BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 31 du 1er août 2018

PARTIE PERMANENTE
Administration Centrale

Texte 5

INSTRUCTION ARM/SGA/DAJ/D2P
relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense.

Du *19 juillet 2018*

DIRECTION DES AFFAIRES JURIDIQUES : *sous-direction du droit public et du droit privé.*

INSTRUCTION ARM/SGA/DAJ/D2P relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense.

Du 19 juillet 2018

NOR A R M S 1 8 5 1 4 6 1 J

Référence :

cf. annexe II. Documents de référence.

Pièce(s) Jointe(s) :

Deux annexe.

Classement dans l'édition méthodique : BOEM 160.5.1

Référence de publication : BOC n° 31 du 1er août 2018, texte 5.

SOMMAIRE

Préambule.

Le 25 mai 2018 est entré en vigueur le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (A) 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 (B) (règlement général sur la protection des données : RGPD).

S'agissant d'un règlement, ses dispositions sont directement applicables dans le droit des Etats membres. Néanmoins, le texte laissant un certain nombre de dispositions à la main des Etats, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, dite « loi informatique et libertés » (LIL), reste applicable, dans une version remise à jour par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, complétée par ses décrets d'application.

Les textes relatifs à la protection des données s'appliquent aux traitements (1) de données à caractère personnel (2), constitués de toute opération portant sur des informations permettant d'identifier directement ou

indirectement des personnes physiques.

Un traitement de données à caractère personnel doit respecter les principes de loyauté et de proportionnalité. Ainsi, la personne concernée par un traitement de ses données doit être informée de la mise en œuvre du traitement. De même, les données collectées doivent être proportionnées par rapport à la finalité poursuivie et leur durée de conservation doit être limitée.

De nombreux traitements de données à caractère personnel sont mis en œuvre dans les entités du ministère de la défense.

Ceux-ci peuvent prendre la forme de systèmes d'information (traitements de données structurés), mais également de fichiers tenus à jour en dehors des systèmes d'information (traitements de données non structurés).

Présentation du RGPD

En application de la loi « informatique et libertés », le ministre de la défense était responsable de l'ensemble des traitements mis en œuvre au ministère. Le RGPD s'inscrit dans une logique de responsabilisation des organismes se traduisant par des désignations de responsables de traitement dans chaque état-major, direction et service (EMDS) du ministère.

Avec l'entrée en vigueur du RGPD, la plupart des formalités préalables qui devaient être effectuées auprès de la CNIL avant la mise en œuvre d'un traitement de données personnelles disparaissent ; s'y substitue la tenue à jour, par chaque responsable de traitement, d'un registre des activités de traitement. Celui-ci recense et décrit chaque traitement mis en œuvre, précisant notamment ses finalités, les données traitées et leur durée de conservation, les destinataires des données, les mesures de sécurité mises en place et les modalités d'exercice des droits des personnes concernées.

Le RGPD renforce les droits conférés aux personnes, existant sous le régime de la loi « informatique et libertés » (droit d'accès, de rectification, d'opposition) et les dote de nouveaux droits (limitation, portabilité, droit à l'oubli).

Par ailleurs, le RGPD renforce la sécurisation des données traitées et met à la charge du responsable de traitement la réalisation d'une analyse de risques (dénommée analyse d'impact) pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées.

La présente instruction précise la mise en œuvre du RGPD au sein du ministère de la défense. Elle ne traite pas l'ensemble des problématiques relatives à la mise en œuvre des textes relatifs à la protection des données personnelles.

CHAPITRE PREMIER. LES NOTIONS.

1. LES DONNÉES À CARACTÈRE PERSONNEL.

1.1. **Les données à caractère personnel (art. 4 du RGPD).**

Toute information permettant d'identifier, directement ou indirectement, une personne physique constitue une donnée à caractère personnel. C'est le cas des nom et prénoms des personnes, ainsi que de toute donnée indirectement identifiante et notamment les coordonnées d'une personne (qu'il s'agisse de ses coordonnées professionnelles ou personnelles), les numéros d'identification et le matricule, ainsi que les traces d'utilisation des services informatiques (adresses IP, logs de connexion, etc.).

1.2. **Les données sensibles (art. 9 du RGPD).**

Les données sensibles constituent une catégorie particulière de données à caractère personnel, obéissant à un régime de protection particulier.

Les données sensibles telles que définies par l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant de la loi de protection des données personnelles, sont :

- les données relatives aux opinions des personnes, philosophiques, religieuses ou syndicales ;

- les données relatives aux origines raciales ou ethniques des personnes ;

- les données relatives à la santé des personnes ;

- les données relatives à l'orientation et à la vie sexuelle des personnes ;

- les données biométriques ;

- les données génétiques.

Par principe, les données sensibles ne doivent pas figurer dans un traitement. Leur utilisation doit rester exceptionnelle. Elle doit être limitée et strictement nécessaire à la finalité du traitement.

Le RGPD (3) prévoit les cas dans lesquels des données sensibles peuvent faire l'objet d'un traitement. C'est notamment possible si la personne concernée a donné son consentement (4). Par ailleurs, les données de santé nécessaires à la médecine de prévention peuvent faire l'objet d'un traitement (5).

Nota : les données sensibles définies par la loi informatique et libertés sont distinctes des "données à caractère personnel sensibles « (DCPS) » identifiées par la DGSIC (6) et des données protégées par la mention « diffusion restreinte » ou « confidentiel personnel » (DR-CP) (7). S'agissant de ce type de données, des mesures de sécurité appropriées doivent être mises en œuvre conformément aux préconisations ministérielles.

1.3. **Des données particulières.**

a) Le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR), plus couramment dénommé « numéro de sécurité sociale » fait partie des catégories particulières de données.

En effet, ce numéro présente plusieurs spécificités :

- il est « signifiant ». Il est composé d'une chaîne de caractères qui permettent de déterminer le sexe, le mois et l'année de naissance, le département et la commune de naissance en France ou l'indication d'une naissance à l'étranger ;

- il est unique et pérenne : un seul numéro est attribué à chaque individu dès sa naissance ;

- il est *a priori* fiable, car il est certifié par l'INSEE à partir des données d'état civil transmises par les mairies.

Ce numéro, facile à reconstituer à partir d'éléments d'état civil, et qui rend plus aisées les possibilités de rapprochements de fichiers et facilite la recherche et le tri des informations dans les fichiers, reste associé au risque d'une interconnexion généralisée ou d'une utilisation détournée des fichiers. Cela justifie donc les précautions prises depuis 1978 par le législateur pour encadrer son usage.

Son utilisation fera l'objet d'un régime particulier défini par la loi « informatique et libertés » et par un décret en Conseil d'État qui fixera la liste des traitements ou des catégories de traitement pour lesquels est autorisée, à titre dérogatoire, l'utilisation de ce numéro.

b) Les données relatives aux condamnations pénales et aux infractions ne peuvent faire l'objet d'un traitement en vertu de l'article 777-3 du code de procédure pénale, à moins que celui-ci ne réponde aux conditions posées par l'article 9 de la loi informatique et libertés ou ne soit autorisé par une disposition législative particulière.

2. LE TRAITEMENT DE DONNÉS À CARACTÈRE PERSONNEL (ART. 4 À 6 DU RGPD).

2.1. **Notion de traitement.**

Le RGPD définit la notion de traitement comme étant toute opération, ou ensemble d'opérations, portant sur des données à caractère personnel (8). Ce traitement peut être automatisé ou non automatisé.

Ainsi, les traitements de données suivants sont soumis au RGPD :

- les traitements de données structurés, prenant la forme de systèmes d'information (par exemple : CONCERTO, ALLIANCE, etc.) ;

- les traitements de données non structurés, pouvant prendre la forme de fichiers papier ou de fichiers numériques, tenus à jour à l'aide de logiciels bureautiques (par exemple : utilisation d'Excel pour la gestion des congés bonifiés).

2.2. **Licéité du traitement.**

Un traitement peut être mis en œuvre dès lors qu'il respecte les conditions de licéité décrites ci-dessous.

a) Finalités du traitement. Les finalités d'un traitement doivent être déterminées, explicites et légitimes (9). Un même traitement peut poursuivre plusieurs finalités qu'il convient d'identifier, sous peine de détournement de finalité (10).

b) Proportionnalité des données traitées. Les données traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement (principe de minimisation) (11).

c) Loyauté. Les données sont traitées de manière loyale, licite et transparente (12). Ainsi, les données traitées doivent être strictement nécessaires au traitement mis en œuvre. Le traitement est loyal dès lors que les personnes dont les données figurent dans un traitement en sont informées (cf. 4. du chapitre III).

d) Exactitude des données traitées. Les données figurant dans le traitement doivent être exactes (13) : ainsi, les personnes concernées par un traitement peuvent demander à tout moment à ce que leurs données soient rectifiées (cf. 4. du chapitre III).

e) Sécurité des données. Des mesures de sécurité appropriées sont mises en place sur les données (14) (cf. 3. du chapitre IV).

f) Durée de conservation des données. Les données traitées sont conservées pour une durée n'excédant pas la durée nécessaire au regard des finalités pour lesquelles elles sont traitées (15).Les données peuvent néanmoins être conservées plus longtemps dans la mesure où elles seront traitées exclusivement à des fins archivistiques (16).

2.3. **Fondement juridique du traitement.**

Le RGPD prévoit différents fondements juridiques à la mise en œuvre d'un traitement de données à caractère personnel, parmi lesquels figurent :

- le respect d'une obligation légale ou règlementaire ;

- l'exécution d'un contrat ;

- le consentement de la personne concernée ;

- l'exécution d'une mission d'intérêt public.

Le fondement juridique du traitement influence les cas d'exercice des droits des personnes (en particulier : droit d'effacement et d'opposition – cf. 4. du chapitre III).

La majorité des traitements mis en œuvre au ministère de la défense est nécessaire à l'exécution de sa mission d'intérêt public. Certains traitements nécessitent néanmoins le recueil du consentement de la personne concernée (cf. 4. du chapitre III).

3. LE CHAMP D'APPLICATION DU RÈGLEMENT (ART. 2 ET 3 DU RGPD).

3.1. **Le champs d'application matériel.**

Le RGPD s'applique à l'ensemble des traitements de données à caractère personnel mis en œuvre au ministère de la défense, à l'exclusion des traitements qui entrent dans le cadre d'une activité qui ne relève pas du droit de l'Union (17) : c'est le cas des traitements mis en œuvre aux fins d'assurer la défense et la sécurité nationale (18), finalités qui doivent être entendues strictement. Ces derniers traitements restent toutefois soumis à un régime de formalités préalables à effectuer auprès de la CNIL conformément aux dispositions de l'article 26 de la loi « informatique et libertés » (cf. 7. du chapitre III).

3.2. **Le champ d'application territorial.**

Sont soumis à l'application du RGPD, les traitements mis en œuvre par un responsable de traitement établi sur le territoire de l'Union européenne, que le traitement ait lieu ou non sur le territoire de l'Union (19).

Les traitements de données à caractère personnel mis en œuvre en dehors du territoire de l'Union européenne peuvent être soumis à l'application du RGPD et doivent respecter les dispositions de la loi informatique et libertés lorsqu'elle leur est applicable.

4. LE RESPONSABLE DE TRAITEMENT (ART. 4 ET 24 DU RGPD).

La personne qui détermine les finalités et les moyens (20) du traitement est appelée « responsable de traitement ». Le responsable de traitement assume la responsabilité juridique et supporte les sanctions en cas de non-respect des dispositions du RGPD (cf. 1. du chapitre II).

Le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément aux dispositions du RGPD.

5. LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (ART. 37 À 39 DU RGPD).

La nomination d'un délégué à la protection des données (DPD) est obligatoire dans les organismes publics. Le DPD dispose d'une autonomie renforcée dans l'exercice de ses missions (21). Celles-ci se déclinent en trois volets (cf. 4. du chapitre II) : il conseille et accompagne les responsables de traitement ; il assure le relai entre les responsables de traitement et la Commission nationale de l'informatique et des libertés (CNIL) ; il assure enfin une mission de contrôle.

CHAPITRE II. L'ORGANISATION MINISTÈRIELLE.

1. LE RESPONSABLE DE TRAITEMENT.

1.1. **La désignation des responsables de traitement.**

La désignation des responsables de traitement a été arrêtée par notes de désignation adressées par les EMDS à la DAJ (22) et formalisées par un arrêté du ministre de la défense (23). Cet arrêté pourra être modifié en tant que de besoin, à l'initiative de la direction des affaires juridiques ou à la demande des états-majors, directions et services.

1.2. **Le rôle du responsable de traitement.**

Le responsable de traitement met en place les mesures techniques et organisationnelles appropriées pour assurer la conformité des traitements de données à caractère personnel mis en œuvre dans son périmètre au titre des dispositions de la loi « informatique et libertés » et du RGPD.

Ainsi, il doit être en mesure d'en démontrer la conformité, en cas de contrôle du DPD ou de la CNIL (cf. chapitre III). Pour ce faire, il doit pouvoir présenter son registre des traitements (cf. chapitre III point 1.) et la documentation associée pour chaque traitement, notamment concernant les mesures mises en place pour assurer la sécurité des données (cf. 3 du chapitre III). Ces mesures comprennent notamment les analyses d'impact que le responsable de traitement décide ou non de mener, qu'il rédige et qu'il signe (cf. 2. du chapitre III), ainsi que la documentation relative aux violations de sécurité (cf. 3. du chapitre III).

Il assure en outre le respect des droits des personnes dont les données figurent dans un traitement de son périmètre (en particulier : droit d'accès, droit de rectification, droit de suppression des données les concernant - cf. 4. du chapitre III) : il met en place une procédure interne permettant de donner suite, dans un délai d'un mois, aux demandes d'accès, de rectification, de suppression que lui adresse toute personne concernée et il tient à jour la liste des demandes qui lui sont parvenues, afin de pouvoir les porter à la connaissance du DPD une fois par an.

Le responsable de traitement s'assure de la conformité des traitements relevant de son périmètre vis-à-vis des dispositions du règlement (cf. 1. du chapitre IV relatif à la mise en œuvre des contrôles internes).

2. LE RESPRÉSENTANT DU RESPONSABLE DE TRAITEMENT.

Le responsable de traitement désigne un représentant (et éventuellement un suppléant) et notifie au DPD son nom, prénom et grade ainsi que ses coordonnées téléphoniques et son adresse électronique. Ce représentant est désigné sur la base de ses compétences juridiques et de sa maîtrise des enjeux technico-organisationnels propres à son entité.

Le responsable de traitement informe par ailleurs le DPD en cas de cessation de fonctions de son représentant.

Chaque responsable de traitement peut décider de mettre en place un réseau de correspondants locaux dans les différents services qui lui sont rattachés. Le réseau local est animé par le représentant nommé par le responsable de traitement.

2.1. **Relation avec le délégué à la protection des données.**

Le représentant du responsable de traitement assure le relai entre son organisme d'appartenance (en liaison avec les responsables de traitement) et le DPD du ministère pour toutes les questions relatives à la protection des données personnelles.

2.2. **Missions au sein de son organisme.**

Il a une vision globale de l'ensemble des traitements placés dans le périmètre de son responsable de traitement et il est l'interlocuteur privilégié du DPD.

Il s'assure que le responsable de traitement a pris en compte ses obligations et l'assiste dans sa démarche de mise en conformité. Il tient notamment à jour le registre des traitements (cf. 1. du chapitre III) ouvert dans le système d'information ministériel Sicl@de et transmet au DPD les analyses d'impact élaborées pour les traitements de son périmètre. Il s'assure notamment du respect des droits des personnes et transmet le cas échéant au DPD les éléments nécessaires au traitement des plaintes transmises par la CNIL.

Il assure par ailleurs la sensibilisation des personnels de son entité aux dispositions de la loi « informatique et libertés » et du RGPD.

Le représentant du responsable de traitement contribue aux contrôles internes menés par le responsable de traitement (cf. 1. du chapitre IV).

3. L'AGENT CHARGÉ DE LA EN OEUVRE DU TRAITEMENT.

L'agent chargé de la mise en œuvre du traitement est le responsable de la conduite d'un projet de système d'information (24) (traitement de données structuré) ou l'agent responsable de l'alimentation et de la mise à jour d'un fichier contenant des données à caractère personnel (traitement de données non structuré).

Il est identifié dans le registre, pour chaque traitement recensé et il est à même de fournir au responsable de traitement et à son représentant les informations nécessaires à l'alimentation du registre (cf. chapitre III point 1.) et à la réalisation d'une analyse d'impact (cf. chapitre III point 2.).

4. LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES.

Cette fonction est assurée au ministère de la défense par le directeur des affaires juridiques (cf. arrêté du 13 juin 2018 portant désignation du délégué à la protection des données au sein du ministère des armées et modifiant l'arrêté du 8 avril 2011 portant organisation de la direction des affaires juridiques).

Le DPD est investi d'une mission principale de conseil et d'accompagnement du responsable de traitement. Il peut également conseiller les établissements publics sous tutelle du ministre de la défense, bien qu'il n'assure pas à leur égard la fonction de délégué à la protection des données.

Le DPD est l'unique point de contact de la CNIL et assure donc le relai entre les responsables de traitement et la CNIL. Il a enfin la possibilité de mener des contrôles de conformité des traitements, au regard des dispositions du RGPD.

4.1. **Conseiller.**

Le responsable de traitement qui souhaite obtenir un conseil du DPD sollicite la direction des affaires juridiques (DAJ) pour toute question relative à l'application des dispositions du RGPD, qu'il s'agisse d'une question juridique ou technique. La DAJ prend, le cas échéant, les renseignements nécessaires auprès de ses appuis techniques (cf. point 5.) et apporte une réponse au responsable de traitement qui l'a sollicitée.

Le responsable de traitement saisit obligatoirement le DPD dans les cas suivants :

- réalisation d'une analyse d'impact : le DPD donne un avis formel sur l'analyse réalisée et évalue la nécessité de la présenter à la CNIL (cf. 2. du chapitre III) ;

- mise en œuvre d'un traitement de données sensibles (cf. 1. du chapitre I) ;

- mise en œuvre d'un traitement comprenant le transfert de données à caractère personnel hors de l'Union européenne (cf. 6. du chapitre III).

Le responsable de traitement informe obligatoirement le DPD dans les cas suivants :

- mise en œuvre d'un traitement utilisant une technologie innovante (cf. 2. du chapitre III) ;

- demande d'accès, de rectification ou de suppression : transmission d'un bilan annuel au DPD en janvier de l'année N +1.

Le responsable de traitement peut consulter le DPD à tout moment, notamment sur les questions suivantes :

- tenue à jour du registre des activités de traitement, en particulier : information et conseil en matière d'identification de la finalité du traitement, de l'origine et de la sensibilité des données traitées, de la base juridique du traitement et de la durée de conservation des données ;

- décision de mener une analyse d'impact pour un traitement ;

- suites à donner en cas d'exercice de leurs droits par les personnes concernées par un traitement. Il tient à jour une liste des demandes qui lui sont formulées pour pouvoir transmettre ces éléments sur sollicitation annuelle du DPD ;

- mesures de sécurité à mettre en place sur leurs traitements, à charge pour le DPD de transmettre la question à son appui technique.

À titre expérimental, durant la première année à compter de l'entrée en vigueur du RGPD, le DPD préconise que la mise en œuvre de tout nouveau traitement soit portée à sa connaissance.

4.2. **Accompagner.**

Le DPD assure une formation des représentants des responsables de traitement lors de leur nomination et peut proposer des formations périodiques. Il peut solliciter le concours de ses appuis techniques pour intervenir sur les aspects techniques lors de ces séances d'information.

4.3. **Assurer le relai avec la CNIL.**

Le DPD assure le relai entre la CNIL et le responsable de traitement. Les responsables de traitement ne doivent pas saisir la CNIL directement.

Le DPD est le point de contact de la CNIL sur les questions relatives aux traitements mis en œuvre au ministère. Il assure les consultations préalables auprès de la CNIL prévues par les textes. Il reçoit également les plaintes déposées par des particuliers auprès de la CNIL à l'égard des responsables de traitement du ministère. Il accompagne enfin les agents de la CNIL en cas de contrôle (cf. chapitre IV).

Le responsable de traitement saisit donc obligatoirement le DPD dans les cas suivants :

- maintien de certaines formalités préalables (cf. 7. du chapitre III) ;

- notification à la CNIL des violations de sécurité (cf. 3. du chapitre III).

4.4. **Contrôler.**

Le DPD assure une mission de contrôle des traitements mis en œuvre au ministère, dans les conditions définies au chapitre IV de l'instruction.

5. LES APPUIS TECHNIQUES DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES.

Dans le cadre de ses missions, la direction générale du numérique et des systèmes d'information et de communication (DGNUM) assure la mise à jour des textes ministériels relatifs à la gouvernance des projets informatiques afin de prendre en compte les dispositions du RGPD.

La DGNUM soutient par ailleurs la DAJ pour les questions techniques liées à l'application du RGPD. Le DPD peut solliciter, si nécessaire, d'autres entités chargées de la gestion des systèmes d'information (notamment la DéSIAG).

En outre, la DGNUM, représentée par l'administrateur ministériel des données (AMD), et le DPD se réunissent périodiquement en vue de faire un point sur la mise en œuvre du RGPD au ministère. Le DPD est associé au comité ministériel de gouvernance des données que doit animer l'AMD.

5.1. **Formations.**

La DGNUM intervient sur les aspects techniques lors des actions de formation dispensées par le DPD à destination des représentants des responsables de traitement.

5.2. **Analyse d'impact.**

La DGNUM participe à l'identification des risques associés aux opérations de traitement et formalise un avis sur toute analyse d'impact réalisée par les responsables de traitement du ministère. Chaque analyse lui est transmise à cette fin par le DPD, qui doit lui-même émettre un avis formel tenant compte de l'étude de la DGNUM (cf. 2. du chapitre III).

5.3. **Contrôles.**

La DGNUM participe aux contrôles menés par le DPD, dans les conditions définies au chapitre IV de l'instruction.

6. LES ACTEURS COMPÉTENTS EN MATIÈRE DE VIOLATIONS DE DONNÉES.

En cas d'incident avéré sur des données, la violation est notifiée selon les processus mis en place au ministère pour les incidents de sécurité.

Les procédures seront définies après concertation avec les services compétents.

CHAPITRE III. LA MISE EN OEUVRE DES TRAITEMENTS.

1. LE REGISTRE DES TRAITEMENTS (ART. 30 DU RGPD).

Le registre des traitements remplace les déclarations préalables des traitements, qui étaient effectuées auprès de la CNIL avant l'entrée en vigueur du RGPD. Il est tenu à jour sur un module dédié de l'outil Sicl@de.

Les traitements qui étaient soumis à l'établissement d'une déclaration normale auprès de la CNIL sont désormais consignés dans le registre des traitements ; des formalités préalables (demandes d'avis et d'autorisation) sont maintenues pour certaines catégories de traitements.

La tenue du registre est obligatoire, ainsi que sa mise à jour régulière. Elle est du ressort de chaque responsable de traitement.

a) Initialisation du registre. Pour initialiser son registre dans Sicl@de, le responsable de traitement peut se fonder sur les formalités CNIL existantes et sur la cartographie des traitements effectuée par la DAJ.

b) Saisie des données. Le responsable de traitement détermine le processus de saisie et de validation de ses données dans le registre. Le responsable de traitement est garant de la qualité de son registre.

c) Contenu du registre. Une notice est disponible dans Sicl@de, explicitant les champs du registre. Pour la plupart d'entre eux, des menus déroulants sont proposés. Le registre contient les éléments qui étaient portés à la connaissance de la CNIL par le biais des formalités préalables, avant l'entrée en vigueur du RGPD ainsi que des champs complémentaires, tenant compte des dispositions du RGPD.

Ainsi, figurent dans le registre les éléments suivants :

- identification du traitement

  - nom du traitement ;

  - responsable de traitement ;

  - finalités du traitement (voir 2. du chapitre I) ;

- analyse d'impact (voir 2. du chapitre II) ;

- description du traitement

  - catégories de personnes concernées par le traitement (catégories de personnes dont les données à caractère personnel figurent dans le traitement) ;

  - catégories de données traitées ;

  - catégories de données sensibles (voir 1. du chapitre I) ;

  - origine des données (provenance des données traitées) ;

  - destinataires des données (personnels ou catégories de personnels amenés à prendre connaissance des données traitées [25]) ;

  - durée de conservation des données (voir 1. du chapitre I) ;

  - modalités d'exercice des droits des personnes (voir 4. du chapitre III) ;

  - mesures de sécurité mises en place (voir 3. du chapitre III) ;

  - interconnexion (transmission de données d'un traitement vers un autre traitement, potentiellement pour des finalités différentes) ;

  - sous-traitance (voir 4. du chapitre III) ;

  - transferts de données hors de l'Union européenne (voir 6. du chapitre III).

2. LES ANALYSES D'IMPACT (ART. 35 ET 36 DU RGPD).

2.1. **Les traitements concernés.**

Une analyse d'impact est obligatoire pour les traitements qui présentent une sensibilité particulière (risque élevé pour les droits et libertés des personnes) et qui sont mis en œuvre à compter de l'entrée en vigueur du RGPD. Les références de ces analyses sont mentionnées dans le registre des traitements.

L'analyse n'est pas requise pour les traitements existant avant l'entrée en vigueur du RGPD. Ces traitements devront être mis en conformité dans un délai de trois ans à compter du 25 mai 2018 (délai fixé par la CNIL). Il est toutefois conseillé au responsable de traitement de ne pas attendre l'expiration du délai de trois ans pour initier la réalisation des analyses d'impact.

La CNIL devrait publier deux listes de référence : une liste de référence contenant les catégories de traitements soumis obligatoirement à la réalisation d'une analyse d'impact (liste noire) et une liste de référence contenant les catégories de traitements non soumis à analyse d'impact (liste blanche).

Dans l'attente de la publication des listes de référence, les responsables de traitement se réfèrent aux lignes directrices du G29 (références en annexe), en utilisant les neuf critères proposés comme un faisceau d'indices susceptibles de mener à l'élaboration d'une analyse d'impact : si un traitement réunit deux des neuf critères proposés, l'élaboration d'une analyse d'impact est obligatoire.

Lorsque les listes de la CNIL auront été publiées, les critères du G29 seront utilisés pour les traitements n'ayant pas été envisagés dans les listes proposées.

Les éléments d'interprétation ci-dessous sont donnés à titre indicatif.

Il revient à chaque responsable de traitement de faire une étude au cas par cas pour déterminer la nécessité ou non de mener une analyse d'impact. Le responsable de traitement devra être en mesure de justifier son choix. Lorsque le responsable de traitement décide d'élaborer une analyse d'impact, il en informe le DPD.

a) Le traitement s'applique à grande échelle : si le RGPD fait référence aux traitements de données à niveau national ou supranational, le G29 recommande aux responsables de traitement d'évaluer le champ d'application de ce critère en fonction du nombre de personnes concernées par le traitement, du volume de données traitées, de la permanence ou non de l'activité de traitement et de l'étendue géographique du traitement. La question de l'opportunité de réaliser une analyse d'impact peut se poser pour les traitements de données à caractère personnel concernant l'ensemble des agents du ministère, voire même une grande proportion d'entre eux, si le traitement comprend un volume important de données.

b) Le traitement collecte des données sensibles. Les données sensibles sont celles mentionnées à l'article 9 du RGPD : données relatives à l'origine raciale ou ethnique des personnes, aux opinions politiques, philosophiques, religieuses ou syndicales, à la santé, à la vie sexuelle et à l'orientation sexuelle, aux données biométriques et génétiques (cf. voir 5 du chapitre III). Par principe, ces données ne peuvent faire l'objet d'un traitement. Cependant, le traitement de données sensibles entrant dans le cadre d'une dérogation peut justifier la réalisation d'une analyse d'impact.

Nota : par ailleurs, le G29 considère que la présence de certaines données dans un traitement peut également justifier la réalisation d'une analyse d'impact, bien qu'il ne s'agisse pas de données sensibles au sens des textes. Il peut s'agir de données telles que des données financières, des données de localisation ou des données relatives à la vie personnelle des individus (le G29 cite à ce titre les correspondances privées). La mise en place d'outils de géolocalisation au ministère peut entrer dans le champ d'application de ce critère. Il en va de même pour certains traitements qui font usage des données bancaires des agents.

Concernant les correspondances privées, bien que la messagerie professionnelle puisse faire l'objet d'une utilisation ponctuelle à des fins personnelles (cf. code de bon usage des SIC, référence en annexe), les messages échangés bénéficient d'une présomption de professionnalité selon la jurisprudence. Par ailleurs, la mise en œuvre des messageries au ministère n'est pas considérée comme constituant un traitement de données à caractère personnel. Ainsi, les correspondances privées utilisant les messageries professionnelles des agents du ministère n'entrent pas dans le champ d'application de ce critère.

c) Le traitement engendre des croisements ou des combinaisons de données, pour des finalités différentes : les traitements mis en œuvre au ministère donnant lieu à de nombreuses interconnexions peuvent entrer dans le champ d'application de ce critère.

d) Le traitement met en œuvre une surveillance systématique des individus : les lignes directrices du G29 font référence à la collecte de données via les réseaux ou dans les lieux publics, sans que la personne concernée n'en soit informée. Les traitements de gestion de logs ou les systèmes de vidéosurveillance mis en œuvre au ministère de la défense sont portés au préalable à la connaissance des agents, via le code de bon usage des SIC, publié au Bulletin officiel des armées pour la gestion des logs et par la mise en place d'un affichage pour les systèmes de vidéosurveillance. Ainsi, ces traitements n'entrent pas, de fait, dans le champ d'application de ce critère.

e) Le traitement concerne des personnes vulnérables : si le RGPD fait référence à des traitements de données concernant des enfants, les lignes directrices du G29 évoquent, à titre de personnes vulnérables, les personnes âgées, les personnes déficientes et les employés. La CNIL fait également référence, dans certaines de ses publications, aux employés comme étant des personnes vulnérables.

Le critère du G29 est rempli dès lors qu'il existe un déséquilibre accru entre le responsable de traitement et la personne concernée par le traitement, de telle sorte que cette dernière pourrait avoir des difficultés à faire valoir ses droits, au titre du RGPD. Les agents du ministère ne se trouvent pas dans une position de subordination telle qu'ils puissent être considérés comme étant des personnes vulnérables au sens du RGPD. En effet, ils sont informés des traitements mis en œuvre sur leurs données et sont en mesure d'exercer les droits qui leur sont reconnus par les textes relatifs à la protection des données. Ainsi, ce critère n'est en

principe pas rempli pour les traitements relatifs aux personnels du ministère de la défense.

f) Le traitement consiste en l'évaluation ou la notation d'individus : ce critère fait référence au profilage, consistant à prédire le comportement des personnes, en particulier dans le domaine du marketing et de la consommation. Ainsi, les évaluations et notations réalisées par les ressources humaines et concourant à la gestion de la carrière des agents du ministère n'entrent pas systématiquement dans le champ d'application de ce critère. En effet, la notation des agents est encadrée de garanties posées par les procédures en place ; elle ne donne pas lieu à elle seule à une décision pouvant affecter la carrière des agents et elle est réalisée au cas par cas, sans faire appel à des processus automatisés qui se substitueraient à une décision humaine.

g) Le traitement consiste en une prise de décision automatisée avec effets juridiques : ce critère nécessite des éclaircissements de la part du G29. Les traitements mis en œuvre au ministère de la défense aux fins de l'évaluation annuelle des agents, menée conformément aux processus de ressources humaines en place, n'entrent pas dans le champ d'application de ce critère (cf. point ci-dessus concernant la notation des agents).

h) Le traitement se livre à une utilisation innovante ou à l'application de nouvelles solutions technologiques ou organisationnelles : les lignes directrices du G29 citent à titre illustratif de ce critère l'Internet des objets ou l'utilisation de différentes technologies de reconnaissance biométrique. Les systèmes de reconnaissance biométrique mis en œuvre par l'Etat aux fins d'authentification des personnes restent soumis à l'accomplissement de formalités préalables auprès de la CNIL (cf. 7. du chapitre III). Néanmoins, ce critère peut être rempli en cas de conception ou d'utilisation d'autres types de technologies innovantes par les EMDS du ministère. Le responsable de traitement consulte le DPD en cas de mise en œuvre de ce type de traitement.

i) Le traitement lui-même a pour but d'empêcher une personne d'avoir accès à un service ou de conclure un contrat : le G29 cite, à titre d'exemple, les traitements réalisés par les banques ayant vocation à accorder ou refuser un prêt à ses clients. Les traitements mis en œuvre au ministère de la défense étant fondés sur l'exécution de sa mission d'intérêt public, ils n'ont, pour la plupart, pas pour objet d'empêcher une personne d'avoir accès à un service ou de conclure un contrat.

2.2. **Le contenu de l'analyse d'impact.**

L'analyse d'impact a pour objet de révéler les risques que présente un traitement de données personnelles pour les droits et libertés des individus.

2.2.1. ***Analyses globale.***

Une seule analyse d'impact peut couvrir plusieurs traitements, s'ils poursuivent la même finalité, traitent les mêmes données et ont les mêmes destinataires.

2.2.2. ***Outils.***

La CNIL met en, ligne sur son site internet, un outil, des guides et des modèles permettant au responsable de traitement de mener son analyse d'impact. Néanmoins, le DPD ministériel a élaboré un modèle d'analyse d'impact à l'attention des responsables de traitement du ministère de la défense.

2.2.3. ***Réévaluation.***

L'analyse d'impact est modifiée par le responsable de traitement lorsque son traitement subit des évolutions substantielles, susceptibles de mener à une réévaluation des risques engendrés pour les droits et libertés des personnes. Le responsable de traitement est invité à remettre à jour l'analyse d'impact réalisée initialement pour son traitement à échéance régulière, soit tous les trois ans.

2.3. **La réalisation de l'analyse d'impact.**

2.3.1. ***Élaboration et validation de l'analyse d'impact.***

Le responsable de traitement fait appel à l'agent chargé de la mise en œuvre du traitement (26) pour rédiger l'analyse d'impact, utilisant le modèle fourni par le DPD. Il s'appuie sur la chaine SSI de son entité d'appartenance.

Les opérateurs internes qui assurent des prestations pour le compte du responsable de traitement (notamment : prestation d'hébergement) sont tenus de donner les informations nécessaires au responsable de traitement, afin qu'il puisse mener à bien son analyse d'impact.

Le responsable de traitement signe l'analyse d'impact et la présente au DPD.

Le DPD émet un avis formel sur l'analyse qui lui est présentée, tenant compte de l'avis de la DGNUM qu'il sollicite sur chaque analyse. Le DPD évalue la nécessité de présenter l'analyse d'impact à la CNIL.

La CNIL dispose d'un délai de deux mois, qui peut être prorogé de six semaines, pour rendre un avis sur l'analyse qui lui a été soumise. La CNIL n'a pas vocation à donner une autorisation de mise en œuvre du traitement, la décision appartenant au responsable de traitement, au regard des risques qu'il présente pour la vie privée des personnes concernées. Les agents de la commission peuvent cependant émettre des recommandations quant aux modalités de mise en œuvre du traitement, proposant notamment des mesures permettant de réduire le risque engendré par le traitement.

2.3.2. ***Sanctions.***

Les manquements à l'obligation de réaliser une analyse d'impact, la mauvaise exécution de celle-ci ou le défaut de consultation de la commission en cas de risque élevé révélé par l'analyse sont susceptibles d'être sanctionnés par la CNIL, qui peut notamment prononcer une limitation du traitement (27).

3. LA SÉCURISATION DES TRAITEMENTS.

3.1. **L'obligation générale de sécurité (art. 32 du RGPD).**

Le responsable de traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (28). Le RGPD cite un certain nombre de mesures de sécurité que le responsable de traitement peut choisir de mettre en œuvre, sans que celles-ci ne soient rendues obligatoires (par exemple : pseudonymisation et chiffrement des données).

Le responsable de traitement doit s'assurer de l'intégrité, de la disponibilité et de la confidentialité des données traitées. Il documente les mesures de sécurité qu'il met en œuvre pour chaque traitement de données :

- par le biais du champ dédié dans le registre des traitements ;

- dans l'analyse d'impact lorsque celle-ci est requise.

En cas de contrôle des traitements réalisés par le DPD ou par la CNIL (cf. chapitre IV), les mesures de sécurité mises en place font l'objet de vérifications.

Le choix des mesures de sécurité est déterminé par la sensibilité du traitement mis en œuvre et par la nature des données traitées. Au sein d'un même traitement, les mesures de sécurité mises en place peuvent être de nature différente en fonction des données.

Les opérateurs internes qui réalisent des prestations pour le compte du responsable de traitement (notamment : prestation d'hébergement) sont tenus d'assurer le niveau de sécurité des données qui leur est demandé par le responsable de traitement.

3.2. **La notification des violations de données (art. 33 et 34 du RGPD).**

Les violations de données intervenant sur un traitement de données à caractère personnel et engendrant un risque pour les droits et libertés des personnes sont notifiées à la CNIL (29) et à la personne concernée par la violation, sauf dérogation (30). Le responsable de traitement s'assure de la notification des violations de sécurité. Il conserve les documents qui s'y rapportent, permettant de démontrer la conformité de ses traitements vis-à-vis des dispositions du RGPD.

3.2.1. ***Notification à la CNIL.***

Les violations de sécurité entraînant un risque pour les droits et libertés des personnes doivent faire l'objet, dans les 72 heures, d'une notification à la CNIL. Le responsable de traitement saisit à cet effet le DPD ministériel qui se rapprochera de la CNIL (cf. 4. du chapitre II).

3.2.2. ***Contenu de la notification.***

La notification de la violation décrit la violation, ses conséquences possibles et les mesures prises par le responsable de traitement pour y remédier.

3.2.3. ***Notification à la personne concernée.***

Si la violation de sécurité est susceptible d'engendrer un risque élevé pour les personnes concernées, le responsable de traitement notifie la violation à la personne concernée. Il décrit la violation, ses conséquences possibles pour la sécurité des données et les mesures prises pour y remédier.

Si le responsable de traitement décide de ne pas notifier la violation à la personne concernée, la CNIL peut le lui imposer. Toutefois, ne sont pas soumis à ce régime les traitements entrant dans le cadre des dérogations prévues par l'article 24 de la loi « informatique et libertés » et dont un décret doit fixer la liste. C'est le cas par exemple des violations intervenant sur des données appartenant à des personnes protégées par le respect de l'anonymat au titre de l'article 39 sexies de la loi du 29 juillet 1881 (C) sur la liberté de la presse.

4 LES DROITS DES PERSONNES (ART. 6 ET 7 ; 12 À 22 DU RGPD).

Le responsable de traitement est tenu de donner suite aux demandes d'accès, de rectification et, le cas échéant de suppression des données qui sont formulées au titre du RGPD.

4.1. **Les droits des personnes.**

4.1.1. ***Information.***

Le responsable de traitement doit assurer l'information des personnes concernées par la mise en œuvre d'un traitement de leurs données à caractère personnel, à charge pour lui de déterminer la forme de l'information adéquate, en fonction du traitement (affichage, mention sur formulaire ou sur site internet, etc.).

Les personnes doivent être informées des finalités du traitement, des catégories de données à caractère personnel traitées, des destinataires des données, de la durée de conservation des données et des modalités d'exercice de leurs droits par les personnes concernées. Ces informations figurent dans le registre des traitements.

Le responsable de traitement doit être en mesure de démontrer qu'il a procédé à l'information des personnes, conformément aux dispositions du RGPD.

4.1.2. ***Accès et rectification.***

Le responsable de traitement donne suite aux demandes d'accès et de rectification dans un délai d'un mois (31) à compter de la formulation de la demande par la personne concernée. Si la demande est imprécise, il peut demander un complément d'information qui suspend le délai.

Le droit d'accès permet à toute personne concernée par le traitement de ses données à caractère personnel d'en demander la communication au responsable de traitement. Le droit de rectification permet à la personne concernée de demander au responsable de traitement à ce que ses données soient corrigées ou complétées. Les droits d'accès et de rectification peuvent être exercés à tout moment et le responsable de traitement est tenu d'y donner suite, quel que soit le traitement concerné, sous la forme souhaitée par le demandeur.

4.1.3. ***Exception au droit d'accès.***

Le responsable de traitement n'est pas tenu de donner suite aux demandes manifestement infondées ou excessives, à charge pour lui d'en démontrer le caractère infondé ou excessif.

Par ailleurs, seuls les documents achevés sont communicables : ainsi, pour les documents préparatoires qui sont rédigés dans le cadre des traitements relatifs à la gestion des ressources humaines, le responsable de traitement n'est tenu de communiquer qu'au moment où la donnée devient définitive.

En cas de doute, le responsable de traitement demande conseil au DPD.

4.1.4. ***Suppression.***

Le responsable de traitement porte à la connaissance des agents leur possibilité de s'opposer au traitement ou de demander à ce que leurs données soient effacées (cf. ci-dessus : information des personnes).

Si le traitement est fondé sur le consentement de la personne, le droit à l'effacement (ou « droit à l'oubli ») sera applicable (32). En revanche, si le traitement est nécessaire à l'exécution d'une mission d'intérêt public (ce qui est en principe le cas des traitements mis en œuvre par le ministère), ce droit n'est pas applicable, la personne concernée pouvant seulement exercer son droit d'opposition (33).

Le responsable de traitement ne pourra utiliser les données d'un agent ayant exercé son droit d'opposition que s'il existe des motifs légitimes au traitement, qui prévalent sur les intérêts et les droits de la personne concernée, notamment les traitements répondant à une obligation légale ou nécessaires à l'exécution d'une mission d'intérêt public (34) (par exemple : SIRH).

4.1.5. ***Consentement.***

Le RGPD prévoit les modalités de recueil du consentement de la personne concernée (35), pour les traitements fondés sur le consentement (36). Les traitements mis en œuvre au ministère de la défense étant fondés sur l'exécution de sa mission d'intérêt public, le consentement des personnes concernées n'est pas requis dans la plupart des cas.

Toutefois, la mise en œuvre de certains traitements requiert néanmoins une réflexion de la part du responsable de traitement, sur la nécessité d'obtenir le consentement des personnes concernées (notamment : mise en œuvre de sites internet ou de traitements de données non obligatoires, fondés sur la volonté de la personne).

De même, le responsable de traitement qui se livre à la collecte de données sensibles au sens de l'article 9 du RGPD, fondée sur le consentement de la personne concernée, doit être en mesure de prouver son obtention. Le RGPD prévoit que le consentement est donné par déclaration écrite (y compris par voie électronique) ou orale de la personne concernée (37). Il est néanmoins conseillé aux responsables de traitement d'obtenir le consentement de la personne concernée par écrit.

4.1.6. ***Limitation.***

Le RGPD prévoit un droit à la limitation des données. Celui-ci permet à la personne concernée de demander au responsable de traitement à ce que ses données soient conservées, mais non traitées. Les cas dans lesquels le droit à la limitation du traitement peut être exercé sont limités (38).

4.1.7. ***Portabilité.***

Le RGPD prévoit un droit à la portabilité des données qui permet à toute personne concernée par un traitement de ses données d'en demander la restitution sous format lisible au responsable de traitement, ou le transfert vers un nouveau responsable de traitement.

Ce droit ne s'applique pas en principe au traitement nécessaire à l'exécution d'une mission d'intérêt public.

4.2. **La mise en oeuvre des droits des personnes.**

4.2.1. ***Procédure.***

Pour pouvoir exercer ses droits, la personne concernée doit prouver son identité auprès du responsable de traitement. Celui-ci lui communique uniquement les données la concernant. Si le responsable de traitement dispose d'une grande quantité de données relatives à la personne concernée, il peut lui demander de préciser sa demande (39).

Si la demande est formulée par voie électronique, le responsable du traitement est tenu d'y répondre dans les mêmes formes et de transmettre à la personne concernée, en plus des informations visées ci-dessus, une copie des données la concernant. Le responsable de traitement peut demander le paiement de frais raisonnables basés sur les coûts administratifs, pour toute copie supplémentaire (40) .

Outre la copie de ses données, le responsable de traitement communique à l'agent les informations suivantes (cf. article 15 du RGPD) :

- les finalités du traitement ;

- les catégories de données collectées ;

- les destinataires des données ;

- la durée de conservation des données.

De plus, le responsable de traitement informe l'agent concerné de son droit de rectification et le cas échéant, de son droit de suppression. Il lui indique la possibilité d'introduire un recours devant la CNIL.

Le responsable de traitement doit être en mesure de prouver qu'il a donné suite aux demandes d'accès et de rectification qui lui sont adressées.

4.2.2. ***Obligation de notification.***

L'exercice de leur droit de rectification, d'effacement ou de limitation par les personnes concernées doit être notifié par écrit à chaque destinataire des données identifié dans le registre.

Les modalités de la notification sont décrites dans la procédure interne à chaque entité, décrivant la mise en œuvre des droits des personnes. Le responsable de traitement doit être en mesure de démontrer qu'il a procédé à la notification demandée, pour chaque demande d'accès, de rectification ou de suppression des données qui lui parvient.

4.3. **Les obligations du responsables de traitement.**

Pour chaque traitement, le responsable identifie, dans le registre, le service auprès duquel s'exercent les droits des personnes. Il indique les coordonnées de la personne à contacter et porte cette information à la connaissance des intéressés (cf. point 4.1.1. ci-dessus sur l'information des personnes).

4.3.1. ***Processus interne.***

Il est conseillé au responsable de traitement de définir un processus interne de mise en œuvre des droits des personnes. Celui-ci doit identifier les modalités d'information des personnes, en fonction des traitements mis en œuvre, les personnes à même de donner suite aux demandes d'accès, de rectification, de suppression, en fonction des traitements de données concernés, ainsi que les conditions de la notification de ces demandes à l'ensemble des destinataires identifiés pour les traitements concernés par une demande d'accès, de rectification ou de suppression.

4.3.2. ***Sollicitation du délégué à la protection des données.***

Tous les ans, le responsable de traitement adresse à la DAJ un bilan des demandes d'exercice de leurs droits par les personnes concernées pour les traitements relevant de son périmètre. Ce bilan doit être transmis en janvier de l'année N + 1. Il contribuera à la mesure de la conformité des organismes du ministère aux dispositions de la loi « informatique et libertés » et du RGPD.

5. LA SOUS-TRAITANCE (ART.28 À 30 DU RGPD).

Le sous-traitant au sens du RGPD est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement (41) . Dès lors, le sous-traitant peut être un opérateur externe ou interne au ministère de la défense. L'opérateur interne est qualifié de sous-traitant si un acte juridique reconnu par le droit de l'Union ou par le droit d'un Etat membre (42) lie les deux parties.

Le RGPD prévoit la possibilité d'engager la responsabilité du sous-traitant en cas de non-conformité vis-à-vis des dispositions du RGPD.

5.1. **Les contrats de la commande publique.**

5.1.1. ***Clauses de confidentialité.***

Le responsable de traitement qui confie la mise en œuvre de traitements de données à caractère personnel pour son compte à un opérateur privé, en vertu d'un contrat de la commande publique, applique les dispositions du RGPD relatives à la sous-traitance.

Dès lors, il est tenu d'insérer des clauses de confidentialité (43) dans le contrat qui le lie à son sous-traitant. Celles-ci permettent de garantir la mise en place, par le sous-traitant, des mesures de sécurité nécessaires, en fonction du traitement de données à caractère personnel qu'il effectue pour le compte du responsable de traitement.

5.1.2. ***Registre.***

De son côté, le titulaire du marché est tenu de renseigner son propre registre des traitements. Il est conseillé au responsable de traitement de vérifier la conformité du registre du titulaire par rapport à son propre registre. Le responsable de traitement peut être sollicité par le sous-traitant pour lui apporter les informations nécessaires à la mise à jour de son registre.

5.1.3. ***Prise en compte de la vie privée dès la conception (« Privacy by design »).***

Le RGPD encourage la prise en compte de la règlementation sur les données à caractère personnel dès la conception du système d'information (44). Le responsable de traitement insère des clauses de « *privacy by design* » dans les documents du marché. Il consulte si nécessaire le DPD sur ce point.

5.2. **Les contrats signés entre différents services de l'administration.**

5.2.1. ***Délégation de gestion.***

Deux entités du ministère liées par un acte juridique reconnu par le droit français appliquent les dispositions du RGPD relatives à la sous-traitance. C'est le cas notamment des entités liées par une convention de délégation de gestion.

Le régime des délégations de gestion est défini par le décret n° 2004-1085 du 14 octobre 2004 (D) relatif à la délégation de gestion dans les services de l'État. L'article 1er du décret définit la délégation de gestion comme étant « l'acte par lequel un ou plusieurs services de l'État confient à un autre service de l'État, pour une durée limitée éventuellement reconductible, la réalisation, pour leur compte, d'actes juridiques, de prestations ou d'activités déterminées concourant à l'accomplissement de leurs missions ».

Ainsi, des clauses de confidentialité doivent être intégrées dans ces contrats.

Le service délégataire apparaît dans le registre du responsable de traitement dans le champ dédié à la sous-traitance. De son côté, le délégataire recense le traitement qu'il effectue pour le compte du responsable de traitement dans un registre distinct, qu'il tient à jour sur un fichier bureautique séparé et qu'il transmet au DPD ministériel une fois par an. Figurent dans son registre : l'identification du responsable de traitement, le nom du traitement qu'il effectue pour son compte, les mesures de sécurité des données et le cas échéant, les transferts de données hors de l'Union européenne.

5.2.2. ***Autres contrats.***

Il existe au sein du ministère de la défense d'autres moyens de contractualisation pouvant prendre la forme, par exemple, de contrats de service. Ceux-ci ne constituant pas des actes juridiques reconnus par le droit de l'Union européenne, la notion de sous-traitant au sens du RGPD ne trouve pas à s'appliquer.

Les entités liées par un contrat de service peuvent recourir à l'insertion de clauses de confidentialité, à titre de bonne pratique, bien que le contrat de service ne soit pas considéré comme un acte juridique formalisant une relation de sous-traitance entre les deux parties.

Les opérateurs internes qui assurent des prestations pour le compte du responsable de traitement (tel que l'hébergement) sont néanmoins tenus d'assurer le niveau de sécurité des données qui leur est demandé par le responsable de traitement.

Le traitement reste recensé dans le registre du responsable de traitement.

6. LES TRANSFERTS DE DONNÉES HORS UNION EUROPÉENNE (ART. 44 ET SUIVANTS DU RGPD).

Le responsable de traitement ne peut transférer des données hors de l'Union européenne, sans s'assurer que l'État, l'organisme (public ou privé) ou l'organisation internationale destinataire est en conformité avec les dispositions du chapitre V du RGPD.

Ainsi, le destinataire des données offre un niveau de protection adéquat des données :

- s'il bénéficie d'une décision d'adéquation de la Commission européenne (45) ;

- s'il présente des garanties appropriées. Les garanties appropriées doivent conduire à un niveau de sécurisation des données suffisant et prévoir la prise en compte des droits des personnes (cf. 4. du chapitre III de l'instruction). Les garanties appropriées peuvent prendre la forme de clauses-types à insérer dans les contrats de transferts, soumis à autorisation de la CNIL. L'adoption de règles d'entreprises contraignantes ou de codes de conduite par l'organisme destinataire des données peuvent également permettre d'apporter les garanties suffisantes nécessaires au transfert de données.

Le responsable de traitement qui envisage un transfert de données hors de l'Union européenne l'indique dans son registre, dans le champ correspondant. Il saisit obligatoirement le DPD.

7. LES FICHIERS SOUMIS À DES FORMALITÉS PRÉALABLES AUPRÈS DE LA CNIL.

Trois catégories de traitement de données sont particulièrement concernées par le maintien de formalités préalables auprès de la CNIL : les traitements de données de santé, les traitements de données biométriques ou génétiques mis en œuvre par l'État aux fins d'authentification des personnes et les traitements qui intéressent la défense et la sécurité nationale au sens de l'article 26 de la loi informatique et libertés (fichiers de souveraineté) (46).

Le responsable de traitement saisit obligatoirement la DAJ lorsqu'il envisage de mettre en œuvre de tels traitements.

CHAPITRE IV. CONTRÔLES ET SANCTIONS.

1. LES CONTRÔLES INTERNES.

1.1. **Les contrôles du responsable de traitement.**

Le responsable de traitement s'assure de la conformité des traitements qu'il met en œuvre vis-à-vis des dispositions du RGPD. Il peut à ce titre, dans le cadre de la mise en œuvre du contrôle interne, du ressort de chaque EMDS du ministère (47), mener des audits internes qui lui permettent d'évaluer sa conformité par rapport aux recommandations émises par le DPD (cf. point suivant).

Le responsable de traitement doit être en mesure de démontrer la conformité des traitements qu'il met en œuvre aux dispositions du RGPD.

Pour ce faire, il conserve dans un dossier associé à chaque traitement, l'ensemble des documents participant à la description du traitement, comprenant notamment :

- la fiche de traitement dans Sicl@de ;

- l'analyse d'impact si elle a été réalisée (ou les éléments justifiant la décision du responsable de traitement de ne pas réaliser d'analyse d'impact pour son traitement) ;

- les documents relatifs à la mise en œuvre des droits des personnes ;

- la documentation relative à la sous-traitance.

1.2. **Les contrôle du délégué à la protection des données.**

Le DPD est chargé de veiller au respect du règlement européen et aux dispositions de droit national en matière de protection des données par le responsable de traitement.

Il émet à ce titre des recommandations à destination du responsable de traitement. Les recommandations du DPD peuvent être émises à titre individuel, vers le responsable de traitement concerné ou elles peuvent être diffusées de manière plus générale à l'ensemble des responsables de traitement du ministère et à son réseau de représentants.

Le DPD s'assure de la conformité des traitements par le biais du registre : celui-ci lui permet d'identifier les traitements présentant un risque particulier pour les droits et libertés des personnes et de vérifier la mise en œuvre des mesures adéquates (notamment : mise en place des mesures de sécurité nécessaires, réalisation d'une analyse d'impact).

La mise en œuvre des recommandations du DPD par le responsable de traitement peut faire l'objet de contrôles sur place, en vue d'améliorer la conformité des traitements du ministère, vis-à-vis des dispositions du RGPD. Ainsi, le DPD peut être amené à s'assurer, auprès du responsable de traitement :

- de la tenue à jour du registre des activités de traitement ;

- de la réalisation des analyses d'impact sur la protection des données lorsqu'elles sont nécessaires ;

- de l'existence des documents relatifs à l'information des personnes (le cas échéant : modèle de recueil du consentement, preuve des consentements) ;

- de l'existence des documents permettant de décrire les mesures de sécurité mises en œuvre sur le traitement ;

- du respect des droits des personnes ;

- de l'existence des documents qui définissent les rôles et les responsabilités des acteurs concernés :

    - procédure interne en cas de violation des données ;

    - procédure interne permettant de répondre aux demandes d'accès, de rectification ou de suppression des données ;

    - procédure interne décrivant les modalités d'alimentation du registre des activités de traitement.

En cas de contrôle sur place, réalisé par le DPD, la DGNUM peut être sollicitée et s'assure du respect, par le responsable de traitement, de la sécurité et de la confidentialité des données, en vérifiant la conformité et l'existence des moyens mis en œuvre, notamment :

- les caractéristiques des applications (architecture des moyens techniques, langages utilisés) par rapport au cadre de cohérence technique du ministère (CCT) ;

- le dossier de sécurité tenue par le RSSI et plus particulièrement la décision d'homologation, la date du dernier audit SSI et la mise en œuvre le cas échéant du plan d'action associé ;

- la conformité des mesures organisationnelles et physiques mises en place au regard du dossier de sécurité et notamment l'existence des « procédures d'exploitation de sécurité » (PES) ;

- la conformité et la mise œuvre des moyens techniques permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

- la conformité et la bonne application des mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des équipements informatiques et des logiciels informatiques ;

- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

- les procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;

- l'évaluation des pratiques et la mise en place de procédures concernant notamment les violations de données.

2. LES CONTRÔLES DE LA CNIL (ART. 57 ET 58 DU RGPD).

Le RGPD prévoit la possibilité pour les autorités nationales de contrôle de contrôler l'application du règlement par les organismes publics et privés relevant de son champ de compétence.
Ainsi, la Commission nationale de l'informatique et des libertés (CNIL) conserve les pouvoirs de contrôle dont elle était investie avant l'entrée en vigueur du RGPD. A ce titre, elle peut effectuer des contrôles sur

place sur les traitements mis en œuvre au ministère de la défense. Elle sollicite pour ce faire le DPD ministériel qui l'accompagne lors des contrôles.

Dans le cadre de sa mission de contrôle, la CNIL peut notamment :

- accéder aux locaux du ministère ou de ses sous-traitants ;

- obtenir la communication de toute documentation utile au contrôle ;

- obtenir l'accès aux données à caractère personnel traitées, nécessaires à l'accomplissement du contrôle ;

- mener des enquêtes sous la forme d'audits sur la protection des données.

Les agents de la CNIL investis d'une mission de contrôle sont habilités à recevoir communication des informations demandées.

3. LES SANCTIONS.

Le non-respect des dispositions du RGPD peut donner lieu à des sanctions administratives prononcées par la CNIL et à des sanctions pénales, prévues par le code pénal.

3.1. **Sanctions de la CNIL (articles 59, 84 et 84 du RGPD).**

En cas de non-conformité, la CNIL peut prononcer l'une des mesures suivantes :

- un rappel à l'ordre ;

- une injonction de mettre en conformité le traitement avec les dispositions de la loi « informatique et libertés » et du RGPD ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;

- une limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation (sauf pour les traitements intéressant la sûreté de l'État ou la défense) ;

- la suspension d'un flux de données hors de l'Union européenne (cf. chapitre III point 6.).

Les traitements mis en œuvre par l'État ne sont pas susceptibles de donner lieu au prononcé d'une sanction pécuniaire.

3.2. **Sanctions pénales (art. 226-16 à 226-24 du code pénal).**

Le non-respect des textes relatifs à la protection des données est susceptible de constituer un délit, passible de cinq d'emprisonnement et 300 000 euros d'amende.

Ainsi, sont notamment sanctionnés :

- le fait de conserver des données au-delà de la durée prévue (48) ;

- le détournement de finalité (49) ;

- le fait de procéder à un transfert illicite de données hors de l'Union européenne (50).

Pour la ministre des armées et par délégation :

L'adjointe à la directrice des affaires juridiques,

Camille FAURE.

(A) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (n.i. BO ; JO de l'Union Européenne n° L119/1 du 4 mai 2016).

(B) n. i. BO ; JO de l'Union Européenne n° L281 du 23 novembre 1995, page 31.

(C) n.i. BO ; JO du 30 juillet 1881.

(D) n.i. BO ; JO n° 241 du 15 octobre 2004, page 17560, texte n° 1.

(1) Article 4 point 2) du RGPD : « traitement », 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, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

(2) Article 4 point 1) du RGPD : « données à caractère personnel », 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 à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

(3) Article 9 point 2.

(4) Article 9 point 2 a).

(5) Article 9 point 2 h).

(6) « Données à caractère personnel sensibles » identifiées par la DGNUM comme étant l'association de données à caractère personnel de militaires ou d'agents du ministère de la défense d'ordre professionnel (statut, etc.) à des données à caractère personnel d'ordre privé (adresse familiale, etc.) au sein de bases de données accessibles via l'Intradef ou l'Internet (cf. note 598/DEF/DGSIC/SDSSI/-- du 25 octobre 2016).

(7) Article 5 de l'arrêté du 23 juillet 2010 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale.

(8) Article 4 point 2 du RGPD.

(9) Article 5 point 1 b) du RGDP.

(10) Article 226-21 du Code pénal.

(11) Article 5 point 1 c) du RGDP.

(12) Article 5 point 1 a) du RGPD.

(13) Article 5 point 1 d) du RGPD.

(14) Article 5 point 1 f) du RGPD.

(15) Article 5 point 1 e) du RGPD.

(16) Article 5 point 1 e) du RGPD.

(17) Article 2 point 2 a) du RGPD.

(18) Considérant 16 du RGPD.

(19) Article 3 point 1 du RGPD.

(20) Moyens techniques, humains, financiers.

(21) Considérant 97 du RGPD.

(22) Note n° 001I18001460/ARM/SGA/ du 15 février 2018.

Note n° DGA01D18024295 DGA/ADM.

Note n° D-18-000729/ARM/EMA/PLANS/CPI/--.

(23) Arrêté du 13 juin 2018 fixant la liste des responsables de traitement au sein des états-majors, directions et services et des organismes qui leur sont rattachés.

(24) Identifié en tant que responsable fonctionnel ou agent chargé de la mise en œuvre du traitement dans le registre.

(25) Article 4 point 9 du RGPD : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ».

(26) Responsable de projet.

(27) Article 58 point 1° - f) du RGPD.

(28) Article 32 du RGPD.

(29) Article 33 du RGPD.

(30) Article 34 du RGPD.

(31) Article 12 point 3 du RGPD.

(32) Article 17 du RGPD.

(33) Article 21 du RGPD.

(34) Considérant 65 du RGPD.

(35) Article 7 du RGPD.

(36) Article 6 1a) du RGPD.

(37) Considérant 32 du RGPD.

(38) Article 18 du RGPD : le droit à la limitation s'applique si la personne concernée exerce son droit de rectification, si le traitement est illicite, si la personne concernée souhaite que ses données soient conservés pour exercer un droit en justice, si la personne concernée a exercé son droit d'opposition.

(39) Considérant 63 du RGPD.

(40) Article 15 point 3 du RGPD.

(41) Article 4 point 8 du RGPD.

(42) Article 28 point 3 du RGPD.

(43) Article 28 point 3 du RGPD.

(44) Article 25 du RGPD.

(45) Bénéficient d'une décision d'adéquation de la Commission les Etats suivants : Andorre, Argentine, Canada, Iles Féroé, Ile de Man, de Guernesey, de Jersey, Israël, Uruguay et Suisse.

(46) Les fichiers demeurent soumis à l'article 26 de la loi informatique et libertés et, à ce titre, doivent être soumis pour avis à la CNIL et faire l'objet d'un acte réglementaire.

(47) Conformément aux textes d'organisation des EMDS.

(48) Article 226-20 du Code pénal.

(49) Article 226-21 du Code pénal.

(50) Article 226-22-21 du Code pénal.

ANNEXE I.

SIGLES UTILISÉS.

DAJ = direction des affaires juridiques (SGA)

DCP = données à caractère personnel

DéSIAG : délégation des systèmes d'information d'administration et de gestion

DGNUM : direction générale du numérique et des systèmes d'information et de communication

DGSIC : direction générale des systèmes d'information et de communication

DPD = délégué à la protection des données (ou DPO = *data protection officer*)

DPID = direction de la protection des installations de défense

DRSD = direction du renseignement et de la sécurité de la défense

EMDS = états-majors, directions et services du ministère

G29 = groupe réunissant les autorités de contrôle des 29 Etats membres de l'Union européenne

IM = Instruction ministérielle

RGPD = règlement général sur la protection des données

RH = ressources humaines

SI = Système d'information

SIRH : système d'information de gestion des ressources humaines

ANNEXE II.

DOCUMENTS DE RÉFÉRENCE.

- 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) – RGPD.

- Code des relations entre le public et l'administration : livre III sur l'accès aux documents administratifs et la réutilisation des informations publiques.

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Décret n° 2004-1085 du 14 octobre 2004 relatif à la délégation de gestion dans les services de l'Etat (n.i. BO ; JO n° 241 du 15 octobre 2004, page 17560, texte n° 1.).

- Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Décret n° 2007-914 du 15 mai 2007 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Arrêté du 23 juillet 2010 (A) portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale.

- Arrêté du 22 octobre 2014 relatif à la mise en œuvre, par le ministère de la défense, d'un traitement automatisé dénommé « intranet défense ».

- INSTRUCTION ministérielle n° 2003/DEF/DGSIC du 20 novembre 2008 portant code de bon usage des systèmes d'information et de communication du ministère de la défense (parue au Bulletin officiel des armées du 9 janvier 2009).

- INSTRUCTION N° 2008/DEF/DGSIC du 10 juillet 2013 fixant les modalités d'approbation et de suivi des systèmes d'information et de communication.

- INSTRUCTION MINISTERIELLE n° 2004/DEF/DGSIC du 14 décembre 2009 relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la défense.

- INSTRUCTION ministérielle n° 900/DEF/CAB/-- du 26 janvier 2012 relative à la protection du secret de la défense nationale au sein du ministère de la défense.

- DIRECTIVE 27/DEF/DGSIC du 24 janvier 2013 portant sur l'homologation des systèmes d'information du ministère de la défense.

- POLITIQUE DE SECURITÉ DES SYSTÈMES D'INFORMATION DES ARMÉES du 8 juillet 2016 N° D-16007151/DEF/EMA/SCOPS/CYBER/-- .

- Lignes directrices du G29 adoptées le 4 avril 2017 concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679.

(A) n.i. BO ; JO n° 184 du 11 août 2010, page 14718, texte n° 1.