une montée en puissance à laquelle il sera difficile de répondre en l'état n'est pas à exclure.

S'agissant des droits d'accès et assimilés, une personne concernée sera en droit le 25 mai 2018 de demander à un responsable de traitement toutes les informations le concernant. Le groupe de travail précité devra donc réfléchir aux moyens de parvenir à une situation satisfaisante sur le plan ministériel, pour permettre de répondre aux demandes des personnes concernées de manière la plus efficace, rapide, traçable et peu coûteuses possible.

4.3 L'amélioration de la sécurité des données personnelles.

La réglementation « protection des données » recommande un certain nombre de techniques pour améliorer la sécurité des données à caractère personnel, et notamment le chiffrement des données, la pseudonymisation et l'anonymisation des données.

Un équilibre reste à trouver entre les contraintes et le coût de ces techniques d'une part, et leurs avantages d'autre part.

Ainsi le chiffrement permet, lors d'une violation de données, d'éviter de devoir assumer les impacts potentiels dommageables mais aussi suspend l'obligation de communiquer l'incident à la CNIL voire aux personnes concernées.

Il faut enfin rappeler que si les sanctions sont largement inexistantes dans la législation actuelle pour

l'inobservance d'une norme de sécurité; il en ira différemment pour un règlement européen qui prévoit des sanctions même en l'absence de faute.

4.4 Les relations avec les sous-traitants.

Le suivi du respect des nouvelles obligations fixées par le règlement devient nécessaire et la mutualisation des expériences au plan ministériel ne pourra que faciliter la transition vers ce nouvel équilibre entre responsable de traitement et sous-traitants.

Il convient de rappeler que le RT doit vérifier que le sous-traitant présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée.

4.5 Mutualisations.

Dans le but de standardiser le process «protection des données personnelles» et de le rendre moins coûteux en ressources, il importe d'identifier tout ce qui est mutualisable dans le cadre de la conformité.

A priori cette action s'orientera autour de trois axes :

- Le regroupement des traitements par mission (finalités) car le pilier « risque » de l'étude d'impact peut regrouper des traitements aux risques POD comparables.

- Le catalogue de données ou de catégories de données avec une sensibilité associée pour permettre une standardisation ministérielle au niveau d'un risque lié à la donnée.

- Une base de connaissances sur la cartographie des risques POD.

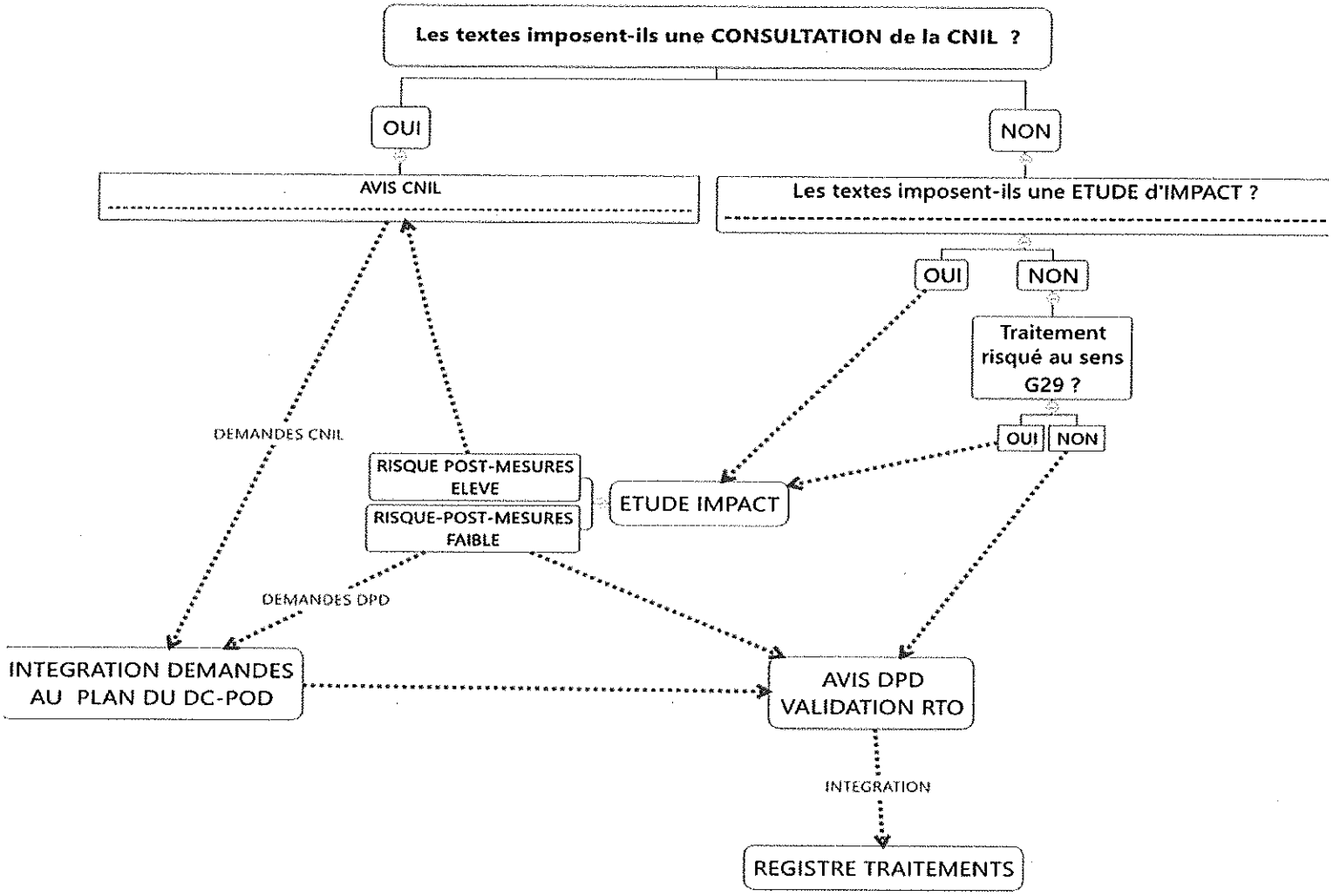
Pour tout complément, les RTO sont invités à solliciter le réseau des DPD dont la constitution est précisée en annexe 1 et peuvent s'adresser au DPD par le mail :

le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr

La Secrétaire générale
des ministères économiques et financiers

Isabelle Braun-Lemaire

Annexe 1	Réseau des référents DPD	
STRUCTURE	REFERENT	SUPPLEANT
AFA	Eric BERNARD	Sarah GEORGE
AIFE	Laurent VIGNALOU	Sandrine LAFFAURIE
APIE	Wilma GALFRE	
CBCM	Thomas GORENC	Joseph BOINNOT
CGEFI	Luc DEGARDIN	
CISIRH	Philippe CUCCURU	
DAE	Gilles DUFOUR	Maxime BOUSSARD
DAJ	Patricia CORITON	VERA Viviane
DB	Esther DESSAINT	
DGAFP	Adrien FRIEZ	Denis ROGY
DGCCRF	Philippe D'AUTHIER-DE-SISGAU	
DGDDI	Virginie DELALANDE	
DGE	Nathalie DENIS	Romain DELASSUS
DGFIP	Valérie GLACE	
DGT	Sandy SANDERS	
DITP	Philippe-Henri MECHET	
DNLF	Johny MARCEL	
IGF	Pierre-Marie CARRAUD	
INSEE	Patrick REDOR	Valérie LEPRETRE
Médiateur Crédit	Christian HABONNEAU	
Médiateur des entreprises	Arnaud LAFONT	
Médiateur MEF	Nadine PARE	Pierre JEANDENAND
SG-SEP	Naima HADDAG	
TRACFIN	Benoit SEGUIN	Alice CHONIK


Les textes imposent-ils une CONSULTATION de la CNIL ?
OUI
NON
AVIS CNIL
Les textes imposent-ils une ETUDE d'IMPACT ?
OUI
NON
Traitement risqué au sens G29 ?
OUI
NON
DEMANDES CNIL
RISQUE POST-MESURES ELEVE
RISQUE-POST-MESURES FAIBLE
ETUDE IMPACT
DEMANDES DPD
INTEGRATION DEMANDES AU PLAN DU DC-POD
AVIS DPD VALIDATION RTO
INTEGRATION
REGISTRE TRAITEMENTS