ALERION.LEXPRESS

FLASH DU CABINET ALERION

AVRIL 2019

PROTECTION DES DONNÉES

Mentions « militaires » dans les fichiers : moins de deux mois pour les supprimer

Depuis le 1er avril 2019, les traitements de données personnelles liées aux militaires (DCPM) font l'objet d'un nouveau régime de protection codifié aux articles L. 4123-9-1 et R. 4123-45 et suivants du Code de la défense.

Ce nouveau régime concerne toutes les entreprises et organisations qui collectent **la profession** de leurs clients et dont les clients peuvent être **militaires** : banques, assurances, mutuelles, organismes de formation, universités, programme de fidélité, etc. **Il nécessite une action avant le 21 juin 2019.**

Dans un contexte de menace terroriste et de risque de failles de sécurité informatique, le gouvernement français a souhaité protéger spécifiquement les données personnelles des militaires. Toutefois, ces mesures avaient été critiquées en raison de leur incohérence avec le RGPD.

Saisissant l'opportunité du vote de la loi n°2018-493 du 20 juin 2018 dite « CNIL 3 » pour l'adapter au RGPD, le dispositif de protection des données à caractère personnel de militaires (DCPM) a été revu par le Gouvernement afin de « *concilier l'impératif de sécurité des militaires qui a prévalu à la mise en œuvre de ce dispositif et l'objectif d'allégement des obligations pesant sur les opérateurs privés* ».

Le décret n°2018-932 du 29 octobre 2018 entré en vigueur le 1er avril 2019 précise donc les nouvelles obligations auxquelles doivent se conformer les responsables de traitements de DCPM.

La définition des DCPM – Une DCPM est **toute donnée qui permet, à sa seule lecture, de révéler la qualité de militaire de la personne concernée**, de façon explicite (grade, état de militaire, photo de la personne en tenue, etc.) ou implicite (abréviation ou code interne à l'entreprise). Mise en relation avec d'autres données personnelles d'identification (nom, adresse, etc.), une telle donnée permet d'identifier directement ou indirectement une personne militaire. Les données personnelles des civils de la défense ne constituent donc pas des DCPM.

Les responsables de traitement concernés – Sont concernés par le dispositif de protection, les opérateurs procédant à des traitements concernant des militaires, à moins que ces traitements soient mis en œuvre pour le compte de l'Etat, des collectivités territoriales et de leurs groupements, ainsi que des associations à but non lucratif. Les opérateurs concernés sont donc principalement ceux qui ne traitent pas des DCPM pour les besoins du service public (banques, assurances, mutuelles, organismes de formation, universités, programme de fidélité, etc.).

Le caractère strictement nécessaire de la collecte – Conformément au respect du principe de minimisation de la collecte (article 5.1 RGPD), les responsables de traitements concernés doivent, en premier lieu, vérifier que la collecte de DCPM est absolument nécessaire à l'une des finalités du traitement mis en œuvre.

Si cette donnée n'est pas nécessaire à la finalité du traitement, toutes les données révélant la qualité de militaire dans l'ensemble des fichiers concernés devront être supprimées ou remplacées par les termes « agent public » avant le 21 juin 2019.

Selon le régime en vigueur jusqu'ici, cette opération n'était pas exécutée par les responsables de traitement de leur propre chef, mais seulement à la demande de la personne concernée.

COMPLIANCE & REGULATORY
FRÉDÉRIC SAFFROY ASSOCIÉ
CORINNE THIÉRACHE ASSOCIÉ
CAROLE BUI AVOCAT
JUSTINE CLERC AVOCAT

ALICE GAUTRON AVOCAT
LAURA RAIMONDO AVOCAT
JEANNE QUENEUDEC AVOCAT

ALERION
www.alerionavocats.com

L'allègement des formalités préalables – Si la collecte de DCPM est nécessaire à la finalité du traitement (ex. traitement relatif aux remboursements de soins par une complémentaire santé réservée aux militaires), le responsable de traitement doit :

- **Informer la Direction du renseignement et de la sécurité de la défense (« DRSD »)** de la mise en œuvre du traitement par le biais d'un formulaire disponible en ligne.

La DRSD demande que chaque entreprise détenant des DCPM désigne un responsable, ayant lui-même accès ou la possibilité d'accéder aux DCPM, qui sera le correspondant de la DRSD, notamment pour la réalisation d'enquêtes administratives de sécurité.

Ce nouveau dispositif met fin au régime d'autorisation de la CNIL délivrée avec l'avis du Ministre de la défense après enquête administrative et répond au principe de responsabilisation des acteurs (article 24 et suivants du RGPD). Le régime déclaratif antérieurement applicable aux associations a également été supprimé.

- **Informer les personnes de son organisation accédant aux DCPM qu'elles sont susceptibles de faire l'objet d'une enquête administrative de sécurité.**

Si l'enquête aboutit à la conclusion que les personnes accédant aux données constituent une menace pour la sécurité des militaires concernés, la DRSD en informe le responsable de traitement dans les trois mois. Le responsable de traitement a alors l'obligation de refuser l'accès de ces personnes aux données et d'avertir la DRSD des mesures prises à cet effet.

L'obligation de double notification en cas de violation des données – En cas de divulgation ou d'accès non autorisé aux données, l'obligation de notifier à l'autorité de contrôle une violation de données (article 33 du RGPD) est désormais doublée par **une obligation de notification à la DRSD.**

Les sanctions applicables – Les sanctions ont été supprimées du Code pénal (articles 226-16 et 226-17-1) pour être intégrées au Code de la défense (article L. 4123-9-1) :

- Est puni d'un **an d'emprisonnement et 100 000 euros d'amende** le manquement, y compris par négligence, à l'obligation d'information de la DRSD de la mise en œuvre du traitement ;
- Sont punis de **3 ans d'emprisonnement et 300 000 euros d'amende** (i) le fait de permettre l'accès aux données à caractère personnel de militaires à des personnes constituant une menace pour la sécurité des militaires concernés et (ii) le fait de ne pas procéder, y compris par négligence, à la notification auprès de la DRSD d'une violation de données à caractère personnel.

En tout état de cause, il est rappelé que quelles que soient les données personnelles traitées, le RGPD est applicable à leur traitement, automatisé ou non (droit d'information et d'accès de la personne concernée, clause de sous-traitance, registre des activités de traitement, sécurité des données personnelles, limitation de la conservation, etc.).

En résumé

La collecte de données révélant la qualité de militaires implique le respect d'un processus contraignant sous le contrôle de la DRSD. Avant de procéder ou de poursuivre la collecte de telles données, les responsables de traitement doivent **avant le 21 juin 2019** s'interroger sur la pertinence et la nécessité d'une telle collecte au regard de la finalité du traitement mis en œuvre.

Si la collecte des DCPM n'apparaît pas indispensable, les responsables de traitement devront, au choix :

- **Supprimer** les données révélant la qualité de militaire, ou
- **Remplacer** les données révélant la qualité de militaire par la qualité « d'agent public ».

Si la collecte des DCPM est indispensable à la finalité du traitement, les responsables de traitement sont alors soumis au **respect du dispositif de protection des DCPM** qui impose de :

1. Informer la DRSD de la collecte des DCPM ;
2. Informer son personnel accédant aux DCPM de la possibilité de faire l'objet d'une enquête administrative ;
3. Refuser aux personnes l'accès aux DCPM si la DRSD l'exige à la suite d'une enquête administrative ;
4. Notifier les violations de données à la DRSD (en plus de l'obligation de notification auprès de la CNIL).

COMPLIANCE & REGULATORY
FRÉDÉRIC SAFFROY ASSOCIÉ
CORINNE THIÉRACHE ASSOCIÉ
CAROLE BUI AVOCAT
JUSTINE CLERC AVOCAT

ALICE GAUTRON AVOCAT
LAURA RAIMONDO AVOCAT
JEANNE QUENEUDEC AVOCAT

ALERION
www.alerionavocats.com